



LAPORAN ONSITE ASSESSMENT INDEKS KAMI



INDEKS
KEAMANAN
INFORMASI

Instansi/Perusahaan: Pemerintah Provinsi Papua Barat	Pimpinan Unit Kerja: Frans P. Istia, S.Sos., M.M. 19690310 199103 1 017
Unit Kerja: Dinas Komunikasi, Informatika, Persandian, dan Statistik Provinsi Papua Barat	Narasumber Instansi: <ol style="list-style-type: none"> Zaenal Fanumbi, S.T. 19810621 200909 1 002 Gusthyni Payuk, S.T., M.Si. 19770821 201004 2 001 Yuliana Moututi, S.H. 19770610 201104 2 001 Ahmad Ismail Samad, S.Kom. 19800915 201004 1 002 Indra Arif Budi Sulistiawan, S.T. 19800720 201004 1 001 Oktofianus R. Manupapam 19830630 200904 1 006
Alamat: Jl. Abraham Atururi (Komplek Perkantoran Arfai), Anday, Distrik Manokwari, Kabupaten Manokwari, Papua Barat. 98315	Asesor: <ol style="list-style-type: none"> Nurchaerani, S.E. 19650708 198710 2 003 Guruh Prasetyo Putro, S.ST., M.Si (Han). 19820527 200312 1 003 Ikrima Galuh Nasucha, S.Tr.TP. 19930329 201412 2 002 Carissa Mega Yulianingrum, S.Tr.TP. 19930720 201611 2 001
Email: diskominfo_persandian @papuabaraprov.go.id	
Tel/ Fax: 082239048229	
A. Ruang Lingkup: <ol style="list-style-type: none"> Instansi / Unit Kerja: Dinas Komunikasi, Informatika, Persandian, dan Statistik Provinsi Papua Barat. Fungsi Kerja: 	

Sesuai dengan Peraturan Gubernur Provinsi Papua Barat Nomor 1 Tahun 2019 disebutkan bahwa Dinas Komunikasi, Informatika, Persandian dan Statistik Provinsi Papua Barat mempunyai tugas membantu Gubernur melaksanakan urusan Pemerintahan di bidang Komunikasi Informatika, Persandian dan Statistik yang menjadi kewenangan daerah dan tugas pertolongan yang diberikan kepada daerah. Dalam melaksanakan tugas tersebut, Dinas Komunikasi, Informatika, Persandian, dan Statistik Provinsi Papua Barat melaksanakan fungsi:

- a. Perumusan kebijakan teknis di bidang komunikasi dan informatika, persandian dan statistik;
- b. Penyelenggaraan urusan pemerintahan dan pelayanan umum di bidang komunikasi dan informatika, persandian dan statistik;
- c. Pembinaan dan pelaksanaan tugas di bidang komunikasi dan informatika, persandian dan statistik;
- d. Pelaksanaan ketatausahaan Dinas; dan
- e. Pelaksanaan tugas lain yang diberikan oleh Gubernur sesuai dengan tugas dan fungsinya.

3. Lokasi:

No	Nama Lokasi	Alamat
1	Kantor Pusat	Jl. Abraham Atururi (Komplek Perkantoran Arfai), Anday, Distrik Manokwari, Kabupaten Manokwari, Papua Barat. 98315
2	Data Center	- Hanya ada server yang dikelola di Bidang TIK untuk mengelola aplikasi pemerintahan.
3	Disaster Recovery Center (DRC)	-

B. Nama /Jenis Layanan Publik:

Layanan Infrastruktur (NOC, Jaringan, Server) dan Aplikasi Sistem informasi yang dikelola oleh Diskominfo Provinsi Papua Barat.

C. Aset TI yang kritikal:

1. Informasi:

- Data pribadi pemilik sertifikat elektronik
- Data pegawai Pemerintah Provinsi Papua Barat

2. Aplikasi:

- Aplikasi SIDASSKEN
- Website Pemprov Papua Barat
- Aplikasi Lapor
- Aplikasi SIAK+
- Aplikasi e-office (masih dalam pengembangan)
- Aplikasi SIMPEG (masih dikelola OPD)
- Aplikasi SIKKEPO (masih dikelola OPD)
- Aplikasi SIPD (masih dikelola OPD)

3. Server:

-

4. Infrastruktur Jaringan/Network:

- Telkom (lokal), Dewata Telematika (global)

D. DATA CENTER (DC):

- ADA, dalam ruangan khusus (Ruang server dikelola internal)
- ADA, jadi satu dengan ruang kerja
- TIDAK ADA

Diskominfo Provinsi Papua Barat belum memiliki infrastruktur data center yang sesuai dengan kelayakan standar sebagai sebuah data center yang memadai.

E. DISASTER RECOVERY CENTER (DRC):

- ADA Dikelola Internal Dikelola Vendor :
- TIDAK ADA

Diskominfo Provinsi Papua Barat belum menerapkan konsep backup data center (Disaster Recovery Center). Ada colocation server secara fisik di Global Internusa, Jogjakarta untuk backup aplikasi jika bermasalah.

