

## LAMPIRAN

### Lampiran 1. Wawancara untuk Mengetahui *as-is* Penerapan Manajemen Risiko

#### SPBE di Organisasi Kominfosanti

| Narasumber                                                                                                                                                                                                                                                                                                                                                                                                                                                             | : Luh Putu Adi Ariwati, SE, M.Pd                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Jabatan                                                                                                                                                                                                                                                                                                                                                                                                                                                                | : Sekretaris Diskominfoanti Kabupaten Buleleng                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Tempat/Tanggal                                                                                                                                                                                                                                                                                                                                                                                                                                                         | : Diskominfoanti Kabupaten Buleleng/15 Desember 2023                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Pertanyaan                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Jawaban                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Terkait manajemen risiko pada area Pemkab Buleleng, saya mendapati Perbub Nomor 1 Tahun 2020 tentang Manajemen Risiko di Lingkungan Pemkab Buleleng, Apakah saat ini Lingkungan Pemkab Buleleng telah memiliki Peraturan Penerapan Manajemen Risiko SPBE yang secara khusus mengatur aspek manajemen risiko terkait dengan Sistem Pemerintahan Berbasis Elektronik (SPBE), mengingat Perbub Nomor 1 Tahun 2020 hanya membahas manajemen risiko organisasi secara umum? | Terkait manajemen risiko di Pemkab masih menyusun fungsi kedinasan saja, sementara untuk manajemen risiko SPBE itu belum disusun mengkhusus namun kedepannya akan disusun. Untuk hal tersebut, sebagai langkah awal Diskominfoanti sudah mengajukan bagaimana mekanisme audit ke inspektorat. Proses manajemen risiko rencananya akan dilakukan pada tahun 2024. Sementara untuk antisipasi kita sudah menggunakan surat edaran bagaimana rekomendasi pengembangan maupun pembangunan sebuah sistem. |
| Bagaimana penerapan manajemen risiko SPBE di lingkungan Diskominfoanti Pemkab Buleleng? Apakah telah ada kebijakan atau panduan khusus yang mengatur manajemen risiko terkait layanan                                                                                                                                                                                                                                                                                  | Secara khusus belum ada, tapi dalam menyusun manajemen risiko kita melakukan identifikasi per-bidang yang mengelolanya di bidang tatakelola dan pengendaliannya ada berupa SK Tim yang mengkaji apakah                                                                                                                                                                                                                                                                                               |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>SPBE yang dimiliki oleh Diskominfosanti?</p>                                                                                                                                                                                                                                                                                                                                                                                                                                          | <p>pengembangan aplikasinya dapat dilakukan kemudian apabila tidak sesuai dengan edaran apa saja yang timbul dari dampaknya. Jadi, Diskominfosanti akan menerima surat ajuan pengembangan aplikasi dari OPD lalu kami akan memberikan rekomendasi bagaimana suatu sistem atau aplikasi dapat dibangun dengan layak.</p> |
| <p>Apakah Diskominfosanti memiliki bagian atau divisi khusus yang bertanggung jawab dalam mengakomodir atau manajemen risiko dari layanan SPBE yang dioperasikan? Jika ya, bagaimana struktur dan fungsi dari bagian atau divisi tersebut?</p>                                                                                                                                                                                                                                           | <p>Saat ini divisi khusus belum ada, tapi tersentral di sekretariat dan dikoordinasikan ke bidang-bidang terkait (tata kelola SDM &amp; SPBE, infrastruktur, persandian, dan PLIP terkait pelayanan informasi publik)</p>                                                                                               |
| <p>Pada observasi yang saya lakukan sebelumnya saat PKL, saya mendapati tugas untuk merancang serta menyampaikan manajemen risiko SPBE ini kepada pihak inspektorat selaku pemilik fungsi pengawasan OPD di lingkup Pemkab Buleleng pada hal manajemen risiko. Akan hal tersebut, Bagaimana alur koordinasi antara Inspektorat sebagai pemilik fungsi pengawasan Organisasi Perangkat Daerah (OPD) di Lingkup Pemkab Buleleng dengan OPD terkait dalam melaksanakan manajemen risiko</p> | <p>Di inspektorat sebagai pengawas, tim audit, sampai saat ini ada tim audit TIK di inspektorat, diskominfosanti dari sisi peraturan harus dikoordinasikan disini, secara alur pengawasan dan audit bersumber dari inspektorat.</p>                                                                                     |

|                                                                                                              |  |
|--------------------------------------------------------------------------------------------------------------|--|
| <p>SPBE? Apakah sudah ada kerangka kerja atau mekanisme tertentu yang memfasilitasi koordinasi tersebut?</p> |  |
|--------------------------------------------------------------------------------------------------------------|--|



Lampiran 2. Wawancara Menentukan Selera Risiko SPBE atau sebagai Nilai Minimum untuk Matrix Risiko

Narasumber : Luh Putu Adi Ariwati, SE, M.Pd  
 Jabatan : Sekretaris Dinas  
 Instansi : Dinas Komunikasi, Informatika, Persandian dan Statistik  
 Tempat/Tanggal : Kantor DiskominfoSanti/2 Maret 2024

| NO. | PERTANYAAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | JAWABAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.  | Pada acara Ajang Komunikasi dan Sosialisasi (AKSI) SPBE tanggal 7 Juli 2020, melalui YouTube Kemenpan RB RI tentang pengisian form manajemen risiko SPBE yang disampaikan oleh Bapak Budi Triswanto. S.T., M.T. selaku Kabid Sistem Informasi dan Tata Kelola Data BSN menyampaikan bahwa IPPD perlu menetapkan selera risiko yang menjadi patokan minimum sebuah risiko entah risiko positif ataupun risiko negatif untuk ditindak lanjuti. Beliau pun sempat menyarankan IPPD agar mengambil nilai 16 sebagai angka moderat sebab nilai tersebut yang menunjukkan bahwa risiko tersebut sering terjadi dan memiliki dampak yang signifikan. Akan hal tersebut, setelah saya telusuri pada Renstra DiskominfoSanti 2023-2026 belum menyebutkan nilai minimum berapa kah pada risiko SPBE yang akan ditindak lanjuti. Untuk itu, apakah saat ini DiskominfoSanti telah menentukan nilai minimum besaran risiko yang akan ditindak lanjuti dalam melakukan manajemen risiko SPBE? | Sampai saat ini belum ada ketetapan nilai minimum berapa sebuah risiko baik positif dan negatif milik DiskominfoSanti agar dapat ditindaklanjuti/di mitigasi. Akan tetapi, melihat berdasarkan saran yang diberikan Bapak Budi Triswanto. S.T., M.T. selaku Kabid Sistem Informasi dan Tata Kelola Data BSN, maka sebagai awal atau uji coba dalam penelitian yang dilakukan peneliti terkait manajemen risiko operasional SPBE ini, Kami akan mengambil saran tersebut, yakni memilih angka 16 sebagai minimum nilai risiko positif dan negatif yang diidentifikasi. |
| 2.  | Pada draft peta rencana SPBE 2024-2028                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Terkait pedoman manajemen risiko                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |

| NO. | PERTANYAAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | JAWABAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     | <p>disebutkan bahwa kondisi Pemkab Saat ini memiliki kebijakan internal berupa Perbup Nomor 1 Tahun 2020 tentang Penerapan Manajemen Risiko di Lingkungan Pemerintah Kabupaten Buleleng dalam rangka pelaksanaan pengendalian intern yang efektif dan efisien. Kebijakan tersebut ditujukan untuk manajemen risiko terkait kemungkinan kejadian yang mengancam pencapaian tujuan dan sasaran Pemkab Buleleng. Lalu, ada pun rencana tindak yang dituju adalah agar Pemkab Buleleng menyusun dokumen pedoman manajemen risiko SPBE yang mengacu pada Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko SPBE serta melakukan Penerapan manajemen risiko sesuai pedoman manajemen risiko SPBE. Berdasarkan hal tersebut, khusus Diskominfosanti sendiri apakah telah memiliki dokumen pedoman manajemen risiko SPBE sesuai dengan Permen PAN RB Nomor 5 Tahun 2020 yang kemudian ditetapkan oleh Pemkab Buleleng?</p> | <p>SPBE tersebut saat ini di <i>follow up</i> ke PJ Pemkab Buleleng dan masih berstatus draft. Apabila draft tersebut disahkan, maka setiap IPPD akan mengikuti arahan tersebut sebagai pedoman pelaksanaan manajemen risiko SPBE. Meski demikian, manajemen risiko SPBE termasuk dalam peta rencana SPBE Pemkab Buleleng 2024-2028 yang menyatakan sejumlah rencana tindak (Halaman 90 s/d 91) dimana salah satunya menyebutkan agar setiap OPD Di Lingkungan Pemkab Buleleng mentaati dan menerapkan pedoman yang berlaku berdasarkan Permen PAN RB Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko SPBE.</p> |

