

	<b>LAPORAN ONSITE ASSESSMENT INDEKS KAMI</b>	 INDEKS KEAMANAN INFORMASI
<b>Instansi/Perusahaan:</b>  Pemerintah Provinsi Bali	<b>Pimpinan Unit Kerja :</b>  Gede Pramana, ST., MT. 19680531 199703 1 002	
<b>Unit Kerja:</b>  Dinas Komunikasi, Informatika, dan Statistik Provinsi Bali	<b>Narasumber Instansi :</b>  1. I Putu Sundika, ST., MT 19761226 200604 1 003 2. I Putu Riska Desthara, S.I.P. 19880505 200701 1 006 3. Ida Bagus Gede Darma Kusuma, SE 19720813 200901 1 006 4. I Made Widiartha, ST., M.A.P 19760726 200604 1 008 5. I Gusti Ngurah Puspa Udiyana, S.Kom, S.E., M.Si 19820204 200604 1 009 6. I Dewa Ketut Agung Purbayana, S.Kom -	
<b>Alamat:</b>  Jl. Panjaitan No.7, Sumerta Kelod, Denpasar Sel, Sumerta Kelod, Denpasar Selatan, Kota Denpasar, Bali 80234		
<b>Email:</b>  diskominfos@baliprov.go.id	<b>Asesor :</b>  1. Dwi Kardono, S.Sos., M.A. 19710218 199110 1 001 2. Guruh Prasetyo Putro, S.ST., M.Si (Han) 19820527 200312 1 003 3. Mochamad Jazuly, S.S.T.TP. 19920625 201412 1 002 4. Rey Citra Kesuma, S.Tr.TP 19960402 201812 1 001	
<b>Tel/ Fax:</b>  (0361) 225859		

**A. Ruang Lingkup:**

## 1. Instansi / Unit Kerja:

Dinas Komunikasi, Informatika, dan Statistik Provinsi Bali.

## 2. Fungsi Kerja:

Sesuai dengan Peraturan Gubernur Provinsi Bali Nomor 56 Tahun 2021 disebutkan bahwa Dinas Komunikasi, Informatika dan Statistik Provinsi Bali mempunyai tugas membantu Gubernur melaksanakan urusan pemerintahan bidang komunikasi, informatika, statistik dan persandian yang menjadi kewenangan daerah, serta melaksanakan tugas dekonsentrasi sampai dengan dibentuknya Sekretariat Gubernur sebagai Wakil Pemerintah Pusat dan melaksanakan tugas pembantuan sesuai bidang tugasnya. Dalam melaksanakan tugas tersebut, Dinas Komunikasi, Informatika, dan Statistik Provinsi Bali melaksakan fungsi:

- a. Perumusan kebijakan teknis dibidang Komunikasi, Informatika, Statistika dan Persandian yang menjadi kewenangan Provinsi;
- b. Pelaksanaan kebijakan di bidang Komunikasi, Informatika, Statistik dan Persandian yang menjadi kewenangan Provinsi;
- c. Penyelenggaraan administrasi Dinas bidang komunikasi, informatika dan
- d. Statistik dan Persandian;
- e. Penyelenggaraan evaluasi dan pelaporan Dinas;
- f. Penyelenggaraan fungsi lain yang diberikan oleh Gubernur terkait dengan tugas dan fungsinya.

## 3. Lokasi:

No	Nama Lokasi	Alamat
1	Kantor Pusat	Jl. Panjaitan No.7, Sumerta Kelod, Denpasar Sel, Sumerta Kelod, Denpasar Selatan, Kota Denpasar, Bali 80234
2	Data Center	Jl. Basuki Rachmat Niti Mandala Renon No. 1, Sumerta Kelod, Denpasar Sel, Sumerta Kelod, Denpasar Selatan, Kota Denpasar, Bali 80234
3	Disaster Recovery Center (DRC)	-

**B. Nama /Jenis Layanan Publik:**

Layanan Infrastruktur (Data Center, NOC, Jaringan, Server) dan Aplikasi Sistem Informasi (SIKUAT, Simpeg, Kantor Virtual, Absensi, SiGapura, Bali Media Center, LoveBali, Sistem Antrian, Sensus Desa Adat) yang dikelola oleh Diskominfos Provinsi Bali.

**C. Aset TI yang kritikal:**

## 1. Informasi:

- Data asesmen keamanan siber di lingkup Pemprov Bali
- Data pribadi pemilik sertifikat elektronik
- Data statistik
- Data pegawai Pemprov Bali

## 2. Aplikasi:

- Aplikasi SSO (kategori SE Strategis)
- Aplikasi SIMPEG
- Aplikasi SIKUAT
- Aplikasi LoveBali
- Aplikasi Sipenda
- Aplikasi Bali Media Center
- Aplikasi Absensi

## 3. Server :

- Server Simpeg
- Server website Provinsi Bali
- Server aplikasi internal OPD

## 4. Infrastruktur Jaringan/Network:

- Telkom, LintasArta, Indosat

**D. DATA CENTER (DC):**

- ADA, dalam ruangan khusus (Ruang server dikelola internal)

Diskominfos Provinsi Bali memiliki data center yang terbatas untuk pengelolaan aplikasi di lingkup Perangkat Daerah se-Provinsi Bali yang berlokasi di Gedung Unit 4 lantai 2 Kantor Gubernur, namun belum memenuhi kelayakan standar sebagai sebuah data center yang memadai.