**Status Ketersediaan Dokumen Kerangka Kerja
Sistem Manajemen Keamanan Informasi (SMKI)**

No	Nama Dokumen	Ya	Tdk	Keterangan (D: Draf, R:Rilis, T:Tersosialisasikan)
	Kebijakan, Sasaran, Rencana, Standar			
1	Kebijakan Keamanan Informasi	Ya		R, Pergub tentang Penyelenggaraan SPBE Pemerintah Provinsi Papua Barat
2	Organisasi, Peran dan Tanggungjawab Keamanan Informasi	Ya		R, Pergub tentang Uraian Tugas dan Fungsi Diskominfo Papua Barat
3	Panduan Klasifikasi Informasi		Tdk	-
4	Kebijakan Manajemen Risiko TIK		Tdk	-
5	Kerangka Kerja Manajemen Kelangsungan Usaha (Business Continuity Management)		Tdk	-
6	Kebijakan Penggunaan Sumberdaya TIK		Tdk	-
	Prosedur/ Pedoman:			
1	Pengendalian Dokumen		Tdk	-
2	Pengendalian Rekaman/Catatan		Tdk	-
3	Audit Internal SMKI	Ya		R, Pergub tentang Penyelenggaraan SPIP di Lingkungan Pemerintah Provinsi Papua Barat
4	Tindakan Perbaikan & Pencegahan		Tdk	-
5	Pelabelan, Pengamanan, Pertukaran & Disposal Informasi	Ya		R, Pergub tentang Pedoman Pelaksanaan Penghapusan Barang Milik Daerah
6	Pengelolaan Removable Media & Disposal Media		Tdk	-

7	Pemantauan (Monitoring) Penggunaan Fasilitas TIK		Tdk	-
8	User Access Management		Tdk	-
9	Teleworking		Tdk	-
10	Pengendalian instalasi software & HAKI		Tdk	-
11	Pengelolaan Perubahan (Change Management) TIK		Tdk	-
12	Pengelolaan & Pelaporan Insiden Keamanan Informasi	Ya		R, Panduan Teknis Penanganan Insiden Siber

Tabel 1. Ceklist Ketersediaan Dokumen SMKI (Indeks KAMI)

Dokumen yang diperiksa:

1. Peraturan Daerah Nomor 1 Tahun 2019 tentang Organisasi dan Tata Kerja Dinas Komunikasi, Informatika, Persandian, dan Statistik Provinsi Papua Barat.
2. Peraturan Daerah Nomor 18 Tahun 2018 tentang Uraian Tugas dan Fungsi Dinas Komunikasi, Informatika, Persandian, dan Statistik Provinsi Papua Barat.
3. Peraturan Daerah Nomor 12 Tahun 2019 tentang Pedoman Pengelolaan Barang Milik Daerah.
4. Peraturan Gubernur Nomor 40 Tahun 2020 tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Pemerintah Provinsi Papua Barat.
5. Peraturan Gubernur Nomor 26 Tahun 2016 tentang Kode Etik Pegawai di Lingkungan Pemda Provinsi Papua Barat.
6. Peraturan Gubernur Nomor 19 Tahun 2014 tentang Pedoman Pelaksanaan Penghapusan Barang Milik Daerah.
7. Peraturan Gubernur Nomor 10 Tahun 2011 tentang Penyelenggaraan Sistem Pengendalian Internal Pemerintah di Lingkungan Pemda Provinsi Papua Barat.
8. Dokumen DPA Tahun 2021.
9. Dokumen Rencana Strategis (Renstra) Tahun 2017-2022.
10. Dokumen Non-disclosure Agreement (NDA) dengan BSrE.
11. Dokumen Rencana Kerja (Renja).
12. Panduan Teknis Penanganan Insiden Siber.

Bukti-bukti (rekaman/arsip) penerapan SMKI:

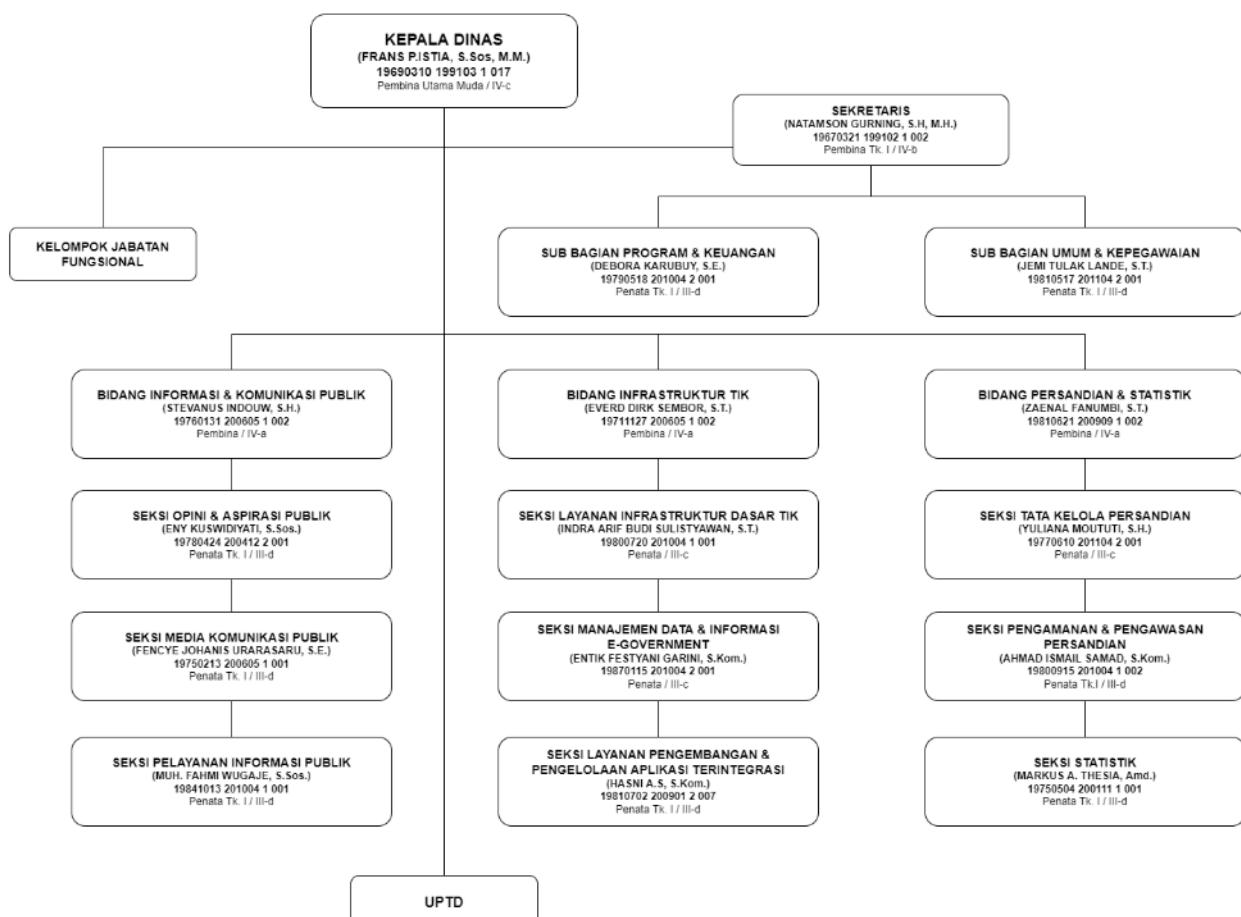
1. Tangkapan Layar Statistik Pengunjung website papuabaraprov.go.id.
2. Foto kegiatan literasi keamanan informasi.
3. Dokumentasi terkait lainnya.

Berdasarkan verifikasi terhadap dokumen dan wawancara terhadap narasumber instansi/lembaga disimpulkan sebagai berikut:

I. KONDISI UMUM:

1. Sesuai dengan Pergub Provinsi Papua Barat Nomor 18 Tahun 2018 disebutkan bahwa Dinas Komunikasi, Informatika dan Statistik Provinsi Papua Barat mempunyai tugas membantu Gubernur melaksanakan urusan pemerintahan bidang Komunikasi, Informatika, Statistik dan Persandian yang menjadi kewenangan daerah, serta melaksanakan tugas dekonsentrasi, yang dipimpin oleh seorang Kepala Dinas, yang berada di bawah dan bertanggung jawab kepada Gubernur melalui Sekretaris Daerah.

Adapun struktur Diskominfo Provinsi Papua Barat adalah sebagai berikut:



Gambar 1. Struktur Organisasi Dinas Komunikasi, Informatika, Persandian, dan Statistik Provinsi Papua Barat

2. SDM Dinas Komunikasi, Informatika, Persandian, dan Statistik Provinsi Papua Barat (per-Tahun 2021) sebanyak 45 orang, dengan rincian sebagai berikut:

Komposisi Status Kepegawaian:

- PNS 34 orang
- CPNS 2 orang
- Non-ASN 9 orang

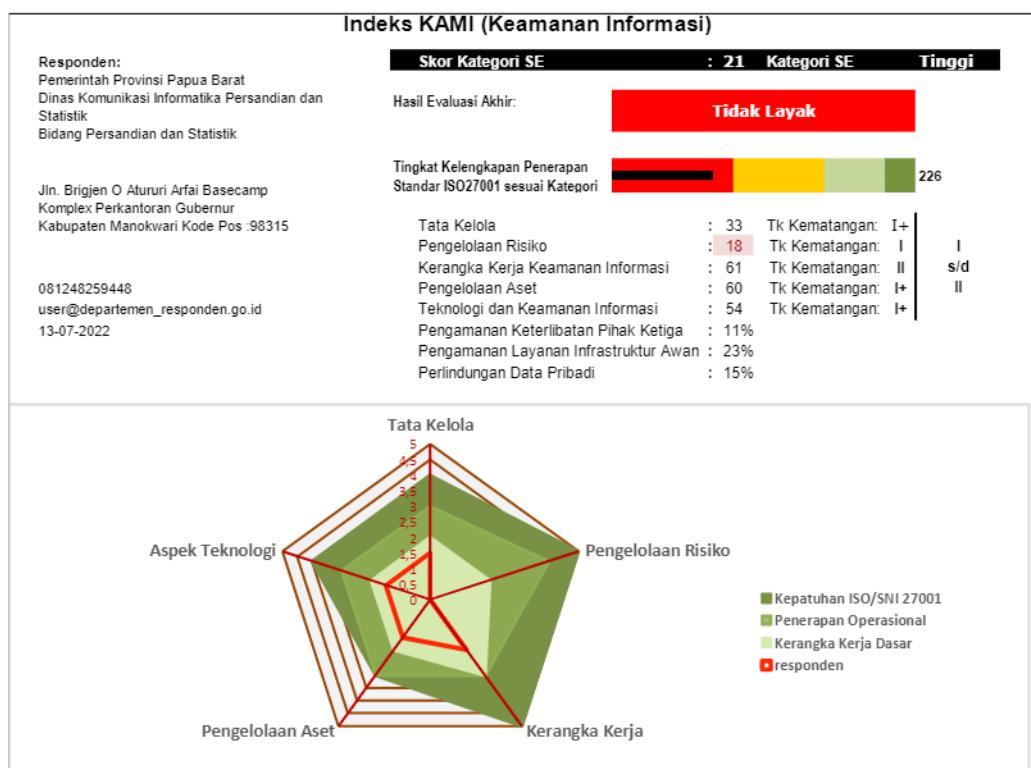
3. Berdasarkan verifikasi terhadap hasil Self Assessment isian file Indeks KAMI diperoleh hasil sebagai berikut:

Dinas Komunikasi, Informatika, Persandian, dan Statistik Provinsi Papua Barat mengelola Sistem Elektronik dalam kategori **TINGGI** dengan hasil evaluasi akhir pada level **TIDAK LAYAK** dengan tingkat kelengkapan penerapan standar ISO 27001 sesuai kategori pada skor nilai **254**.

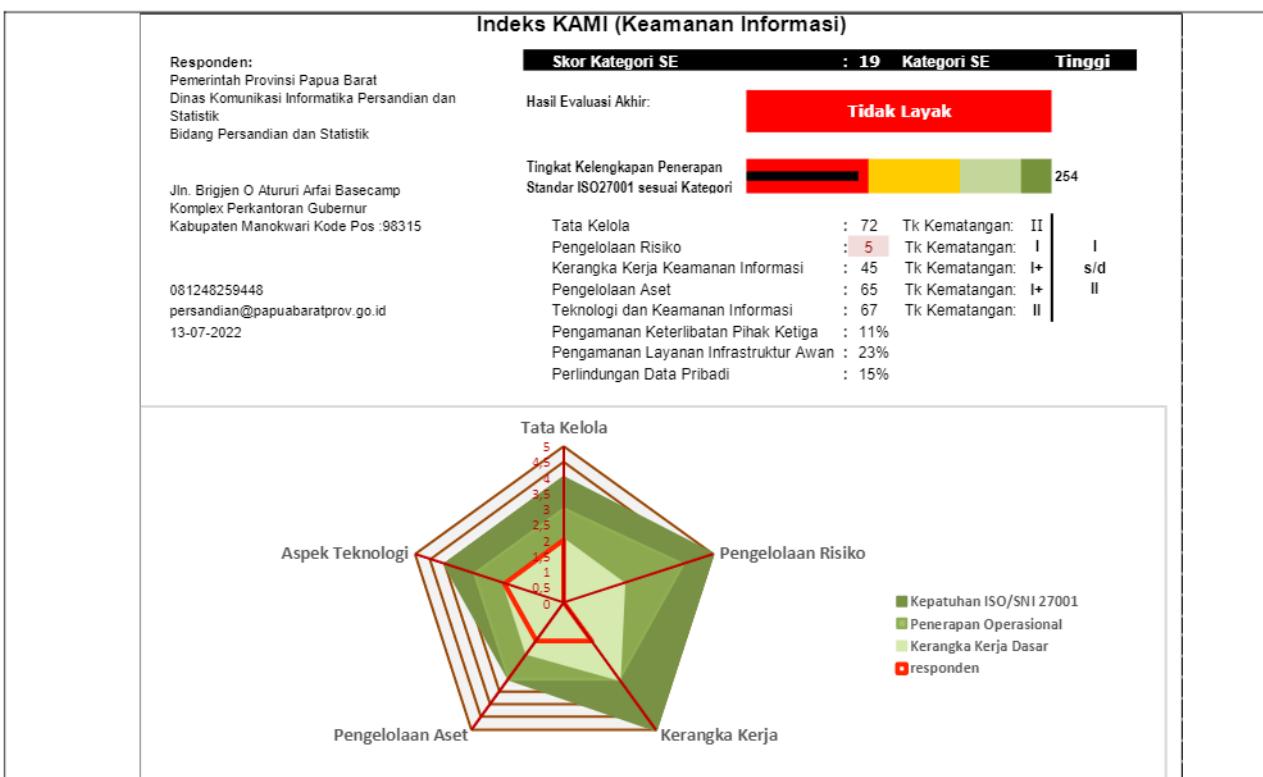
Catatan:

Verifikasi pada Area Suplemen tidak dilakukan karena belum tersajinya data dukung oleh pihak Diskominfo Provinsi Papua Barat dan juga karena keterbatasan waktu verifikasi oleh Tim BSSN. Diharapkan penilaian pada Area Suplemen dapat dilakukan pada kegiatan verifikasi selanjutnya.