**Dokumen Manajemen Risiko Diskominfosanti yang diserahkan:**

| NO. | NAMA DATA/DOKUMEN                      | TANGGAL          | KETERANGAN                                            |
|-----|----------------------------------------|------------------|-------------------------------------------------------|
| 1.  | Peta Rencana Pemkab Buleleng 2024-2028 | 3 Maret 2024     | SK Bupati Buleleng – Arsitektur dan Peta Rencana SPBE |
| 2.  | Pedoman Manajemen Risiko               | 20 Desember 2023 | Masih berstatuskan draft                              |

| NO. | NAMA DATA/DOKUMEN                                                                                                                                                                         | TANGGAL          | KETERANGAN                                                                                            |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|-------------------------------------------------------------------------------------------------------|
|     | SPBE                                                                                                                                                                                      |                  |                                                                                                       |
| 3.  | Peraturan Bupati Buleleng Nomor 1 Tahun 2020 tentang Manajemen Risiko di Lingkungan Umum Pemerintah Kabupaten Buleleng                                                                    | 20 Desember 2023 | Telah di terbitkan pada <a href="https://jdih.bulelengkab.go.id/">https://jdih.bulelengkab.go.id/</a> |
| 4.  | Surat Edaran Nomor: 400.13.53/1853/T.Kelola.Ko minfosanti/VII/2023 tentang Pedoman Penyelenggaraan Audit Teknologi Informasi dan Komunikasi (TIK) Lingkup Pemerintah Kabupaten Buleleng   | 15 Desember 2023 | Masih pada tahap usulan                                                                               |
| 5.  | Surat Pengantar Nomor: 700.1/1198/Sekr.Kominfo santi/X/2023 tentang Penyampaian Risk Register (RR) Dinas Komunikasi, Informatika, Persandian dan Statistik Kabupaten Buleleng Tahun 2023. | 15 Desember 2023 | -                                                                                                     |

Sekretaris Diskominfo santi,



**Luh Putu Adi Ariwati, SE, M.Pd**  
NIP. 198107112001121002

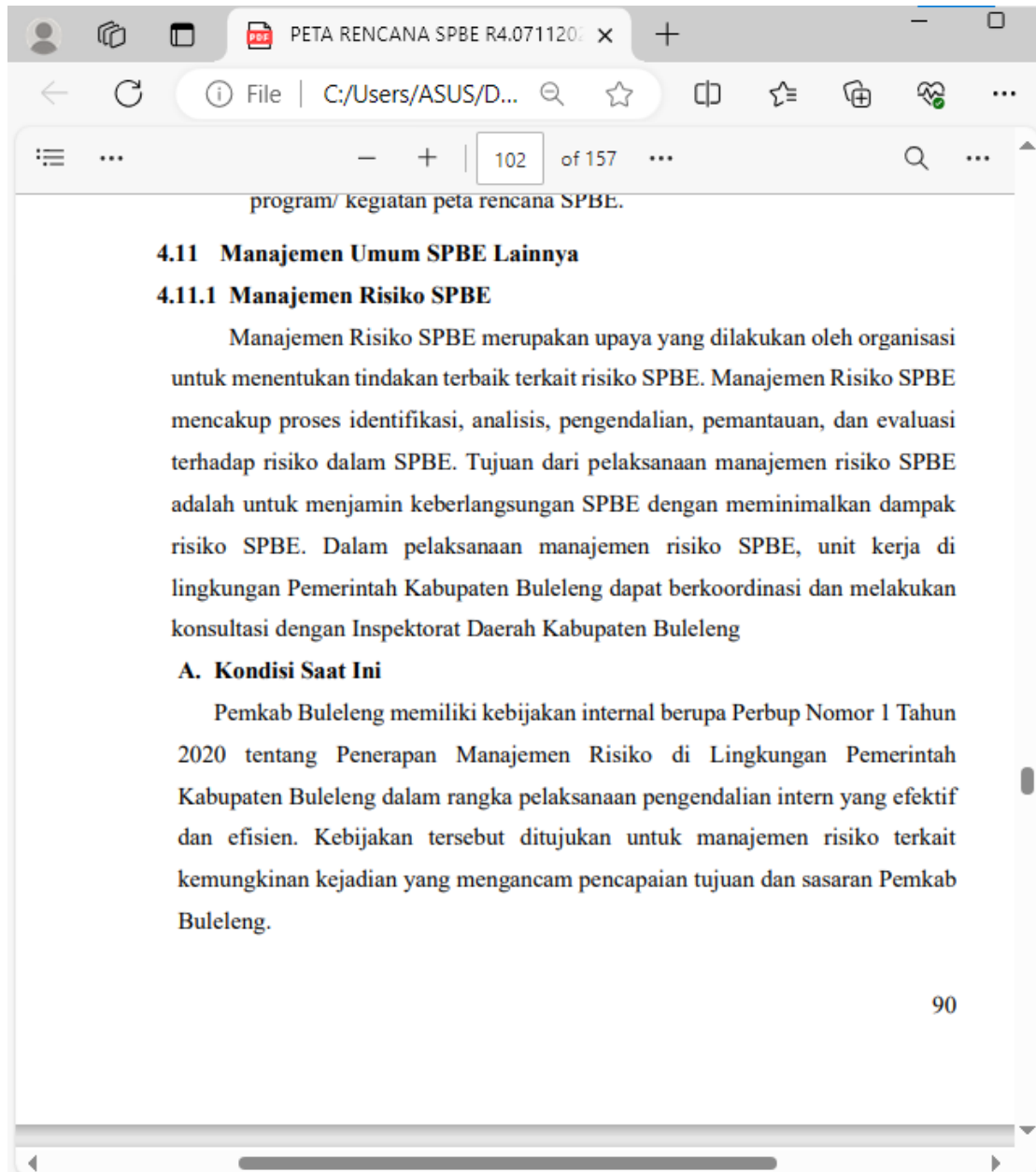
Singaraja. 13 Maret 2024

Peneliti,



**Vany Adelia Putri**

### Lampiran 3. Peta Rencana Pemkab Buleleng 2024-2028



PETA RENCANA SPBE R4.0711201 x

File | C:/Users/ASUS/D... 103 of 157

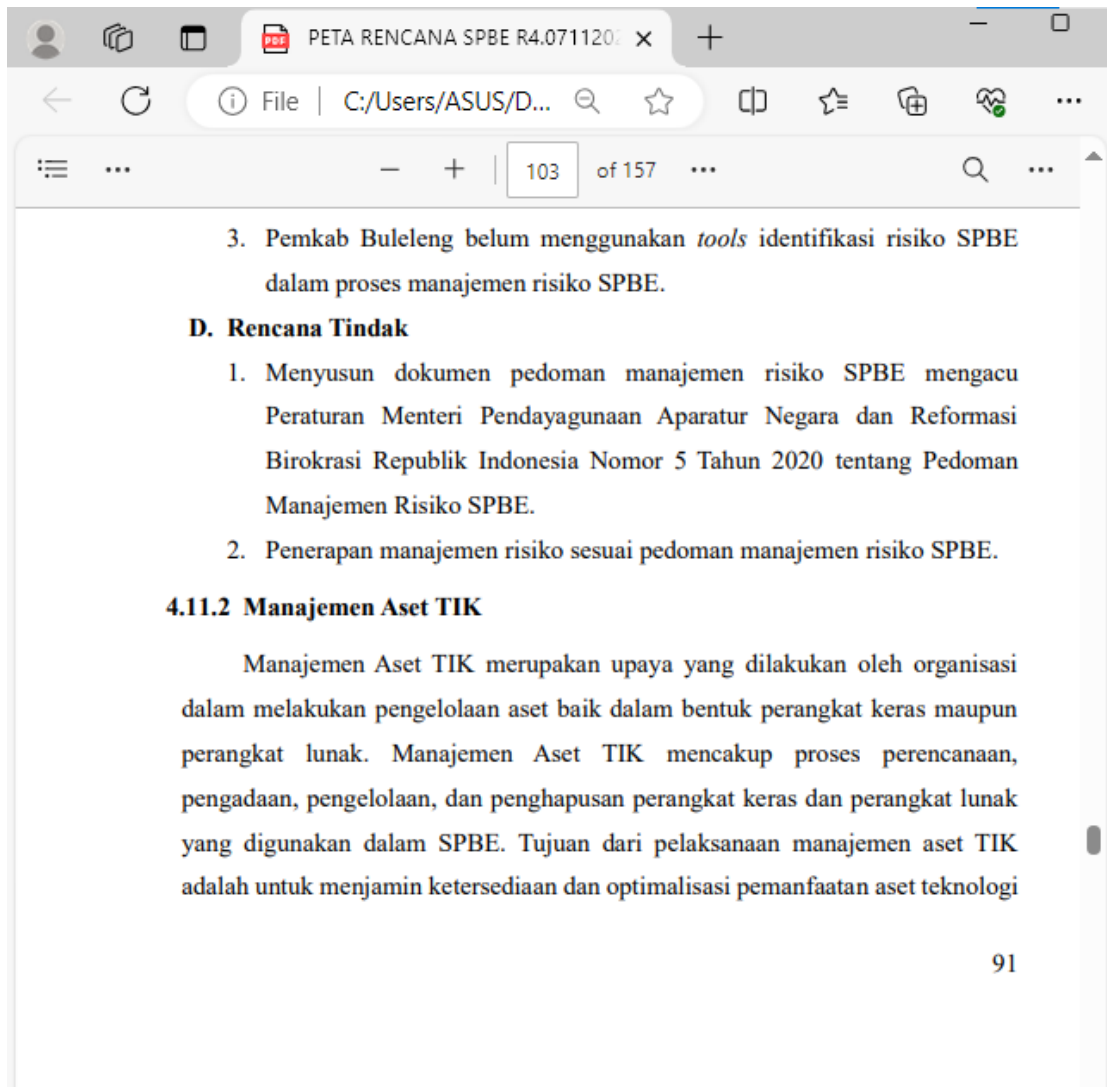
**B. Kondisi Target**

1. Pemkab Buleleng memiliki pedoman manajemen risiko SPBE mengacu Peraturan Menteri Pendayagunaan Aparatur Negara dan Reformasi Birokrasi Republik Indonesia Nomor 5 Tahun 2020 tentang Pedoman Manajemen Risiko SPBE.
2. Pemkab Buleleng memiliki program/rincian kegiatan penerapan manajemen risiko SPBE yang termuat dalam dokumen perencanaan (Peta Rencana SPBE)
3. Pemkab Buleleng menerapkan dan mendokumentasikan manajemen risiko mengacu pedoman manajemen risiko SPBE.
4. Hasil identifikasi Risiko SPBE dijadikan dasar pengendalian keamanan informasi SPBE.