- ADA, jadi satu dengan ruang kerja

- TIDAK ADA

**E. DISASTER RECOVERY CENTER (DRC):**

- ADA       Dikelola Internal       Dikelola Vendor :  
 TIDAK ADA

Diskominfos Provinsi Bali belum menerapkan konsep backup data center (Disaster Recovery Center) secara menyeluruh. Untuk saat ini layanan backup database aplikasi dikelola dengan memanfaatkan layanan berbasis Cloud Computing yang disediakan oleh Amazon (AWS).

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

No	Nama Dokumen	Ya	Tdk	Keterangan (D: Draf, R:Rilis, T:Tersosialisasikan)
	<b>Kebijakan, Sasaran, Rencana, Standar</b>			
1	Kebijakan Keamanan Informasi	Ya		R, Pedoman Manajemen Keamanan Informasi
2	Organisasi, Peran dan Tanggungjawab Keamanan Informasi	Ya		R, Pergub Perangkat Daerah
3	Panduan Klasifikasi Informasi	Ya		R, Pergub Pelayanan Informasi Publik
4	Kebijakan Manajemen Risiko TIK	Ya		R, Pedoman Manajemen Risiko SPBE
5	Kerangka Kerja Manajemen Kelangsungan Usaha (Business Continuity Management)	Ya		R, Panduan Penanganan Insiden
6	Kebijakan Penggunaan Sumberdaya TIK	Ya		R, Pedoman Keamanan Informasi SPBE, Pedoman Keamanan Siber
	<b>Prosedur/ Pedoman:</b>			
1	Pengendalian Dokumen		Tdk	Pergub Persandian

2	Pengendalian Rekaman/Catatan		Tdk	
3	Audit Internal SMKI		Tdk	Pergub SPBE
4	Tindakan Perbaikan & Pencegahan		Tdk	Keputusan Gubernur Pembentukan CSIRT
5	Pelabelan, Pengamanan, Pertukaran & Disposal Informasi		Tdk	Pergub Tata Kearsipan
6	Pengelolaan Removable Media & Disposal Media	Ya		R, Pedoman Keamanan Siber
7	Pemantauan (Monitoring) Penggunaan Fasilitas TIK	Ya		R, Pedoman Keamanan Siber
8	User Access Management	Ya		R, Pedoman Manajemen Keamanan Informasi
9	Teleworking	Ya		R, Pedoman Manajemen Keamanan Informasi
10	Pengendalian instalasi software & HAKI	Ya		R, Pedoman Manajemen Keamanan Informasi
11	Pengelolaan Perubahan (Change Management) TIK		Tdk	Pergub SPBE
12	Pengelolaan & Pelaporan Insiden Keamanan Informasi		Tdk	Keputusan Gubernur Pembentukan CSIRT

Tabel 1. Ceklist Ketersediaan Dokumen SMKI (Indeks KAMI)

**Dokumen yang diperiksa:**

1. Peraturan Gubernur Bali tentang Sistem Pemerintahan Berbasis Elektronik Pemerintah Provinsi Bali.
2. Peraturan Gubernur Bali tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi, Serta Tata Kerja Perangkat Daerah di Lingkungan Pemerintah Provinsi Bali.
3. Peraturan Gubernur Bali tentang Penyelenggaraan Persandian Untuk Pengamanan Informasi di Lingkungan Pemerintah Provinsi Bali.