Total Score Sebelum Verifikasi: 226 (ref. Penilaian Indeks KAMI 2022)



Total Score Setelah Verifikasi: 254 (ref. file Indeks KAMI pasca Verifikasi)



II. ASPEK TATA KELOLA:

A. Kekuatan/Kematangan

1. Pimpinan dari Diskominfo Papua Barat sudah menetapkan program keamanan informasi sebagai bagian dari tanggung jawab manajemen di antaranya sudah adanya penetapan kebijakan keamanan informasi. Salah satu hal ini adalah dengan dibuktikan terkait program keamanan informasi dalam ITSP atau inisiatif-inisiatif proyek terkait.
2. Diskominfo Papua Barat sudah menetapkan fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab dalam mengelola dan mengimplementasikan program keamanan informasi dan memasikannya kepatuhannya.
3. Pejabat/petugas pelaksana pengamanan informasi sudah ditunjuk di dalam organisasi yang mempunyai wewenang untuk mengimplementasikan program keamanan informasi yang akan dilaksanakan.
4. Alokasi sumber daya terkait pelaksanaan program keamanan informasi sudah direncanakan dan disediakan dalam rangka memastikan pengelolaan keamanan informasi telah memadai dan dipastikan kepatuhannya.
5. Peran fungsi pelaksana pengamanan informasi belum semuanya telah dipetakan pada kebutuhan program keamanan informasi secara lengkap, termasuk

kebutuhan audit internal dan persyaratan segregasi kewenangan terhadap kontrol-kontrol keamanan yang dilaksanakan.

6. Diskominfo Papua Barat sudah mendefinisikan persyaratan/standar kompetensi dan keahlian khususnya terkait pelaksana pengelolaan keamanan informasi.
7. Semua pelaksana pengamanan informasi yang terlibat di Diskominfo Papua Barat belum semuanya memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku khususnya terkait aspek kontrol teknis dan operasional keamanan informasi.
8. Pimpinan Diskominfo Papua Barat dan fungsi pengelola keamanan informasi sudah merencanakan dan menerapkan program sosialisasi dan peningkatan pemahaman terhadap keamanan informasi melalui beberapa media (seperti email, poster, training, dll) dan dievaluasi hasil penerapannya untuk memastikan kepatuhannya bagi semua pihak yang terkait.
9. Program peningkatan kompetensi dan keahlian sudah diidentifikasi terhadap pelaksana pengelolaan keamanan informasi namun belum direncanakan setiap tahun dalam rangka memastikan kebutuhan penerapan kontrol keamanan informasi telah terpenuhi.
10. Beberapa persyaratan keamanan informasi yang terdapat dalam standard yang berlaku sudah terintegrasi ke dalam proses kerja yang ada namun sebagian lainnya masih bersifat aktivitas kontrol tambahan yang dilakukan.
11. Diskominfo Papua Barat belum semuanya mengidentifikasi data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku.
12. Tanggung jawab pengelolaan keamanan informasi yang didelegasikan kepada fungsi pengelola keamanan informasi sudah mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, dan untuk mengidentifikasi persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada namun belum terimplementasi secara memadai.
13. Fungsi pengelola keamanan informasi sudah secara rutin melaporkan kepada manajer mengenai kondisi, kinerja/efektivitas dan kepatuhan program keamanan informasi.
14. Metrik, parameter dan proses pengukuran kinerja pengelolaan keamanan informasi sudah didefinisikan yang mencakup mekanisme, waktu pengukuran, pelaksananya, dan harus diukur dan dievaluasi pemantauannya secara berkala serta dilakukan eskalasi pelaporan kepada manajer untuk memastikan efektivitas dari proses pengelolaan program dan kontrol keamanan informasi yang diterapkan.
15. Pimpinan Diskominfo Papua Barat sudah mendefinisikan dan menerapkan program penilaian kinerja terkait penerapan proses keamanan informasi bagi individu (pejabat & petugas) pelaksananya sebagai bagian dari proses evaluasi

tingkat pemahaman individu tersebut terhadap pengelolaan keamanan informasi di organisasi.

16. Target dan sasaran pengelolaan keamanan informasi tidak semua kontrol utama yang telah didefinisikan dan diformulasikan, serta dilakukan evaluasi dan mengkaji hasil pencapaianya namun belum secara rutin dilaksanakan. Hasil evaluasi terhadap target dan sasaran tersebut dapat dilaporkan statusnya kepada pimpinan organisasi belum konsisten terealisasi ditindaklanjuti.

B. Kelemahan/Kekurangan

1. Fungsi pengelola keamanan informasi belum secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan, dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak.
2. Diskominfo Papua Barat belum menetapkan tanggung jawab untuk merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity and disaster recovery plans*) termasuk pengalokasian kebutuhan sumber daya dan proses yang diperlukan dalam rangka menjamin kelangsungan bisnis ketika terjadi kondisi darurat.
3. Setiap permasalahan keamanan informasi yang terjadi di Diskominfo Papua Barat belum menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis dalam melakukan tindakan perbaikan yang diperlukan untuk meningkatkan efektivitas pelaksanaan kontrol keamanan informasi.
4. Diskominfo Papua Barat belum menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya.

III. ASPEK RISIKO:

A. Kekuatan/Kematangan

1. Program kerja pengelolaan risiko keamanan informasi sudah menjadi perencanaan organisasi namun belum disetujui secara resmi oleh pimpinan Diskominfo Papua Barat.