**C. Analisis Gap**

1. Pemkab Buleleng belum memiliki pedoman manajemen risiko SPBE.
2. Pemkab Buleleng belum menggunakan pedoman manajemen risiko SPBE dalam proses manajemen risiko SPBE, penerapan manajemen risiko SPBE di Pemkab Buleleng tanpa program/ kegiatan yang terencana.
3. Pemkab Buleleng belum menggunakan *tools* identifikasi risiko SPBE dalam proses manajemen risiko SPBE.





Lampiran 4. Draft Pedoman Manajemen Risiko SPBE Pemkab Buleleng

Table 19

**Formulir 2.3 Struktur Pelaksana Manajemen Risiko SPBE Pemerintah Kabupaten Buleleng**

| Struktur Pelaksana Manajemen Risiko SPBE |                                                                                                                                |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Pemilik Risiko SPBE                      | Ketut Suwarmawan, S.STP., MM<br>Kepala Dinas Komunikasi dan Informatika,<br>Persandian dan Statistik Kabupaten Buleleng        |
| Koordinator Risiko SPBE                  | Luh Putu Adi Ariwati, S.E, M.Pd<br>Sekretaris Dinas Komunikasi dan Informatika,<br>Persandian dan Statistik Kabupaten Buleleng |
| Pengelola Risiko SPBE                    | Ngakan Gde Dwi Dharma Yudha, S.E., M.A.P<br>Kepala Bidang Tata Kelola dan Sumber Daya<br>Manusia SPBE                          |

## Lampiran 5. Dokumen Penyampaian Risk Register (RR) DiskominfoSanti



ပီတိရှိသော ကရင်ပြည်နယ်  
 PEMERINTAH KABUPATEN BULELENG  
 သိသောရန်ကုန်မြို့နယ်၊ ကရင်ပြည်နယ်၊ ကရင်ပြည်နယ်၊ ကရင်ပြည်နယ်  
**DINAS KOMUNIKASI, INFORMATIKA, PERSANDIAN DAN STATISTIK**  
 ကရင်ပြည်နယ်၊ ကရင်ပြည်နယ်၊ ကရင်ပြည်နယ်၊ ကရင်ပြည်နယ် (၁၀၈၈၈၈၈၈)၊ ကရင်ပြည်နယ်  
 Jl. Pahlawan No. 1 Singaraja Telp./Fax (0362) 21146  
 Web Site : [kominfosanti.bulelengkab.go.id](http://kominfosanti.bulelengkab.go.id) Email : [kominfosanti@bulelengkab.go.id](mailto:kominfosanti@bulelengkab.go.id)

---

Singaraja, 30 Oktober 2023

Kepada

Yth. Inspektur Daerah Kabupaten Buleleng

di-

Singaraja

**SURAT PENGANTAR**

Nomor : 700.1/1198/Sekr.Kominfosanti/X/2023

| NO. | URAIAN                                                                                                                       | VOLUME             | KETERANGAN                                                          |
|-----|------------------------------------------------------------------------------------------------------------------------------|--------------------|---------------------------------------------------------------------|
| 1.  | Penyampaian <i>Risk Register</i> (RR) Dinas Komunikasi, Informatika, Persandian dan Statistik Kabupaten Buleleng Tahun 2023. | 1 (Satu)<br>Gabung | Dikirim dengan hormat untuk dapat dipergunakan sebagaimana mestinya |



Ditandatangani secara elektronik oleh  
 Kepala Dinas Komunikasi,  
 Informatika, Persandian dan Statistik  
 Kabupaten Buleleng  
**Ketut Suwarnawati, SSTP., MM**  
 Pembina Tek. (13/10)  
 NIP. 1983071120061210002



Balai Sertifikasi Elektronik

Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara



|       |                                                                                            |                                                       |                                                                                                   |                 |               |                                                                                                                                                                                                                   |                        |   |                                                                                                                                                             |                                      |
|-------|--------------------------------------------------------------------------------------------|-------------------------------------------------------|---------------------------------------------------------------------------------------------------|-----------------|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------|---|-------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| 1.2   | Sasaran 3.2.2 Terwujudnya peningkatan e-government Pemkab Buleleng sesuai dengan ketentuan | Nilai Sistem Pemerintah an Berbasis Elektronik (SPBE) | Tidak dapat diaksesnya aplikasi layanan pemerintahan dan layanan publik                           | RSP.23.02.23.03 | Kepala Daerah | 1. Serangan dan gangguan dari pihak luar (hacker)<br>2. Kualitas dan kuantitas tenaga teknis belum maksimal (Tenaga programmer)<br>3. Sarana Prasarana keamanan aplikasi belum memadai (Sistem keamanan aplikasi) | Eksternal              | C | 1. Pelayanan publik terganggu<br>2. Pelayanan administrasi pemerintahan tidak maksimal                                                                      | Kepala Daerah Masyarakat OPD Terkait |
|       |                                                                                            |                                                       | Informasi publik yang disampaikan melalui Website Pemkab Buleleng tidak bisa diakses              | RSP.23.02.23.04 | Kepala Daerah | 1. Aplikasi website mengalami masalah<br>2. Server website mengalami masalah<br>3. Domain website mengalami masalah<br>4. Serangan hacker                                                                         | internal dan eksternal | C | 1. Website tidak bisa diakses di internet<br>2. Informasi yang diunggah di website tidak tersampaikan                                                       | Kepala Daerah Masyarakat OPD Terkait |
|       |                                                                                            |                                                       | Menurunnya Indeks SPBE                                                                            | RSP.23.02.23.05 | Kepala Daerah | 1. Kurangnya koordinasi dengan semua perangkat daerah terkait evaluasi SPBE<br>2. Pemahaman terkait semua indikator pertanyaan dalam kegiatan evaluasi SPBE kurang                                                | Internal               | C | 1. Menurunnya kredibilitas Pemerintah Daerah<br>2. Mempengaruhi terkait indeks penilaian lain yang terkait SPBE misal Penilaian Reformasi Birokrasi (RB)    | Kepala Daerah OPD Terkait            |
| 1.2.1 | Program Pengelolaan Aplikasi Informatika                                                   |                                                       | Terhambatnya seluruh layanan pemerintah berupa aplikasi online yang menggunakan jaringan internet | RSP.23.02.23.06 | Kepala Daerah | Kurangnya kemampuan untuk menganalisa spesifikasi kebutuhan layanan dan kurangnya jumlah personil yang memiliki kemampuan teknis untuk penanganan gangguan jaringan internet                                      | Internal               | C | 1. Gangguan jaringan yang disebabkan oleh beberapa faktor teknis tidak teratasi dengan baik<br>2. Layanan pemerintah yang bersifat online menjadi terhambat | OPD Terkait                          |