4. Peraturan Gubernur Bali tentang Penyelenggaraan Sertifikat Elektronik di Lingkungan Pemerintah Provinsi Bali.
5. Keputusan Kepala Dinas Komunikasi, Informatika dan Statistik Provinsi Bali tentang Pedoman Manajemen Keamanan Informasi di Lingkungan Dinas Komunikasi, Informatika dan Statistik Provinsi Bali.
6. Peraturan Gubernur Provinsi Bali Nomor 13 Tahun 2014 tentang Tata Kearsipan Pemerintah Provinsi Bali.
7. Keputusan Gubernur Bali tentang Pembentukan dan Susunan Keanggotaan Tim Koordinasi Sistem Pemerintahan Berbasis Elektronik di Lingkungan Pemerintah Provinsi Bali.
8. Instruksi Gubernur tentang Penyelenggaraan Sistem Pemerintahan Berbasis Elektronik Pemerintah Provinsi Bali.
9. Keputusan Kepala Dinas Komunikasi, Informatika dan Statistik Provinsi Bali tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik Provinsi Bali.
10. Keputusan Gubernur Bali tentang Pembentukan dan Susunan Keanggotaan Computer Security Incident Response Team Provinsi Bali (BALIPROV-CSIRT)
11. Surat Edaran Sekda Pemprov Bali tentang Pemanfaatan Tanda Tangan Elektronik pada Dokumen Informasi Publik Pemerintah Provinsi Bali.
12. Pedoman Teknis Pelaksanaan Seleksi Pengadaan Tim Pengembangan Sistem Pemerintahan Berbasis Elektronik (SPBE) di Lingkungan Dinas Komunikasi, Informatika dan Statistik Provinsi Bali Pada Tahun Anggaran 2021.
13. Keputusan Kepala Dinas Komunikasi, Informatika dan Statistik Provinsi Bali tentang Pedoman Keamanan Siber Bagi Pegawai di Lingkungan Dinas Komunikasi, Informatika dan Statistik Provinsi Bali.
14. Perjanjian Kerjasama Antara Pemerintah Provinsi Bali dengan Balai Sertifikasi Elektronik Badan Siber dan Sandi Negara tentang Pemanfaatan Sertifikat Elektronik pada Sistem Elektronik di Lingkungan Pemerintah Provinsi Bali.
15. Keputusan Kepala Dinas Komunikasi, Informatika dan Statistik Provinsi Bali tentang Peta Jalan Sistem Pemerintahan Berbasis Elektronik (SPBE) menuju Bali Smart Island 2020-2024.
16. Nota Dinas Laporan Insiden Keamanan.
17. Dokumen Non-disclosure Agreement (NDA) dengan pihak ketiga.
18. Dokumen Non-disclosure Agreement (NDA) dengan tenaga non-ASN.
19. SKP ASN pada Bidang Persandian.
20. Renja Diskominfos 2022
21. Renstra Diskominfos 2018-2023
22. Laporan Akhir Kegiatan Diskominfos Tahun 2021

23. Hasil Survey Pedoman Kamsiber.
24. Data Aset TIK pada Aplikasi SIMDA
25. DPA Dinas Kominfos Provinsi Bali Tahun 2021.
26. SOP Manajemen Risiko
27. SOP Pelayanan Permohonan Informasi Publik.
28. SOP Penghancuran Dokumen Dengan Mesin Penghancur Kertas.
29. SOP Email Sanapati.
30. SOP Pengembangan Aplikasi.
31. Syarat dan Kebutuhan Tim Pengembangan Sistem Pemerintahan Berbasis Elektronik (SPBE) Menuju Bali Smart Island Tahun Anggaran 2021.
32. SK Tenaga Kontrak.
33. SPK Tenaga Kontrak.
34. Kartu Inventaris Ruangan.
35. Surat Pernyataan Perjanjian Kerahasiaan (Non Disclosure Agreement).
36. Risk Register
37. Panduan Penanganan Insiden Siber (CSIRT).
38. Laporan IT Security Assessment.

**Bukti-bukti (rekaman/arsip) penerapan SMKI:**

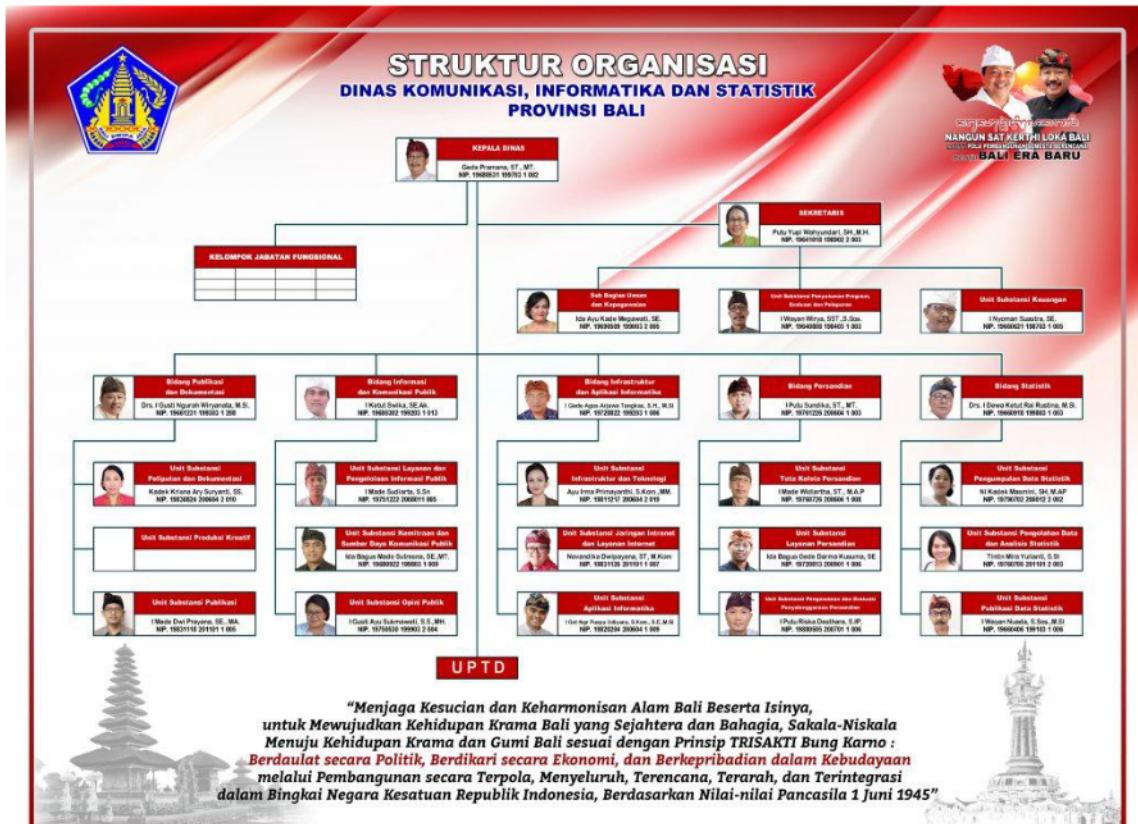
1. Foto Sosialisasi Pedoman Kamsiber, Berita Kegiatan Lentera Siber, Laporan Pelaksanaan Program Literasi Lentera Siber, Notulen Pelatihan Kamsiber.
2. Tangkapan layar Berita Kegiatan Lentera Siber di Media Cetak, Website, Media Sosial, Youtube.
3. Tangkapan layar Aplikasi SSO
4. Tangkapan layar terkait lainnya