B. Kelemahan/Kekurangan

1. Pimpinan Diskominfo Papua Barat belum menentukan penanggung jawab proses manajemen risiko yang dilakukan dan proses eskalasi terhadap pelaporan hasil analisa risiko keamanan informasi sampai ke tingkat pimpinan organisasi

2. Kerangka kerja pengelolaan risiko keamanan informasi belum terdokumentasi dalam dokumen metodologi manajemen risiko sehingga belum dapat digunakan secara resmi.
3. Kerangka kerja pengelolaan risiko ini belum mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian di Diskominfo Papua Barat.
4. Ambang batas tingkat risiko yang dapat diterima belum ditetapkan oleh pimpinan Diskominfo Papua Barat dalam rangka melakukan evaluasi terhadap tingkatan risiko yang dianalisa.
5. Dalam proses pengelolaan manajemen risiko, Diskominfo Papua Barat belum terdapat pendefinisian mengenai kepemilikan dan pihak pengelola (*custodian*) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut.
6. Ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama belum teridentifikasi.
7. Pada proses analisa risiko belum ditetapkan mengenai dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sesuai dengan definisi yang ada.
8. Diskominfo Papua Barat belum menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi).
9. Langkah-langkah mitigasi dan penanggulangan risiko yang ada belum disusun secara sistematis dan memadai.
10. Langkah mitigasi risiko belum disusun sesuai dengan tingkat prioritas dan target penyelesaiannya serta penanggungjawabnya dan belum terdapat mekanisme untuk memastikan efektivitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalkan dampak terhadap operasional layanan TIK.
11. Status penyelesaian langkah mitigasi risiko belum dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya.
12. Belum terdapat proses evaluasi yang obyektif/terukur terhadap penyelesaian langkah mitigasi yang telah diterapkan untuk memastikan konsistensi dan efektivitasnya.
13. Profil risiko berikut bentuk mitigasinya belum secara berkala dikaji ulang dalam rangka memastikan akurasi dan validitasnya, termasuk merevisi profil tersebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru.
14. Kerangka kerja pengelolaan risiko tidak dikaji untuk memastikan/meningkatkan efektivitasnya.

15. Pengelolaan risiko belum menjadi bagian dari kriteria proses penilaian obyektif kinerja efektivitas pengamanan..

IV. ASPEK KERANGKA KERJA:

A. Kekuatan/Kematangan

1. Kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan didokumentasikan dengan jelas, termasuk peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya.
2. Kebijakan keamanan informasi sudah ditetapkan secara formal, namun belum dipublikasikan kepada semua staf/karyawan termasuk pihak terkait.
3. Sudah adanya proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga.
4. Proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi sudah baku namun pelaksanaan dalam penetapan sebagai insiden keamanan informasi untuk ditindaklanjuti belum sesuai dengan prosedur yang diberlakukan.
5. Diskominfo Papua Barat sudah menetapkan dan menerapkan kebijakan dan prosedur operasional terkait implementasi security patch, alokasi tanggung jawab untuk memonitor adanya rilis security patch baru, hingga pelaporannya.
6. Aspek keamanan informasi sudah diidentifikasi untuk beberapa aktivitas proyek selama proses manajemen proyek yang dilakukan namun belum semuanya tertuang dalam dokumentasi.
7. Proses pengembangan sistem yang aman (*Secure SDLC*) sudah diterapkan dalam proses pengembangan namun belum sepenuhnya mengacu kepada prinsip atau metode sesuai standar platform teknologi yang digunakan.
8. Strategi penerapan keamanan informasi sudah dirumuskan dan ditetapkan sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi.
9. Strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko sudah diidentifikasi namun belum dirumuskan dan ditetapkan secara resmi tetapi beberapa telah terealisasi.
10. Strategi penerapan keamanan informasi sudah direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi.
11. Rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) sudah direalisasikan secara konsisten.

B. Kelemahan/Kekurangan

1. Belum diinformalkan mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya.
2. Kebijakan dan prosedur keamanan informasi yang sudah ditetapkan belum menyeluruh merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyektif tertentu yang telah ditetapkan.
3. Kontrak dengan pihak ketiga belum mencakup aspek-aspek kontrol keamanan informasi seperti proses pelaporan insiden, keharusan menjaga kerahasiaan, penggunaan perangkat lunak yang berlisensi (HAKI), dan tata tertib penggunaan dan pengamanan aset maupun layanan TIK.
4. Konsekuensi dari pelanggaran kebijakan keamanan informasi belum didefinisikan, dikomunikasikan dan ditegakkan pada seluruh pegawai dan pihak ketiga.
5. Belum adanya prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindaklanjuti konsekuensi dari kondisi ini.
6. Belum ada proses yang baku untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul.
7. Ketika terdapat penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, Diskominfo Papua Barat belum terdapat proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya.
8. Kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mencakup persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya belum disusun dan didokumentasikan.
9. Perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) belum ditentukan mengenai komposisi, peran, wewenang dan tanggung jawab tim yang ditunjuk.
10. Uji coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) belum dilakukan sesuai jadwal.
11. Hasil dari perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) belum dievaluasi. Langkah perbaikan atau pemberian yang diperlukan (misal, apabila hasil uji coba menunjukkan bahwa proses pemulihan tidak bisa (gagal)) tidak ditetapkan secara jelas dalam suatu dokumentasi yang resmi.
12. Seluruh kebijakan dan prosedur keamanan informasi belum dievaluasi kelayakannya secara berkala.