Kertas Kerja  
Identifikasi Risiko Strategis OPD

| Nama Pemda           | : Pemerintah Kabupaten Buleleng, Provinsi Bali                                                                                  |                                                       |                                                                 |                 |                           |                                                                                                                                                                                                                                            |          |        |      |                                                                                                                                                                |                                                                        |
|----------------------|---------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------|-----------------------------------------------------------------|-----------------|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------|--------|------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------|
| Nama OPD             | : Dinas Komunikasi, Informatika, Persandian dan Statistik                                                                       |                                                       |                                                                 |                 |                           |                                                                                                                                                                                                                                            |          |        |      |                                                                                                                                                                |                                                                        |
| Tahun Penilaian      | : 2023                                                                                                                          |                                                       |                                                                 |                 |                           |                                                                                                                                                                                                                                            |          |        |      |                                                                                                                                                                |                                                                        |
| Periode yang dinilai | : Periode Renstra (Tahun 2019-2023)                                                                                             |                                                       |                                                                 |                 |                           |                                                                                                                                                                                                                                            |          |        |      |                                                                                                                                                                |                                                                        |
| Tujuan Strategis     | : Meningkatnya layanan pemerintahan dibidang komunikasi, informatika, persandian serta statistik yang efektif dan efisien       |                                                       |                                                                 |                 |                           |                                                                                                                                                                                                                                            |          |        |      |                                                                                                                                                                |                                                                        |
| Urusan Pemerintahan  | : Urusan Wajib Bukan Pelayanan Dasar                                                                                            |                                                       |                                                                 |                 |                           |                                                                                                                                                                                                                                            |          |        |      |                                                                                                                                                                |                                                                        |
| No                   | Tujuan/Sasaran Strategis                                                                                                        | Indikator Kinerja                                     | Risiko                                                          |                 |                           | Sebab                                                                                                                                                                                                                                      |          |        | CIUC | Dampak                                                                                                                                                         |                                                                        |
| a                    | b                                                                                                                               | c                                                     | Uraian                                                          | Kode Risiko     | Pemilik                   | Uraian                                                                                                                                                                                                                                     | Sumber   | Uraian |      | Pihak yang Terkena                                                                                                                                             |                                                                        |
|                      |                                                                                                                                 |                                                       | d                                                               | e               | f                         | g                                                                                                                                                                                                                                          | h        | i      |      | j                                                                                                                                                              | k                                                                      |
| 1                    | Tujuan: Meningkatnya layanan pemerintahan dibidang komunikasi, informatika, persandian serta statistik yang efektif dan efisien |                                                       |                                                                 |                 |                           |                                                                                                                                                                                                                                            |          |        |      |                                                                                                                                                                |                                                                        |
|                      | Sasaran Strategis OPD: Terwujudnya peningkatan pelayanan kebutuhan data sektoral sesuai standar                                 | Persentase pemenuhan data sektoral Pemkab Buleleng    | Terhambatnya penginputan data dari produsen                     | RSO.23.02.23.01 | Kepala Dinas Kominfosanti | 1. Terlambatnya pengumpulan data oleh produsen data/OPD karena sering kalinya ada pergantian personil.<br>2. Tingkat kompetensi tenaga ASN dan Non ASN yang tidak berlatar belakang stastisi<br>3. Kurangnya fasilitas perangkat yang ada. | Internal | C      |      | 1. Data diolah dan dirilis/atau dipublikasikan menjadi terlambat<br>2. Publikasi menjadi biasa tidak bervariasi<br>3. Pengolahan menjadi lambat dan terkendala | Diskominfoasanti, Pmpinan Pengguna data, OPD Pengguur data, masyarakat |
|                      | Program: Penyelenggaraan Statistik Sektoral                                                                                     |                                                       |                                                                 |                 |                           |                                                                                                                                                                                                                                            |          |        |      |                                                                                                                                                                |                                                                        |
|                      | Sasaran Strategis OPD : Terwujudnya pengamanan informasi sesuai standar                                                         | Persentase keamanan data dan informasi sesuai standar | Pengelolaan keamanan data dan informasi belum memenuhi standar  | RSO.23.02.23.02 | KepalaDinas Kominfosanti  | Kesadaran terhadap keamanan informasi siber masih rendah                                                                                                                                                                                   | Internal | UC     |      | serangan siber masih terjadi                                                                                                                                   | user                                                                   |
|                      | Program : Penyelenggaraan Persandian Untuk Pengamanan Informasi                                                                 |                                                       | Layanan VIP dengan metode persandian (jammer) sering terkendala | RSO.23.02.23.03 | KepalaDinas Kominfosanti  | Kegiatan yang melibatkan pimpinan vip menggunakan mic wirelles, wifi dan akses internet                                                                                                                                                    | Internal | C      |      | kegiatan terganggu dan terkendala                                                                                                                              | Pimpinan, pemilik kegiatan                                             |
|                      |                                                                                                                                 |                                                       | Layanan insiden siber sistem informasi belum maksimal           | RSO.23.02.23.04 | Kepala Dinas Kominfosanti | Kegiatan insiden siber berupa deface, malware, virus, dll masih belum memiliki sdm sendiri yang cukup, dan harus kolaborasi dengan bidang lain                                                                                             | internal | C      |      | penanganan insiden terkesan lambat                                                                                                                             | OPD, pimpinan Dinas Kominfosanti                                       |
|                      |                                                                                                                                 |                                                       | Layanan Jaringan Radio Komunikasi masih belum maksimal          | RSO.23.02.23.05 | Kepala Dinas Kominfosanti | Repeater yang diperlukan kurang/rusak berat                                                                                                                                                                                                | internal | C      |      | tidak maksimalnya ketersediaan jaringan frekuensi radio komunikasi di wilayah kab buleleng                                                                     | user, pimpinan                                                         |

|  |  |  |                                                                                                    |                 |               |                                                                                         |          |   |                                                                                                                                                                     |             |
|--|--|--|----------------------------------------------------------------------------------------------------|-----------------|---------------|-----------------------------------------------------------------------------------------|----------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
|  |  |  | Terhambatnya akses layanan aplikasi pemerintahan yang menggunakan domain atau subdomain pemerintah | RSP.23.02.23.07 | Kepala Daerah | Kurangnya tenaga teknis yang dapat melaksanakan jasa pengelolaan nama domain/ subdomain | Internal | C | 1. Pengajuan subdomain dari OPD terkait tidak dapat dikonfigurasi<br>2. Domain/subdomain milik pemerintah yang terhubung dengan aplikasi online tidak dapat diakses | OPD Terkait |
|--|--|--|----------------------------------------------------------------------------------------------------|-----------------|---------------|-----------------------------------------------------------------------------------------|----------|---|---------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|

Keterangan:

Kolom a diisi dengan nomor urut

Kolom b diisi dengan tujuan strategis urusan wajib sebagai mana tercantum dalam RPJMD/Renstra

Kolom c diisi dengan indikator kinerja tujuan strategis

Kolom d diisi dengan uraian peristiwa yang merupakan risiko

Kolom e diisi dengan Kode risiko

Kolom f diisi dengan Penilik risiko, pihak/ unit yang bertanggung jawab/ berkepentingan untuk mengelola risiko

Kolom g diisi dengan penyebab timbulnya risiko. Untuk mempermudah identifikasi sebab risiko, sebab risiko bisa dikategorikan ke dalam : *Man, Money, Method, Machine* , dan *Material*

Kolom h diisi dengan sumber risiko (eksternal/internal)

Kolom i diisi dengan C, jika unit kerja mampu untuk mengendalikan penyebab risiko, atau UC jika unit kerja tidak mampu mengendalikan risiko

Kolom j diisi dengan uraian akibat yang ditimbulkan jika risiko benar-benar terjadi. Untuk mempermudah identifikasi dampak risiko, dampak risiko bisa dikategorikan ke dalam: Keuangan, Kinerja, Reputasi dan Hukum

Kolom k diisi dengan pihak/ unit yang menderita/terkena dampak jika risiko benar-benar terjadi



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

Kolom f diisi dengan Kode risiko

Kolom g diisi dengan Penilik risiko, pihak/ unit yang bertanggung jawab/ berkepentingan untuk mengelola risiko

Kolom h diisi dengan penyebab timbulnya risiko, Untuk mempermudah identifikasi sebab risiko, sebab risiko bisa dikategorikan ke dalam : *Man, Money, Method, Machine*, dan Material

Kolom i diisi dengan sumber risiko (eksternal/internal)

Kolom j diisi dengan C, jika unit kerja mampu untuk mengendalikan penyebab risiko, atau UC jika unit kerja tidak mampu mengendalikan penyebab risiko

Kolom k diisi dengan uraian akibat yang ditimbulkan jika risiko benar-benar terjadi. Untuk mempermudah identifikasi dampak risiko, dampak risiko bisa dikategorikan ke dalam: Keuangan, Kinerja, Reputasi dan Hukum

Kolom l diisi dengan pihak/ unit yang menderita/terkena dampak jika risiko benar-benar terjadi



Dokumen ditanamkan secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

Kertas Kerja  
Hasil Analisis Risiko

| Nama Pemda                                         |                                                                                                    | : Pemerintah Kabupaten Buleleng, Provinsi Bali                                                                            |                            |                                 |                            |
|----------------------------------------------------|----------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|----------------------------|---------------------------------|----------------------------|
| Tahun Penilaian                                    |                                                                                                    | : 2023                                                                                                                    |                            |                                 |                            |
| Tujuan Strategis                                   |                                                                                                    | : Meningkatkan layanan pemerintahan dibidang komunikasi, informatika, persandian serta statistik yang efektif dan efisien |                            |                                 |                            |
| Urusan Pemerintahan                                |                                                                                                    | : Urusan Wajib Bukan Pelayanan Dasar                                                                                      |                            |                                 |                            |
| No.                                                | "Risiko" yang Teridentifikasi                                                                      | Kode Risiko                                                                                                               | Analisis Risiko            |                                 |                            |
|                                                    |                                                                                                    |                                                                                                                           | Skala Dampak <sup>a)</sup> | Skala Kemungkinan <sup>b)</sup> | Skala Risiko <sup>c)</sup> |
| a                                                  | b                                                                                                  | c                                                                                                                         | d                          | e                               | f=g x h                    |
| <b>I Risiko Strategis</b>                          |                                                                                                    |                                                                                                                           |                            |                                 |                            |
| 1                                                  | Menurunnya citra pemerintah daerah di mata masyarakat                                              | RSP 23.02.23.01                                                                                                           | 4                          | 5                               | 20                         |
| 2                                                  | Informasi publik tidak tersampaikan kepada masyarakat luas                                         | RSP 23.02.23.02                                                                                                           | 4                          | 5                               | 20                         |
| 3                                                  | Tidak dapat diaksesnya aplikasi layanan pemerintahan dan layanan publik                            | RSP 23.02.23.03                                                                                                           | 5                          | 4                               | 20                         |
| 4                                                  | Informasi publik yang disampaikan melalui Website Pemkab Buleleng tidak bisa diakses               | RSP 23.02.23.04                                                                                                           | 4                          | 3                               | 12                         |
| 5                                                  | Menurunnya Indeks SPBE                                                                             | RSP 23.02.23.05                                                                                                           | 5                          | 4                               | 20                         |
| 6                                                  | Terhambatnya seluruh layanan pemerintah berupa aplikasi online yang menggunakan jaringan internet  | RSP 23.02.23.06                                                                                                           | 4                          | 4                               | 16                         |
| 7                                                  | Terhambatnya akses layanan aplikasi pemerintahan yang menggunakan domain atau subdomain pemerintah | RSP 23.02.23.07                                                                                                           | 3                          | 3                               | 9                          |
| <b>II Risiko Strategis OPD 1: Dinas Kominfo</b>    |                                                                                                    |                                                                                                                           |                            |                                 |                            |
| 1                                                  | Keterlambatan dalam pengumpulan data oleh Produsen Data/OPD                                        | RSO 23.02.23.01                                                                                                           | 3                          | 3                               | 9                          |
| 2                                                  | Pengelolaan data menjadi buku/metadana yang masih kurang                                           | RSO 23.02.23.02                                                                                                           | 3                          | 3                               | 9                          |
| 3                                                  | Penginputan data dari produsen data masih lambat                                                   | RSO 23.02.23.03                                                                                                           | 4                          | 4                               | 16                         |
| 4                                                  | Pengelolaan keamanan data dan informasi masih sedang proses standarisasi                           | RSO 23.02.23.04                                                                                                           | 3                          | 3                               | 9                          |
| 5                                                  | Layanan VIP dengan metode persandian (jammer) sering terkendala                                    | RSO 23.02.23.05                                                                                                           | 2                          | 4                               | 8                          |
| 6                                                  | Layanan insiden siber sistem informasi belum maksimal                                              | RSO 23.02.23.06                                                                                                           | 4                          | 4                               | 16                         |
| 7                                                  | Layanan Jaringan Radio Komunikasi masih belum maksimal                                             | RSO 23.02.23.07                                                                                                           | 2                          | 4                               | 8                          |
| <b>III Risiko Operasional OPD 1: Dinas Kominfo</b> |                                                                                                    |                                                                                                                           |                            |                                 |                            |
| 1                                                  | Keterlambatan pengumpulan data dari produsen/OPD                                                   | ROO 23.02.23.01                                                                                                           | 3                          | 3                               | 9                          |
| 2                                                  | Terkendalanya pengolahan data akibat data yang tidak tersedia sesuai jadwal                        | ROO 23.02.23.02                                                                                                           | 3                          | 3                               | 9                          |
| 3                                                  | Penyusunan tidak bisa dilaksanakan sesuai jadwal karena data belum diolah                          | ROO 23.02.23.03                                                                                                           | 3                          | 3                               | 9                          |
| 4                                                  | Terlambatnya pencetakan dan penyebaran dokumen data sektoral                                       | ROO 23.02.23.04                                                                                                           | 4                          | 4                               | 16                         |
| 5                                                  | Dasar dari literasi yang harus jelas, tidak sebatas mitos                                          | ROO 23.02.23.05                                                                                                           | 3                          | 3                               | 9                          |
| 6                                                  | Literasi kurang menarik                                                                            | ROO 23.02.23.06                                                                                                           | 3                          | 3                               | 9                          |
| 7                                                  | Literasi sulit untuk dipahami                                                                      | ROO 23.02.23.07                                                                                                           | 4                          | 4                               | 16                         |