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

**I. KONDISI UMUM:**

1. Sesuai dengan Pergub Provinsi Bali Nomor 56 Tahun 2021 disebutkan bahwa Dinas Komunikasi, Informatika dan Statistik Provinsi Bali 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 Diskominfos Provinsi Bali adalah sebagai berikut:



Gambar 1. Struktur Organisasi Dinas Komunikasi, Informatika, dan Statistik Provinsi Bali

2. SDM Dinas Komunikasi, Informatika, dan Statistik Provinsi Bali (per-Tahun 2021) sebanyak 231 orang, dengan rincian sebagai berikut:

#### Komposisi Status Kepegawaian :

- PNS 71 orang (30,73%)
- CPNS 5 orang (2,16%)
- Non-ASN 155 orang (67,09%)

#### Komposisi Eselon PNS :

- Eselon II.a 1 orang
- Eselon III.a 6 orang
- Eselon IV.a 16 orang
- Staf 53 orang

#### Komposisi Jabatan PNS :

- Jabatan Struktural 25 orang (10,82%)
- Jabatan Fungsional Tertentu orang (2,16%)

#### Arsiparis Tk. Ahli ( 0,86% ) :

- Arsiparis Madya 1 orang (0,43%)
- Arsiparis Penyelia 1 orang (0,43%)
- Penerjemah Muda 1 orang (0,43%)
- Jabatan Fungsional Umum 45 orang (19,48%)

#### Pranata Humas Tk. Ahli (2,16%) :

- Pranata Humas Pertama 1 orang (0,43%)

- Pranata Humas Muda 1 orang (0,43%)
- Pranata Humas Madya 3 orang (1,29%)

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

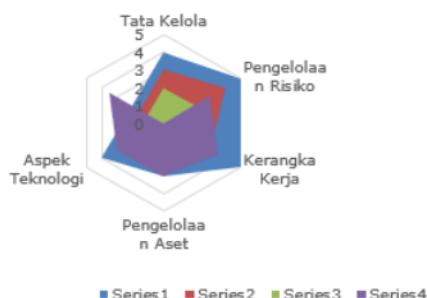
Dinas Komunikasi, Informatika, dan Statistik Provinsi Bali mengelola Sistem Elektronik dalam kategori **STRATEGIS** dengan hasil evaluasi akhir pada level **CUKUP BAIK** dengan tingkat kelengkapan penerapan standar ISO 27001 sesuai kategori pada skor nilai **546**.

Catatan:

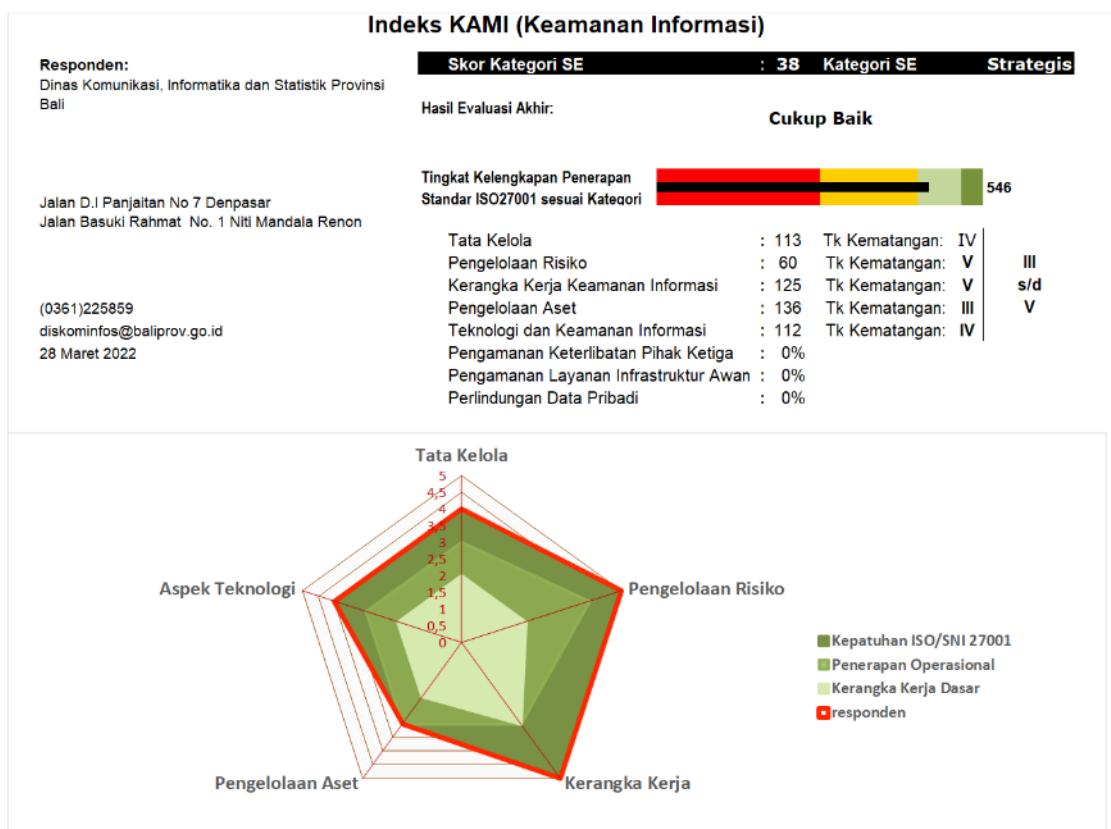
Verifikasi pada Area Suplemen tidak dilakukan karena belum tersajinya data dukung oleh pihak Diskominfos Provinsi Bali dan juga karena keterbatasan waktu verifikasi oleh Tim BSSN. Diharapkan penilaian pada Area Suplemen dapat dilakukan pada kegiatan verifikasi selanjutnya.

### **Total Score Sebelum Verifikasi: 572 (ref. File penilaian Indeks KAMI versi 4.1 Tahun 2022)**

<b>Indeks KAMI (Keamanan Informasi)</b>			
<b>Responden:</b> Dinas Komunikasi, Informatika dan Statistik Provinsi Bali	<b>Skor Kategori SE</b> : 41	<b>Kategori SE</b> Strategis	
Jalan D.I Panjaitan No 7 Denpasar	<b>Hasil Evaluasi Akhir:</b> Cukup Baik		
<b>Tingkat Kelengkapan Penerapan Standar</b>			572
Tata Kelola : 113 Tk Kematangan III Pengelolaan Risiko : 58 Tk Kematangan III+ III Kerangka Kerja Keamanan Informasi : 141 Tk Kematangan III Pengelolaan Aset : 150 Tk Kematangan III Teknologi dan Keamanan Informasi : 110 Tk Kematangan III+ Pengamanan Keterlibatan Pihak Ketiga : 100% Pengamanan Layanan Infrastruktur Aw : 100% Perlindungan Data Pribadi : 100%			
(0361)225859 diskominfos@baliprov.go.id 28 Maret 2022			



**Total Score Setelah Verifikasi: 546 (ref. file Indeks KAMI versi 4.2 pasca Verifikasi)**



## **II. ASPEK TATA KELOLA:**

### **A. Kekuatan/Kematangan**

1. Pimpinan dari Diskominfos Provinsi Bali sudah menetapkan program keamanan informasi sebagai bagian dari tanggung jawab manajemen diantaranya 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. Diskominfos Provinsi Bali sudah menetapkan fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab dalam mengelola dan mengimplementasikan program keamanan informasi dan memasukan 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 sudah dipetakan terkait pengelolaan program keamanan informasi secara lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan terhadap kontrol-kontrol keamanan yang dilaksanakan.
6. Diskominfos Provinsi Bali sudah mendefinisikan persyaratan/standar kompetensi dan keahlian khususnya terkait pelaksana pengelolaan keamanan informasi.
7. Pimpinan Diskominfos Provinsi Bali 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.
8. 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.
9. Seluruh persyaratan keamanan informasi yang terdapat dalam standard yang berlaku sudah terintegrasi kedalam proses kerja yang ada sehingga diharapkan kontrol keamanan informasi dapat berjalan secara konsisten.
10. Diskominfos Provinsi Bali sudah mengidentifikasi data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku.
11. 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.
12. Fungsi pengelola keamanan informasi sudah 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.
13. Fungsi pengelola keamanan informasi sudah secara rutin melaporkan kepada manajemen mengenai kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi harus secara rutin.
14. Setiap permasalahan keamanan informasi yang terjadi di Diskominfos Provinsi Bali sudah menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis dalam melakukan tindakan perbaikan yang diperlukan untuk meningkatkan efektifitas pelaksanaan kontrol keamanan informasi.

15. Diskominfos Provinsi Bali sudah menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya.
16. Pimpinan Diskominfos Provinsi Bali 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.
17. Target dan sasaran pengelolaan keamanan informasi sudah didefinisikan dan diformulasikan, serta dilakukan evaluasi dan mengkaji hasil pencapaianya secara rutin. Laporan hasil evaluasi terhadap target dan sasaran tersebut telah dilaporkan statusnya kepada pimpinan organisasi.
18. Pimpinan Diskominfos Provinsi Bali sudah mendelegasikan pihak terkait / unit kerja / fungsi pengelola keamanan inforamsi pada internal Diskominfos Provinsi Bali untuk mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi serta dipastikan untuk dipatuhi dengan menganalisa tingkat kepatuhannya.