13. Diskominfo Papua Barat belum menetapkan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku).
14. Audit internal yang dilakukan tersebut belum mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi.
15. Hasil audit internal tersebut belum dikaji/dievaluasi terkait langkah pemberian dan pencegahan yang diperlukan, ataupun inisiatif peningkatan kinerja keamanan informasi.
16. Hasil audit internal tidak dilaporkan kepada pimpinan organisasi sehingga belum secara memadai ditetapkan langkah-langkah perbaikan atau program peningkatan kinerja keamanan informasi.
17. Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, belum terdapat proses dalam melakukan analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya.
18. Diskominfo Papua Barat belum secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pemberian yang diperlukan, telah diterapkan secara efektif.

V. ASPEK PENGELOLAAN ASET:

A. Kekuatan/Kematangan

1. Daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi sudah didokumentasikan secara lengkap, akurat dan terpelihara (termasuk kepemilikan aset).
2. Sudah adanya proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) namun tidak semuanya tercatat secara sistematis.
3. Sudah tersedianya proses pengelolaan konfigurasi yang diterapkan namun belum terdokumentasi secara konsisten.
4. Beberapa penerapan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko sudah tersedia. Hal ini seperti:
 - Sebagian sudah ada definisi tanggung jawab pengamanan informasi secara individual untuk semua personil di Diskominfo Papua Barat

- Telah ada proses mengenai pengelolaan identitas elektronik dan proses otentifikasi (*username & password*) termasuk kebijakan terhadap pelanggarannya namun tidak terdokumentasi dalam kebijakan/prosedur.
- Beberapa sistem sudah ditetapkan persyaratan dan prosedur pengelolaan/pemberian akses, otentifikasi dan otorisasi untuk menggunakan aset informasi
- Telah ada ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data.
- Sudah berjalannya proses pengecekan latar belakang SDM.
- Sudah ada mekanisme terkait pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.
- Sebagian proses penghancuran data/aset yang sudah tidak diperlukan diatur dalam suatu prosedur.

Beberapa kekuatan dalam pengamanan fisik antara lain:

5. Pengamanan fasilitas fisik (lokasi kerja) sudah diterapkan sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang namun beberapa kontrol fisik belum dilaksanakan.
6. Sudah formalnya proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik.
7. Infrastruktur komputasi telah terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya.
8. Infrastruktur komputasi yang terpasang telah terlindungi dari gangguan pasokan listrik atau dampak dari petir.
9. Proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris) sudah ada namun belum ditetapkan mekanisme ketetapannya.
10. Konstruksi ruang penyimpanan perangkat pengolah informasi penting sudah menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai.
11. Sudah adanya proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting namun pelaksanaannya belum dilakukan secara berkala.

B. Kelemahan/Kekurangan

1. Definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku belum didefinisikan.
2. Proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Diskominfo Papua Barat dan keperluan pengamanannya belum didefinisikan dan ditetapkan secara resmi.
3. Definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut belum didokumentasikan.
4. Belum ditetapkannya proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi.
5. Beberapa penerapan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko belum tersedia. Hal ini seperti:
 - Tidak adanya tata tertib penggunaan komputer, email, internet dan intranet.
 - Belum ditetapkannya tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI.
 - Tidak ada aturan terkait instalasi piranti lunak di aset TI milik Diskominfo Papua Barat.
 - Belum diatur mengenai penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi.
 - Tidak ada ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya.
 - Belum tersedianya proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi.
 - Tidak ada prosedur mengenai proses back-up dan uji coba pengembalian data (restore) secara berkala.
 - Belum adanya ketentuan mengenai pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya.
 - Belum tersedianya prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya (*user access rights*) berikut langkah pemberahan apabila terjadi ketidaksesuaian (*non-conformity*) terhadap kebijakan yang berlaku.
 - Belum ada ketentuan dan prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.
6. Daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya belum didokumentasikan.
7. Belum terdokumentasinya daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya.
8. Prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan belum ditetapkan dan didokumentasikan.
9. Beberapa kelemahan dalam pengamanan fisik antara lain:

- Belum ditetapkannya peraturan pengamanan perangkat komputasi milik Diskominfo Papua Barat apabila digunakan di luar lokasi kerja resmi (kantor).
- Belum ada mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga.
- Belum didefinisikan dan ditetapkannya peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera, dll).
- Belum adanya proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Diskominfo Papua Barat.