Keterangan:

Kolom a diisi dengan nomor urut

Kolom b diisi dengan risiko yang teridentifikasi sesuai lampiran 6a dan 6b

Kolom c diisi dengan kode risiko sesuai lampiran 6a dan 6b

Kolom d diisi dengan skala dampak berdasarkan perhitungan rata-rata / modus skala dampak yang diberikan peserta diskusi

Kolom e diisi dengan skala kemungkinan berdasarkan perhitungan rata-rata / modus skala kemungkinan yang diberikan peserta diskusi

Kolom f diisi dengan hasil perkalian antara skala dampak dan skala kemungkinan



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh  
Badan Sertifikasi Elektronik, Badan Siber dan Sandi Negara

| Kertas Kerja<br>Daftar Risiko Prioritas                                  |                                                                                                   |                                                                                                                                                                                                                               |              |                      |                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                        |
|--------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Nama Pemda<br>Tahun Penilaian<br>Tujuan Strategis<br>Usuran Pemerintahan |                                                                                                   | : Pemerintah Kabupaten Buleleng, Provinsi Bali<br>: 2023<br>: Meningkatnya layanan pemerintahan dibidang komunikasi, informatika, persandian serta statistik yang efektif dan efisien<br>: Usuran Wajib Bukan Pelayanan Dasar |              |                      |                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                        |
| No                                                                       | Risiko Prioritas                                                                                  | Kode Risiko                                                                                                                                                                                                                   | Skala Risiko | Pemilik Risiko       | Penyebab                                                                                                                                                                                                          | Dampak                                                                                                                                                                                                                                                 |
| a                                                                        | b                                                                                                 | c                                                                                                                                                                                                                             | d            | e                    | f                                                                                                                                                                                                                 | g                                                                                                                                                                                                                                                      |
| <b>I Risiko Strategis</b>                                                |                                                                                                   |                                                                                                                                                                                                                               |              |                      |                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                        |
| 1                                                                        | Menurunnya citra pemerintah daerah di mata masyarakat                                             | RSP.23.02.23.01                                                                                                                                                                                                               | 20           | Kepala Daerah        | Kurangnya pemberitaan baik rilis maupun postingan di media resmi Pemkab Buleleng                                                                                                                                  | 1. Kurangnya Rilis positif di website resmi Pemkab Buleleng<br>2. Kurangnya postingan positif (citra Pemkab) di Media Sosial resmi Pemkab Buleleng<br>3. Kurangnya penyebaran rilis/berita ke media eksternal yang bekerja sama dengan Pemkab Buleleng |
| 2                                                                        | Informasi publik tidak tersampaikan kepada masyarakat luas                                        | RSP.23.02.23.02                                                                                                                                                                                                               | 20           | Kepala Daerah        | Sarana prasarana serta media untuk penyebarluasan informasi belum memadai                                                                                                                                         | 1. Kurang masifnya penyebaran informasi publik ke masyarakat<br>2. Penyebaran informasi publik harus menyesuaikan dengan kultur budaya, usia penerima informasi dan beragamnya platform media yang ada                                                 |
| 3                                                                        | Tidak dapat diaksesnya aplikasi layanan pemerintahan dan layanan publik                           | RSP.23.02.23.03                                                                                                                                                                                                               | 20           | Kepala Daerah        | 1. Serangan dan gangguan dari pihak luar (hacker)<br>2. Kualitas dan kuantitas tenaga teknis belum maksimal (Tenaga programmer)<br>3. Sarana Prasarana keamanan aplikasi belum memadai (Sistem keamanan aplikasi) | 1. Pelayanan publik terganggu<br>2. Pelayanan administrasi pemerintahan tidak maksimal                                                                                                                                                                 |
| 4                                                                        | Informasi publik yang disampaikan melalui Website Pemkab Buleleng tidak bisa diakses              | RSP.23.02.23.04                                                                                                                                                                                                               | 12           | Kepala Daerah        | 1. Aplikasi website mengalami masalah<br>2. Server website mengalami masalah<br>3. Domain website mengalami masalah<br>4. Serangan hacker                                                                         | 1. Website tidak bisa diakses di internet<br>2. Informasi yang diunggah di website tidak tersampaikan                                                                                                                                                  |
| 5                                                                        | Menurunnya Indeks SPBE                                                                            | RSP.23.02.23.05                                                                                                                                                                                                               | 20           | Kepala Daerah        | 1. Kurangnya koordinasi dengan semua perangkat daerah terkait evaluasi SPBE<br>2. Pemahaman terkait semua indikator pertanyaan dalam kegiatan evaluasi SPBE kurang                                                | 1. Menurunnya kredibilitas Pemerintah Daerah<br>2. Mempengaruhi terkait indeks penilaian lain yang terkait SPBE misal Penilaian Reformasi Birokrasi (RB)                                                                                               |
| 6                                                                        | Terhambatnya seluruh layanan pemerintah berupa aplikasi online yang menggunakan jaringan internet | RSP.23.02.23.06                                                                                                                                                                                                               | 16           | Kepala Daerah        | Kurangnya kemampuan untuk menganalisa spesifikasi kebutuhan layanan dan kurangnya jumlah personil yang memiliki kemampuan teknis untuk penanganan gangguan jaringan internet                                      | 1. Gangguan jaringan yang disebabkan oleh beberapa faktor teknis tidak teratasi dengan baik<br>2. Layanan pemerintah yang bersifat online menjadi terhambat                                                                                            |
| <b>II Risiko Strategis OPD 1</b>                                         |                                                                                                   |                                                                                                                                                                                                                               |              |                      |                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                        |
| 1                                                                        | Penginputan data dari produsen data masih lambat                                                  | RSO.23.02.23.03                                                                                                                                                                                                               | 16           | Kepala Dinas Kominfo | Masih Kurangnya Fasilitas Perangkat yang ada                                                                                                                                                                      | Pengolahan menjadi lambat dan terkendala                                                                                                                                                                                                               |
| 2                                                                        | Layanan insiden siber sistem informasi belum maksimal                                             | RSO.23.02.23.06                                                                                                                                                                                                               | 16           | Kepala Dinas Kominfo | Kegiatan insiden siber berupa deface, malware, virus, dll masih belum memiliki sdm sendiri yang cukup, dan harus kolaborasi dengan bidang lain                                                                    | penanganan insiden terkesan lambat                                                                                                                                                                                                                     |
| <b>III Risiko Operasional OPD 1: Dinas Kesehatan</b>                     |                                                                                                   |                                                                                                                                                                                                                               |              |                      |                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                        |
| 1                                                                        | Terlambatnya pencetakan dan penyebarluasan dokumen data sektoral                                  | ROO.23.02.23.04                                                                                                                                                                                                               | 16           | Kepala Dinas Kominfo | Akibat terlambatnya proses pengumpulan, pengolahan dan penyusunan data                                                                                                                                            | Penerbitan dan penyebarluasan dokumen data statistik tidak tepat waktu                                                                                                                                                                                 |
| 2                                                                        | Literasi sulit untuk dipahami                                                                     | ROO.23.02.23.07                                                                                                                                                                                                               | 16           | Kepala Dinas Kominfo | Literasi menggunakan bahasa yang awam                                                                                                                                                                             | Rendahnya tingkat keamanan sesuai standar                                                                                                                                                                                                              |

Keterangan  
 Kolom a diisi dengan nomor urut  
 Kolom b diisi dengan risiko prioritas  
 Kolom c diisi dengan kode risiko  
 Kolom d diisi dengan skala risiko (sesuai lampiran 7)  
 Kolom e diisi dengan pemilik risiko sesuai Lampiran 6a dan 6b  
 Kolom f diisi dengan penyebab sesuai Lampiran 6a dan 6b  
 Kolom g diisi dengan dampak sesuai dengan Lampiran 6a dan 6b