## **B. Kelemahan/Kekurangan**

1. Pelaksana pengamanan informasi yang terlibat di Diskominfos Provinsi Bali belum semuanya memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku khususnya terkait aspek kontrol teknis dan operasional keamanan informasi.
2. Diskominfos Provinsi Bali 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. Metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi (misal: mekanisme, waktu pengukuran, pelaksananya) sudah didefinisikan namun belum dijabarkan secara lengkap. Sudah ada evaluasi pemantauannya perlu dilakukan namun belum diukur efektifitasnya dan tidak ada eskalasi pelaporan kepada manajemen untuk memastikan efektifitas dari proses pengelolaan program dan kontrol keamanan informasi yang diterapkan.
4. Diskominfos Provinsi Bali belum seluruhnya telah mendefinsikan mengenai kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata).

## **III. ASPEK RISIKO:**

### **A. Kekuatan/Kematangan**

1. Program kerja pengelolaan risiko keamanan informasi sudah terdokumentasi dan diterapkan secara memadai dalam proses penilaian dan evaluasi risiko.
2. Pimpinan Diskominfos Provinsi Bali sudah menentukan penanggung jawab proses manajemen risiko yang berwenang dalam eskalasi terhadap pelaporan hasil analisa risiko keamanan informasi sampai ke tingkat pimpinan organisasi.
3. Kerangka kerja pengelolaan risiko keamanan informasi sudah terdokumentasi dalam dokumen metodologi manajemen risiko sehingga dapat digunakan secara resmi.
4. Kerangka kerja pengelolaan risiko ini sudah mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian di Diskominfos Provinsi Bali.
5. Ambang batas tingkat risiko yang dapat diterima sudah ditetapkan oleh manajemen Diskominfos Provinsi Bali dalam rangka melakukan evaluasi terhadap tingkatan risiko yang dianalisa.
6. Dalam proses pengelolaan manajemen risiko, Diskominfos Provinsi Bali sudah terdapat pendefinisian mengenai kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut.
7. Ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi.
8. Pada proses analisa risiko sudah ditetapkan mengenai dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sesuai dengan definisi yang ada.
9. Diskominfos Provinsi Bali sudah 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).
10. Langkah-langkah mitigasi dan penanggulangan risiko yang ada sudah disusun secara sistematis dan memadai.
11. Langkah mitigasi risiko sudah disusun sesuai dengan tingkat prioritas dan target penyelesaiannya serta penanggungjawabnya dan telah terdapat mekanisme untuk memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK.

## B. Kelemahan/Kekurangan

1. Status penyelesaian langkah mitigasi risiko sudah diidentifikasi namun belum konsisten dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya.

2. Proses evaluasi yang obyektif/terukur terhadap penyelesaian langkah mitigasi yang telah diterapkan belum sepenuhnya mempertimbangkan konsistensi dan efektifitasnya.
3. Profil risiko berikut bentuk mitigasinya sudah dikaji ulang dalam rangka memastikan akurasi dan validitasnya namun tidak rutin terlaksana.
4. Kerangka kerja pengelolaan risiko sudah direncanakan untuk dikaji namun belum secara berkala dilakukan untuk memastikan/meningkatkan efektifitasnya.
5. Pengelolaan risiko sudah disusun namun belum sepenuhnya menjadi acuan dalam penentuan kriteria proses penilaian obyektif kinerja efektifitas 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, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya.
3. Sudah diformalkan mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya.
4. Sudah adanya proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga.
5. Kebijakan dan prosedur keamanan informasi yang sudah ditetapkan sudah merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyektif tertentu yang telah ditetapkan.
6. Sudah adanya proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan.
7. Kontrak dengan pihak ketiga sudah 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.
8. Konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan pada seluruh pegawai dan pihak ketiga.

9. Sudah adanya tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi dari kondisi ini.
10. Diskominfos Provinsi Bali sudah menetapkan dan menerapkan kebijakan dan prosedur operasional terkait implementasi security patch, alokasi tanggung jawab untuk memonitor adanya rilis security patch baru, hingga pelaporannya.
11. Aspek keamanan informasi sudah diperhatikan dalam proses manajemen proyek yang terkait dengan ruang lingkup.
12. Proses pengembangan sistem yang aman (Secure SDLC) sudah menerapkan prinsip atau metode sesuai standar platform teknologi yang digunakan.
13. Seluruh kebijakan dan prosedur keamanan informasi sudah dievaluasi kelayakannya secara berkala.
14. Strategi penerapan keamanan informasi sudah dirumuskan dan ditetapkan sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi.
15. Strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko sudah ditetapkan secara resmi.
16. Strategi penerapan keamanan informasi sudah direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi.
17. Diskominfos Provinsi Bali sudah 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).
18. Audit internal yang dilakukan tersebut sudah mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi.
19. Hasil audit internal tersebut sudah dikaji/dievaluasi terkait langkah pemberian dan pencegahan yang diperlukan, ataupun inisiatif peningkatan kinerja keamanan informasi.
20. Hasil audit internal sudah dilaporkan kepada pimpinan organisasi sehingga telah secara memadai ditetapkan langkah-langkah perbaikan atau program peningkatan kinerja keamanan informasi.
21. Rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) sudah direalisasikan secara konsisten.