VI. ASPEK TEKNOLOGI:

A. Kekuatan/Kematangan

1. Layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan.
2. Jaringan komunikasi sudah disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll).
3. Konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi sudah didokumentasikan namun belum semua dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan.
4. Analisa kepatuhan penerapan konfigurasi standar yang ada sudah dianalisa secara berkala.
5. Jaringan, sistem dan aplikasi yang digunakan secara rutin sudah dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi.
6. Keseluruhan infrastruktur jaringan, sistem dan aplikasi sudah dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada.
7. Keseluruhan infrastruktur jaringan, sistem dan aplikasi sudah dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada.
8. Setiap perubahan dalam sistem informasi sudah direkam pada suatu log pada sistem.
9. Upaya akses oleh yang tidak berhak sudah terrekam di dalam log.
10. Enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada sudah diterapkan pada sebagian data.
11. Semua sistem dan aplikasi sebagian sudah secara otomatis menerapkan manajemen dalam penggantian password secara otomatis pada sistem,

termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama.

12. Beberapa akses yang digunakan untuk mengelola sistem (administrasi sistem) sudah menggunakan bentuk pengamanan khusus yang berlapis.
13. Sudah ada proses untuk menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan.
14. Setiap desktop dan server telah dilindungi dari penyerangan virus (malware).
15. Beberapa rekaman dan hasil analisa (*jejak audit - audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis sudah tersimpan.
16. Sudah adanya proses pelaporan penyerangan virus/malware yang gagal/sukses namun sebagian telah ditindaklanjuti dan diselesaikan.
17. Keseluruhan jaringan, sistem dan aplikasi sudah tersinkronisasi waktu yang akurat, sesuai dengan standar yang ada.
18. Lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yang dibangun telah diterapkan namun belum menyeluruh.

B. Kelemahan/Kekurangan

1. Semua log belum dilakukan analisa secara berkala.
2. Diskominfo Papua Barat belum mempunyai standar dalam menggunakan enkripsi.
3. Pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya belum diterapkan.
4. Sistem dan aplikasi yang digunakan belum menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login, dan penarikan akses.
5. Pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi belum diterapkan.
6. Sistem operasi untuk setiap perangkat desktop dan server belum dimutakhirkan dengan versi terkini.
7. Aplikasi yang ada tidak memiliki dokumentasi mengenai spesifikasi dan fungsi keamanan yang diverifikasi/divalidasi pada saat proses pengembangan dan uji coba.
8. Diskominfo Papua Barat tidak melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin.

VII. REKOMENDASI

Berikut ini rekomendasi yang diberikan dari proses verifikasi:

1. Diskominfo Provinsi Papua Barat segera merumuskan draf Peraturan Gubernur terkait Sistem Manajemen Keamanan Informasi yang diharapkan dapat melengkapi kekurangan substansi dalam penerapan SMKI di ruang lingkupnya.
2. Diskominfo Provinsi Papua Barat segera menetapkan kebijakan terkait manajemen risiko untuk dijadikan pedoman dalam proses manajemen risiko SMKI.
3. Penyusunan dokumen *risk register* (khususnya di ruang lingkup TI) dapat segera dilaksanakan dan disahkan oleh pimpinan.
4. Diskominfo Provinsi Papua Barat segera menyusun prosedur-prosedur terkait yang diperlukan dalam implementasi SKMI sesuai yang dibutuhkan dalam ruang lingkupnya.
5. Perlu dibuatkan penyusunan prosedur BCP dan DRP sebagai upaya pengelolaan kelangsungan layanan TIK di Provinsi Papua Barat.
6. Perlu diperhatikan kembali pemenuhan kelayakan standar infrastruktur data center yang memadai dengan mengevaluasi beberapa keterbatasan yang ada saat ini.
7. Pengintegrasian dan pengelolaan sistem elektronik dan aplikasi di Pemerintah Provinsi Papua Barat dapat segera dilakukan satu pintu di Diskominfo Provinsi Papua Barat.
8. Diskominfo Provinsi Papua Barat sebaiknya merumuskan kebijakan dan prosedur terkait perlindungan data pribadi untuk menjadi pedoman tertulis dalam implementasi yang telah diterapkan saat ini.
9. Kebijakan dan prosedur tentang pengujian aplikasi sebaiknya menjadi syarat wajib dalam pemenuhan keamanan informasi dalam setiap aplikasi yang dikembangkan di Provinsi Papua Barat.

VIII. PENUTUP

Demikian Laporan Onsite Assessment Indeks KAMI Pemerintah Daerah Provinsi Papua Barat T.A. 2022 ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam pelaksanaan pengamanan informasi Pemerintah Daerah Provinsi Papua Barat.

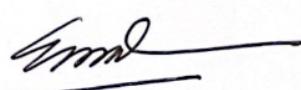
Laporan Onsite Assessment Indeks KAMI Pemerintah Daerah Provinsi Papua Barat T.A. 2022 ini disampaikan kepada:

1. Kepala Badan Siber dan Sandi Negara;
2. Gubernur Provinsi Papua Barat; dan
3. Sekretaris Daerah Provinsi Papua Barat.

Manokwari, 22 Juli 2022

Kepala Bidang Persandian dan
Statistik

Sandiman Madya pada
Direktorat Keamanan Siber dan Sandi
Pemerintah Daerah



Zaenal Fanumbi, S.T.
19810621 200909 1 002



Nurchaerani, S.E.
19650708 198710 2 003

Mengetahui,
Kepala Diskominfo Persandian dan Statistik
Provinsi Papua Barat



Trans P. Istia, S.Sos., M.M.
19690310 199103 1 017