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

Penilaian atas Kegiatan Pengendalian yang Ada dan Masih Dibutuhkan  
(RTP atas Hasil Identifikasi Risiko)

| Nama Pemda Tahun Penilaian                   |                                                                                                   | : Pemerintah Kabupaten Buleleng, Provinsi Bali : 2023                                                                     |                                                                                                                                                                                                                         |                                                                                                                                                                              |                                                                                                                                                           |                           |                           |
|----------------------------------------------|---------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------|---------------------------|
| Tujuan Strategis                             |                                                                                                   | : Meningkatkan layanan pemerintahan dibidang komunikasi, informatika, persandian serta statistik yang efektif dan efisien |                                                                                                                                                                                                                         |                                                                                                                                                                              |                                                                                                                                                           |                           |                           |
| Urusan Pemerintahan                          |                                                                                                   | : Urusan Wajib Bukan Pelayanan Dasar                                                                                      |                                                                                                                                                                                                                         |                                                                                                                                                                              |                                                                                                                                                           |                           |                           |
| No                                           | Risiko Prioritas                                                                                  | Kode Risiko                                                                                                               | Uraian Pengendalian yang Sudah Ada *)                                                                                                                                                                                   | Celah Pengendalian                                                                                                                                                           | Rencana Tindak Pengendalian                                                                                                                               | Pemilik/ Penanggung Jawab | Target Waktu Penyelesaian |
| a                                            | b                                                                                                 | c                                                                                                                         | d                                                                                                                                                                                                                       | e                                                                                                                                                                            | f                                                                                                                                                         | g                         | h                         |
| <b>I. Risiko Strategis</b>                   |                                                                                                   |                                                                                                                           |                                                                                                                                                                                                                         |                                                                                                                                                                              |                                                                                                                                                           |                           |                           |
| 1                                            | Menurunnya citra pemerintah daerah di mata masyarakat                                             | RSP 23.02 23.01                                                                                                           | Menyampaikan berita/risiko positif tentang Pemkab Buleleng                                                                                                                                                              | Sulitnya mendeteksi postingan yang kontra dengan pemerintah di media sosial                                                                                                  | Melakukan pemantauan terhadap grup yang ada di media sosial kemudian mengonfirmasi apabila ada postingan yang bernilai negatif terhadap pemerintah daerah | Kepala Daerah             | Tn Wulan IV 2023          |
| 2                                            | Informasi publik tidak tersampaikan kepada masyarakat luas                                        | RSP 23.02 23.02                                                                                                           | Menyebarkan informasi kepada masyarakat luas melalui berbagai media yang populer di masyarakat, seperti media sosial                                                                                                    | Informasi yang tersampaikan terkadang di sebarluaskan dengan narasi yang menyimpang oleh pihak yang tidak bertanggungjawab                                                   | Informasi disampaikan hanya melalui akun-akun media sosial resmi Pemkab Buleleng                                                                          | Kepala Daerah             | Tn Wulan IV 2023          |
| 3                                            | Tidak dapat diaksesnya aplikasi layanan pemerintahan dan layanan publik                           | RSP 23.02 23.03                                                                                                           | Melakukan pengecekan dan maintenance terhadap aplikasi yang mengalami kendala                                                                                                                                           | Masih lemahnya sarana pengamanan aplikasi dan kurangnya tenaga SDM yang memadai                                                                                              | Mengusulkan pengadaan sarana pengamanan aplikasi dan peningkatan kualitas SDM                                                                             | Kepala Daerah             | Tn Wulan IV 2023          |
| 4                                            | Informasi publik yang disampaikan melalui Website Pemkab Buleleng tidak bisa diakses              | RSP 23.02 23.04                                                                                                           | Monitoring website secara berkala                                                                                                                                                                                       | Kurangnya tenaga teknis yang dapat melaksanakan jasa pengelolaan nama domain/ subdomain                                                                                      | Melakukan pembinaan dan monitoring pengelolaan website secara berkala                                                                                     | Kepala Daerah             | Tn Wulan IV 2023          |
| 5                                            | Menurunnya Indeks SPBE                                                                            | RSP 23.02 23.05                                                                                                           | 1. Melaksanakan koordinasi dengan perangkat daerah terkait dengan evaluasi SPBE<br>2. Meningkatkan pemahaman terhadap SK Men PAN/ RB No. 962 Tahun 2021 Tentang Pedoman Teknis Pelaksanaan Pemantauan dan Evaluasi SPBE | Kurangnya SDM pada internal Dinas Kominfo untuk membantu pengumpulan data terkait evaluasi SPBE                                                                              | Rekrutmen tenaga baru maupun lebih mengoptimalkan SDM yang ada                                                                                            | Kepala Daerah             | Tn Wulan IV 2023          |
| 6                                            | Terhambatnya seluruh layanan pemerintah berupa aplikasi online yang menggunakan jaringan internet | RSP 23.02 23.06                                                                                                           | Menyediakan Back up internet, melakukan monitoring secara berkala                                                                                                                                                       | Kurangnya kemampuan untuk menganalisa spesifikasi kebutuhan layanan dan kurangnya jumlah personil yang memiliki kemampuan teknis untuk penanganan gangguan jaringan internet | Melakukan rekrutmen tenaga ahli dan melakukan pelatihan teknis tenaga jaringan                                                                            | Kepala Daerah             | Tn Wulan III 2023         |
| <b>II. Risiko Strategis Dinas Kominfo</b>    |                                                                                                   |                                                                                                                           |                                                                                                                                                                                                                         |                                                                                                                                                                              |                                                                                                                                                           |                           |                           |
| 1                                            | Pengumpulan data dari produsen data masih lambat                                                  | RSO 23.02 23.03                                                                                                           | Pemintaan data kepada produsen melalui link excel spreadsheet                                                                                                                                                           | link excel spreadsheet dapat diakses oleh semua orang                                                                                                                        | Memberikan hak akses hanya kepada pemilik link akses excel spreadsheet                                                                                    | Kepala Dinas Kominfo      | Tn Wulan III 2023         |
| 2                                            | Layanan insiden siber sistem informasi belum maksimal                                             | RSO 23.02 23.06                                                                                                           | Melakukan pengecekan terhadap sistem/perangkat yang terkena insiden bersama tenaga ahli/programmer                                                                                                                      | Masih kurangnya tenaga SDM yang dapat menangani insiden siber                                                                                                                | Melakukan koordinasi dan pelaporan ke BSSN RI                                                                                                             | Kepala Dinas Kominfo      | Tn Wulan II 2023          |
| <b>III. Risiko Operasional Dinas Kominfo</b> |                                                                                                   |                                                                                                                           |                                                                                                                                                                                                                         |                                                                                                                                                                              |                                                                                                                                                           |                           |                           |
| 1                                            | Terlambatnya pencetakan dan penyebarluasan dokumen data sektoral                                  | ROO 23.0 2.23.04                                                                                                          | Pemintaan data kepada produsen melalui link excel spreadsheet                                                                                                                                                           | link excel spreadsheet dapat diakses oleh semua orang                                                                                                                        | Memberikan hak akses hanya kepada pemilik link akses excel spreadsheet                                                                                    | Kepala Dinas Kominfo      | Tn Wulan III 2023         |
| 2                                            | Literasi sulit untuk dipahami                                                                     | ROO 23.0 2.23.07                                                                                                          | Memperbanyak sumber-sumber bahan literasi                                                                                                                                                                               | Literasi yang disampaikan dengan bahasa yang masih sulit dipahami dan dengan konsep jargon sehingga kurang menarik                                                           | Membuat literasi yang lebih menarik dan mudah dimengerti dengan menggunakan video dan animasi                                                             | Kepala Dinas Kominfo      | Tn Wulan III 2023         |

Keterangan  
Kolom a diisi dengan nomor urut  
Kolom b diisi dengan risiko prioritas  
Kolom c diisi dengan kode risiko  
Kolom d diisi dengan uraian pengendalian-pengendalian yang sudah ada/ terpasang. Agar diungkap tidak hanya nama SOP nya, Contoh SOP Pemeliharaan Gedung dibersihkan 2 kali sehari.  
Kolom e diisi dengan alasan tidak efektif  
(1) Kebijakan dan Prosedur pengendalian sudah dilakukan, namun belum mampu menangani risiko yang teridentifikasi,  
(2) Prosedur pengendalian belum/ tidak dapat dilaksanakan,  
(3) Kebijakan belum diikuti dengan prosedur baku yang jelas,  
(4) Kebijakan dan prosedur yang ada tidak sesuai dengan peraturan dasarnya  
Kolom f diisi dengan pengendalian yang masih dibutuhkan  
Kolom g diisi dengan pihak/ unit penanggung jawab untuk menyalenggarakan kegiatan pengendalian  
Kolom h diisi dengan target waktu penyelesaian RTP



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Badan Sertifikasi Elektronik, Badan Siber dan Sandi Negara