## B. Kelemahan/Kekurangan

1. Evaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul sudah dilakukan namun prosesnya belum dilakukan secara berkala.

2. Ketika terdapat penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, Diskominfos Provinsi Bali belum memiliki proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya.
3. Kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mencakup persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya belum disusun dan didokumentasikan.
4. Perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) belum ditentukan mengenai komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk.
5. Uji coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) belum dilakukan sesuai jadwal.
6. 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.
7. Keperluan untuk merevisi kebijakan dan prosedur yang berlaku sudah dijalankan, namun belum semuanya mengacu kepada analisa lainnya seperti menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya.
8. Diskominfos Provinsi Bali sudah melakukan proses untuk menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk namun langkah pemberian yang diperlukan belum diterapkan secara efektif.

## **V. ASPEK PENGELOLAAN ASET:**

### **A. Kekuatan/Kematangan**

1. Telah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi sudah didokumentasikan secara lengkap, akurat dan terpelihara (termasuk kepemilikan aset ).
2. Definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku sudah didefinisikan.
3. Proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Diskominfos Provinsi Bali dan keperluan pengamanannya sudah didefinisikan dan ditetapkan secara resmi.

4. Sudah adanya proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi).
5. Sudah tersedianya proses pengelolaan konfigurasi yang diterapkan secara konsisten.
6. Beberapa penerapan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko sudah tersedia. Hal ini seperti:
  - a. Sudah adanya definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Diskominfos Provinsi Bali
  - b. Sudah adanya tata tertib penggunaan komputer, email, internet dan intranet.
  - c. Sudah ditetapkannya tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI.
  - d. Telah ada aturan terkait instalasi piranti lunak di aset TI milik Diskominfos Provinsi Bali.
  - e. Telah ada proses mengenai pengelolaan identitas elektronik dan proses otentikasi (*username & password*) termasuk kebijakan terhadap pelanggarannya.
  - f. Sudah ditetapkannya persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi
  - g. Telah ada ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data.
  - h. Sudah ada ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya.
  - i. Sudah tersedianya proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi.
  - j. Sudah berjalannya proses pengecekan latar belakang SDM.
  - k. Sudah ada mekanisme terkait pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.
  - l. Telah ada prosedur penghancuran data/aset yang sudah tidak diperlukan.
  - m. Sudah tersedianya prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya (*user access rights*) berikut langkah pemberhanan apabila terjadi ketidaksesuaian (*non-conformity*) terhadap kebijakan yang berlaku.
  - n. Telah ada ketentuan dan prosedur untuk user yang mutasi/keluar atau tenaga kontrak/outsource yang habis masa kerjanya.
7. Sudah 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 sudah ditetapkan dan didokumentasikan.

9. Beberapa kekuatan dalam pengamanan fisik antara lain:
10. 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.
11. Sudah formalnya proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik.
12. Infrastruktur komputasi telah terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya.
13. Infrastruktur komputasi yang terpasang telah terlindungi dari gangguan pasokan listrik atau dampak dari petir.
14. Sudah ditetapkannya peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor).
15. Sudah ditetapkannya proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris).
16. Konstruksi ruang penyimpanan perangkat pengolah informasi penting sebagian 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.
17. Sudah ada mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga.

## B. Kelemahan/Kekurangan

1. Definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut sudah diidentifikasi namun belum semua akses dan pengguna yang didokumentasikan.
2. Sudah ditetapkannya proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi namun belum mencakup keseluruhan sistem dan tidak semua terdokumentasi.
3. Beberapa penerapan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko belum tersedia. Hal ini seperti:
  - a. Belum diatur mengenai penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi.
  - b. Belum adanya ketentuan mengenai pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya.

- c. Telah ada prosedur mengenai proses *back-up* namun belum diatur mekanisme uji coba pengembalian data (*restore*).
- 4. Daftar data/informasi yang harus di-backup dan laporan analisa kepatuhan terhadap prosedur backup-nya belum didokumentasikan.
- 5. Belum adanya proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting.
- 6. 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).
- 7. Belum adanya proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Diskominfos Provinsi Bali.

## **VI. ASPEK TEKNOLOGI:**

### **A. Kekuatan/Kematangan**

- 1. Jaringan komunikasi sudah disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll).
- 2. Analisa kepatuhan penerapan konfigurasi standar yang ada sudah dianalisa secara berkala.
- 3. Keseluruhan infrastruktur jaringan, sistem dan aplikasi sudah dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada.
- 4. Setiap perubahan dalam sistem informasi sebagian sudah direkam pada suatu log pada sistem.
- 5. Upaya akses oleh yang tidak berhak sudah terekam di dalam log.
- 6. Beberapa log telah dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik) namun tidak semuanya telah dilakukan untuk keseluruhan sistem.
- 7. Diskominfos Provinsi Bali sudah menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada.
- 8. Diskominfos Provinsi Bali sudah mempunyai standar dalam menggunakan enkripsi.
- 9. Pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya sudah diterapkan.
- 10. Semua sistem dan aplikasi sudah secara otomatis menerapkan manajemen dalam penggantian password secara otomatis pada sistem, termasuk menon-

aktifkan password, mengatur kompleksitas/panjangnya dan penggunaan kembali password lama.

11. Akses yang digunakan untuk mengelola sistem (administrasi sistem) sudah menggunakan bentuk pengamanan khusus yang berlapis.
12. Sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses timeouts, lockout setelah kegagalan login, dan penarikan akses.
13. Sudah ada proses untuk menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan.
14. Sistem operasi untuk setiap perangkat desktop dan server sudah dimutakhirkan dengan versi terkini.
15. Setiap desktop dan server telah dilindungi dari penyerangan virus (malware).
16. Sudah tersimpannya rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis.
17. Sudah adanya proses pelaporan penyerangan virus/malware yang gagal-sukses yang ditindaklanjuti dan diselesaikan.
18. Keseluruhan jaringan, sistem dan aplikasi sudah tersinkronisasi waktu yang akurat, sesuai dengan standar yang ada.
19. Aplikasi yang ada telah memiliki dokumentasi mengenai spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba.
20. 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.
21. Diskominfos Provinsi Bali telah melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin.

## B. Kelemahan/Kekurangan

1. Layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi namun belum lebih dari 1 lapis pengamanan.
2. 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.
3. Semua log belum dilakukan analisa secara berkala.
4. Pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi sudah diterapkan namun belum dievaluasi berkala.

5. Jaringan, sistem dan aplikasi yang digunakan masih sebagian yang sudah dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi.
6. Infrastruktur jaringan, sistem dan aplikasi masih sebagian yang sudah dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada.

## **VII. REKOMENDASI**

Berikut hasil rekomendasi untuk perbaikan:

1. Diskominfos Provinsi Bali perlu memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity and disaster recovery plans*) dan mengalokasikan personil penangung jawab pada setiap aktivitas pemulihan.
2. Perlu dilakukan penjadwalan uji coba BCP secara berkala untuk memastikan kesiapan dan kehandalan infrastruktur dalam pemulihan yang dilakukan saat bencana tersebut terjadi. Perlu adanya pendelegasian yang jelas mengenai peran dan wewenang dalam rencana pemulihan tersebut.
3. Perlu disusun aturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi.
4. Perlu memformalkan daftar backup informasi yang diperlukan sesuai dengan tingkat kekritisan terkait kebutuhan ketersediaan atas data / informasi tersebut.
5. Perlu disusun ketentuan mengenai pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya.
6. Perlu diperketat dalam melakukan segmentasi jaringan yang ada dimana akses Tamu lebih dibatasi lagi untuk tidak dapat mengakses jaringan internal.
7. Perlu dilakukan program kegiatan formal terkait monitoring dan evaluasi keamanan aplikasi untuk mengidentifikasi potensi kerawanan (*vulnerability assessment*) yang dapat menimbulkan kerugian bagi organisasi.
8. Perlu dilakukan evaluasi dan penyesuaian terhadap beberapa kebijakan keamanan informasi yang telah dimiliki.
9. Penyusunan prosedur-prosedur terkait kebutuhan keamanan informasi dapat segera dilaksanakan dan dilegalisasi oleh pimpinan.
10. Untuk proses verifikasi selanjutnya dapat memperhatikan penggunaan drive resmi milik Diskominfos Provinsi Bali sebagai media berbagi data dan informasi yang dibutuhkan.

## VIII. PENUTUP

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

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

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

**Denpasar, 15 Juli 2022**

Kepala Bidang Persandian  
Dinas Komunikasi, Informatika, dan  
Statistik Provinsi Bali



Ditandatangani secara elektronik oleh  
**Kepala Bidang Persandian**  
**I Putu Sundika**  
NIP. 19761226 200604 1 003

I Putu Sundika, ST., MT  
19761226 200604 1 003

Sandiman Madya pada  
Direktorat Keamanan Siber dan Sandi  
Pemerintah Daerah selaku Lead Asesor:



Ditandatangani secara elektronik oleh:  
**SANDIMAN AHLI MADYA**  
**Dwi Kardono, S.Sos., M.A.**  
Pembina Utama Muda (IV/c)

Dwi Kardono, S.Sos., M.A.  
19710218 199110 1 001

Mengetahui,  
Kepala Dinas Komunikasi, Informatika, dan Statistik  
Provinsi Bali



Ditandatangani secara elektronik oleh :  
**KEPALA DINAS**  
**Gede Pramana**  
NIP. 19680531 199703 1 002

Gede Pramana, ST., MT.  
19680531 199703 1 002