CONTOH  
PENCATATAN KEJADIAN RISIKO (RISK EVENT) DAN PELAKSANAAN RTP

| Nama Pemda                 |                                                                                                   |                 | : Pemerintah Kabupaten Buleleng, Provinsi Bali                                                                         |                                              |                                                     |                                                        |                                                                                                                                                                |                         |                           |                                                     |
|----------------------------|---------------------------------------------------------------------------------------------------|-----------------|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------|-----------------------------------------------------|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------|---------------------------|-----------------------------------------------------|
| Tahun Penilaian            |                                                                                                   |                 | : 2023                                                                                                                 |                                              |                                                     |                                                        |                                                                                                                                                                |                         |                           |                                                     |
| Tujuan Strategis           |                                                                                                   |                 | : Meningkatkan layanan pemerintahan dibidang komunikasi, informatika, persandian serta statistik yang efektif dan efis |                                              |                                                     |                                                        |                                                                                                                                                                |                         |                           |                                                     |
| Urusan Pemerintahan        |                                                                                                   |                 | : Urusan Wajib Bukan Pelayanan Dasar                                                                                   |                                              |                                                     |                                                        |                                                                                                                                                                |                         |                           |                                                     |
| No                         | "Risiko" yang Teridentifikasi                                                                     | Kode Risiko     | Kejadian Risiko                                                                                                        |                                              |                                                     | Keterangan                                             | RTP                                                                                                                                                            | Rencana Pelaksanaan RTP | Realisasi Pelaksanaan RTP | Keterangan                                          |
|                            |                                                                                                   |                 | Tanggal terjadi                                                                                                        | Sebab                                        | Dampak                                              |                                                        |                                                                                                                                                                |                         |                           |                                                     |
| II Risiko Strategis Pemda  |                                                                                                   |                 |                                                                                                                        |                                              |                                                     |                                                        |                                                                                                                                                                |                         |                           |                                                     |
| 1                          | Menurunnya citra pemerintah daerah di mata masyarakat                                             | RSP.23.02.23.01 | Tidak Terjadi                                                                                                          | Tidak Terjadi                                | Tidak Terjadi                                       | Tidak Terjadi                                          | Telah dilaksanakannya pengelodaan komunikasi publik resmi Pemkab Buleleng secara berkelanjutan                                                                 | Triwulan IV             | Oct-23                    | Telah dilaksanak efektifitas RTP belum dapat diukur |
| 2                          | Informasi publik tidak tersampaikan kepada masyarakat luas                                        | RSP.23.02.23.02 | Tidak Terjadi                                                                                                          | Tidak Terjadi                                | Tidak Terjadi                                       | Tidak Terjadi                                          | Telah dilaksanakannya penyebaran informasi secara berkelanjutan melalui semua kanal/media resmi milik Pemkab Buleleng, baik secara konvensional maupun digital | Triwulan IV             | Nov-23                    | Telah dilaksanak efektifitas RTP belum dapat diukur |
| 3                          | Tidak dapat diaksesnya aplikasi layanan pemerintahan dan layanan publik                           | RSP.23.02.23.03 | Tidak Terjadi                                                                                                          | Tidak Terjadi                                | Tidak Terjadi                                       | Tidak Terjadi                                          | Monitoring aplikasi                                                                                                                                            | 12 bulan                | Januari s/d Desember 2023 | Telah dilaksanak efektifitas RTP belum dapat diukur |
| 4                          | Informasi publik yang disampaikan melalui Website Pemkab Buleleng tidak bisa diakses              | RSP.23.02.23.04 | Tidak Terjadi                                                                                                          | Tidak Terjadi                                | Tidak Terjadi                                       | Tidak Terjadi                                          | Monitoring website Resmi Pemkab Buleleng                                                                                                                       | Triwulan 2              | April                     | Telah dilaksanak dan ditindaklanj                   |
| 5                          | Menurunnya Indeks SPBE                                                                            | RSP.23.02.23.05 | tidak terjadi                                                                                                          | Tidak Terjadi                                | Tidak Terjadi                                       | Tidak Terjadi                                          | Penyusunan arsitektur dan peta rencana SPBE di tahun 2023                                                                                                      | Triwulan III            | Juli 2023                 | Telah dilaksanak efektifitas RTP belum dapat diukur |
| 6                          | Terhambatnya seluruh layanan pemerintah berupa aplikasi online yang menggunakan jaringan internet | RSP.23.02.23.06 | 3-Oct-23                                                                                                               | Adanya gangguan jalur internet dari Penyedia | Jaringan internet mengalami kendala di seluruh SKPD | Terhambatnya layanan pemerintah berupa aplikasi online | Kontrding dan konfigurasi backup internet secara berkala                                                                                                       | Triwulan IV             | Oct-23                    | Telah dilaksanak dan ditindaklanj                   |
| III Risiko Strategis Dinas |                                                                                                   |                 |                                                                                                                        |                                              |                                                     |                                                        |                                                                                                                                                                |                         |                           |                                                     |

|                                     |                                                              |                 |               |               |               |               |                                                                                                 |               |                   |                                        |
|-------------------------------------|--------------------------------------------------------------|-----------------|---------------|---------------|---------------|---------------|-------------------------------------------------------------------------------------------------|---------------|-------------------|----------------------------------------|
| 1                                   | Penginputan data dan produsen data masih lambat              | RSO.23.02.23.03 | Tidak Terjadi | Tidak Terjadi | Tidak Terjadi | Tidak Terjadi | Mengadakan verifikasi validasi dan sekaligus pematapan penginputan ke aplikasi Portal Satu Data | Triwulan IV   | 18 September 2023 | Telah dilaksanakan dan ditindaklanjuti |
| 2                                   | Layanan insiden siber sistem informasi belum maksimal        | RSO.23.02.23.06 | Tidak Terjadi | Tidak Terjadi | Tidak Terjadi | Tidak Terjadi | Melaksanakan monitoring Keamanan Siber ke seluruh OPD                                           | Triwulan II   | Maret - Juli 2023 | Telah dilaksanakan dan ditindaklanjuti |
| <b>III Risiko Operasional Dinas</b> |                                                              |                 |               |               |               |               |                                                                                                 |               |                   |                                        |
| 1                                   | Terlambatnya pencetakan dan penyebaran dokumen data sektoral | ROO.23.02.23.04 | Tidak Terjadi | Tidak Terjadi | Tidak Terjadi | Tidak Terjadi | Proses Penyusunan Buku sudah selesai                                                            | Triwulan IV   | Nov-23            | Proses tindaklanjuti                   |
| 2                                   | Literasi sulit untuk dipahami                                | ROO.23.02.23.07 | Tidak Terjadi | Tidak Terjadi | Tidak Terjadi | Tidak Terjadi | Terus berupaya dengan literasi masif dan terus-menerus, dengan desain yang mudah dipahami       | Setiap Minggu | 2023              | Telah dilaksanakan dan ditindaklanjuti |

**Keterangan**

Kolom a diisi dengan nomor urut

Kolom b diisi dengan risiko yang teridentifikasi

Kolom c diisi dengan kode risiko

Kolom d diisi dengan tanggal terjadinya risiko pada tahun berjalan

Kolom e diisi dengan penyebab peristiwa risiko saat terjadi pada tahun berjalan

Kolom f diisi dengan dampak peristiwa risiko pada tahun berjalan

Kolom g diisi dengan keterangan tambahan



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara



## Lampiran 6. Pedoman Penyelenggaraan Audit TIK Lingkup Pemkab Buleleng



### PEMERINTAH KABUPATEN BULELENG DINAS KOMUNIKASI, INFORMATIKA, PERSANDIAN DAN STATISTIK

Jl. Pahlawan No. 1 Singaraja Fax./Telp. 21146  
Web Site: [www.bulelengkab.go.id](http://www.bulelengkab.go.id) E-Mail: [kominfosanti@bulelengkab.go.id](mailto:kominfosanti@bulelengkab.go.id)

Nomor : 180/1307/T.Kelola.Kominfosanti/XI/2023

Singaraja, 29 November 2023

Lampiran : -

Kepada

Perihal : **Regulasi Audit TIK**

Yth. Inspektur Kabupaten Buleleng  
di –

**Singaraja**

Menindaklanjuti instruksi Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE) dan Peraturan Bupati Buleleng Nomor 58 Tahun 2019 tentang Tata Kelola Sistem Pemerintahan Berbasis Elektronik, maka kami lampirkan kembali Surat Edaran Sekretaris Daerah Buleleng Nomor: 400.13.53/1853 /T.Kelola.Kominfosanti/VII/2023 Tanggal 07 Juli 2023 tentang Pedoman Penyelenggaraan Audit Teknologi Informasi dan Komunikasi (TIK) Lingkup Pemerintah Kabupaten Buleleng (*terlampir*).

Mencermati hal tersebut di atas dapat sekiranya untuk menjadi pertimbangan untuk dapat ditindaklanjuti menjadi regulasi berupa Peraturan Kepala Daerah (Perbup) ataupun Perda sesuai kewenangan pengawasan di bidang TIK. Apabila memungkinkan dapat sekiranya diteruskan menjadi usulan peraturan ke Bagian Hukum Setda untuk pengusulan penyusunan peraturan di tahun 2024.

Demikian yang disampaikan agar mendapat perhatian dan pertimbangan tindak lanjut. Atas pertimbangannya disampaikan terima kasih.



**Tembusan**, disampaikan kepada Yth. :

1. PJ. Bupati Buleleng, sebagai laporan;
2. Sekda Kab. Buleleng, sebagai laporan;
3. Plt. Asisten Administrasi Umum, sebagai laporan;
4. Arsip.



Balai  
Sertifikasi  
Elektronik

Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

LAMPIRAN SURAT SEKRETARIS DAERAH  
KABUPATEN BULELENG  
NOMOR 400.13.53/1853/T.Kelola.Kominfo/VII/2023  
TENTANG  
PEDOMAN PENYELENGGARAAN AUDIT TEKNOLOGI  
INFORMASI DAN KOMUNIKASI (TIK) LINGKUP  
PEMERINTAH KABUPATEN BULELENG

TAHAPAN PENYELENGGARAAN AUDIT TEKNOLOGI INFORMASI DAN KOMUNIKASI  
(TIK) LINGKUP PEMERINTAH KABUPATEN BULELENG

BAB I  
STANDAR PELAKSANAAN AUDIT SPBE

Standar pelaksanaan Audit TIK adalah Batasan minimal bagi regulator dan auditor untuk membantu pelaksanaan audit sesuai prosedur dalam rangka pencapaian tujuan audit.

Standar Pelaksanaan Audit TIK memiliki tujuan sebagai berikut:

- a. Menetapkan prinsip-prinsip dasar bagi pelaksanaan Audit TIK;
- b. Menyusun Kerangka Kerja dalam pemberian layanan jasa Audit TIK, guna menambah nilai kepada yang diaudit (Auditee) melalui perbaikan proses dan operasionalnya; dan
- c. Menyusun dasar dalam melakukan evaluasi terhadap regulasi dan pelaksanaan Audit TIK guna mendorong rencana perbaikan.

Standar Pelaksanaan Audit TIK mencakup hal-hal sebagai berikut:

1.1 Standar Umum;

- a. Standar Umum memberikan prinsip dasar untuk mengatur Auditor TIK dalam melaksanakan tugasnya dan sehingga pelaksanaan pekerjaan Audit TIK hingga pelaporannya dapat terlaksana dengan baik dan efektif.
- b. Dalam rangka memastikan kehandalan dan keamanan sistem teknologi informasi dan komunikasi di lingkungan Pemerintah Kabupaten Buleleng perlu dilakukan audit TIK secara berkala dan berkelanjutan
- c. Objek Audit TIK tersebut terdiri dari :
  1. Infrastruktur SPBE yang terdiri dari Pusat Data, Jaringan Intra Pemerintah Kabupaten Buleleng dan Sistem Penghubung Layanan Pemerintah Kabupaten Buleleng;



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

2. Aplikasi SPBE Pemerintah Kabupaten Buleleng, yang merupakan aplikasi khusus yang dikembangkan, dikelola dan/atau digunakan oleh Perangkat Daerah guna mendukung uraian tugas pokok dan fungsi serta memenuhi kebutuhan khusus Perangkat Daerah; dan
  3. Keamanan infrastruktur dan keamanan aplikasi SPBE Pemerintah Kabupaten Buleleng yang terkait pada poin a dan b diatas.
- d. Lingkup cakupan Audit TIK yang dilaksanakan meliputi pemeriksaan hal pokok teknis pada setiap objek audit yaitu :
1. penerapan tata kelola dan manajemen teknologi informasi dan komunikasi;
  2. fungsionalitas teknologi informasi dan komunikasi;
  3. kinerja teknologi informasi dan komunikasi yang dihasilkan; dan
  4. aspek teknologi informasi dan komunikasi lainnya.
- e. Permintaan Audit TIK diajukan untuk satu atau lebih dari tujuan berikut ini:
1. Peningkatan kinerja birokrasi dan pelayanan publik;
  2. Penilaian kesesuaian dengan standar/prosedur/pedoman dan kesesuaian dengan rencana/kebutuhan/kondisi;
  3. Identifikasi status teknologi yang dimiliki, identifikasi kemampuan teknologi, termasuk dalam hal ini adalah inventarisasi dan pemetaan aset teknologi;
  4. Perencanaan pengembangan sistem/teknologi dan perencanaan perbaikan kelemahan; dan/atau
  5. Pengungkapan suatu sebab atau fakta terkait dengan suatu kejadian atau peristiwa yang biasanya berimplikasi pada kondisi yang membahayakan keselamatan atau keamanan.
- f. Audit TIK di lingkungan Pemerintah Kabupaten Buleleng terdiri atas audit Internal dan Eksternal
1. Audit eksternal TIK dilaksanakan oleh lembaga pelaksana Audit TIK pemerintah atau lembaga pelaksana Audit TIK yang terakreditasi dan auditor yang tersertifikasi sesuai dengan ketentuan peraturan perundang-undangan. Sebelum dilakukan audit eksternal TIK pada Pemerintah Kabupaten Buleleng, harus terlebih dahulu melaksanakan audit internal TIK Pemerintah Kabupaten Buleleng.
  2. Audit internal TIK dilaksanakan oleh tim auditor internal TIK Pemerintah Kabupaten Buleleng yang mempunyai kompetensi teknis sesuai objek audit dan lingkup audit dan ditetapkan oleh Sekretaris Daerah selaku Koordinator SPBE Pemerintah Kabupaten Buleleng. Audit internal TIK dapat dilakukan dengan bantuan tenaga ahli audit TIK yang tersertifikasi atau lembaga audit TIK yang terakreditasi, dengan :



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

- 1) memastikan bahwa tenaga ahli yang digunakan mempunyai kompetensi, kualifikasi profesi, pengalaman yang relevan, dan independensi; dan
  - 2) melakukan evaluasi terhadap hasil kerja tenaga ahli yang digunakan dan menyimpulkan tingkatan ketergunaannya.
- g. Tujuan, wewenang dan tanggung jawab suatu aktivitas Audit TIK harus didefinisikan dengan jelas, tertuang dalam suatu dokumen formal berupa piagam audit (*audit charter*), surat tugas, atau dokumen-dokumen yang setara. Hal yang perlu diperhatikan sebagai berikut:
- 1) Surat tugas atau piagam audit (*audit charter*) menjelaskan tujuan audit, ruang lingkup, kewenangan tim audit dan etika yang harus dipatuhi oleh tim audit.
  - 2) Penugasan Tim Auditor TIK dalam melaksanakan Audit TIK berupa Surat Tugas yang diberikan oleh Sekretaris Daerah selaku Koordinator SPBE Pemerintah Kabupaten Buleleng dan ditembuskan kepada Dinas teknis terkait TIK dan Auditee.
  - 3) Kegiatan Audit TIK dilakukan berdasarkan uraian yang disusun di dalam surat penugasan kerja Audit TIK. Surat penugasan kerja Audit TIK berisikan antara lain:
    1. Tujuan Audit TIK;
    2. Lingkup Audit TIK;
    3. Wewenang auditor;
    4. Tanggung jawab auditor;
    5. Periode penugasan; dan
    6. Tata pelaporan hasil Audit TIK.
- h. Integritas Auditor TIK diwujudkan melalui sikap independen, objektif, dan menjaga kerahasiaan. Dalam melaksanakan tugasnya, Auditor TIK dituntut untuk menjalankan hal-hal sebagai berikut:
- 1) Menggunakan keahlian profesionalnya dengan cermat dan seksama (*due professional care*) serta berhati-hati (*prudent*) dalam setiap penugasan;
  - 2) Senantiasa mengasah dan melatih kecermatan profesionalnya;
  - 3) Meningkatkan pengetahuan, keahlian, dan kompetensi lain yang diperlukannya dengan mengikuti pendidikan dan pelatihan berkelanjutan;
  - 4) Mematuhi prosedur yang ditetapkan dan mematuhi aturan perundangan; dan
  - 5) Memiliki pengetahuan (*knowledge*), keterampilan (*skill*), sikap (*attitude*) dan pengalaman (*experience*) yang sesuai /guna memenuhi tanggung jawabnya dalam pelaksanaan audit.



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

### 1.2 Standar Pelaksanaan;

- a. Tim Audit TIK terdiri dari posisi-posisi dengan uraian tugas dan tanggung jawab sebagai berikut:

1. Ketua Tim Audit (*Lead Auditor*), bertanggung jawab merencanakan Audit TIK, melaksanakan Audit TIK di lapangan, mengendalikan data dan melaporkan hasil Audit TIK serta secara efektif mengelola aktivitas audit untuk menjamin agar tujuan Audit TIK tercapai.

Ketua tim audit (*Lead Auditor*) harus melakukan hal-hal sebagai berikut:

- 1) Menyusun dan menetapkan rencana audit (*audit plan*) guna menentukan prioritas-prioritas dalam kegiatan Audit TIK yang konsisten dengan tujuan audit sesuai dengan piagam audit (*audit charter*);
- 2) Menyampaikan rencana audit (*audit plan*) kepada Auditee untuk dikaji dan diberi persetujuan, serta mengkomunikasikan dampak dari keterbatasan sumberdaya;
- 3) Mengelola sumber daya audit yang tepat, memadai, dan efektif untuk melaksanakan rencana audit yang telah disetujui;
- 4) Melakukan koordinasi dengan pimpinan Lembaga Audit TIK (LATIK) untuk menjamin bahwa pelaksanaan Audit TIK dapat berjalan efektif dan efisien; dan
- 5) Memberi laporan yang memadai kepada pimpinan unit kerja yang diaudit mengenai tujuan, wewenang, tanggung jawab, dan kinerja audit.
2. Auditor, bertugas membantu *Lead Auditor* dalam aktivitas Audit TIK;
3. Asisten Auditor, bertugas membantu Auditor dalam aktivitas Audit TIK. Asisten Auditor harus sudah mengikuti sosialisasi Audit TIK;
4. Teknisi, bertugas membantu Auditor dalam pengumpulan data lapangan;
5. Pengawas Mutu, berperan melakukan monitoring dan evaluasi aktivitas Audit TIK untuk menjamin pelaksanaan Audit TIK sesuai dengan ketentuan peraturan perundang-undangan. Pengawas mutu dapat berasal dari pihak eksternal; dan
6. Narasumber, berperan memberi masukan yang berkaitan dengan isu, status industri dan teknologi, serta keilmuan yang relevan dengan lingkup yang diaudit.

Dalam pelaksanaan suatu Audit TIK, Tim Audit TIK minimal terdiri dari seorang Ketua Tim Audit (*Lead Auditor*) dan Auditor.

- b. Pemeriksaan yang dilakukan terhadap Auditee mencakup:

1. Penerapan tata kelola dan manajemen SPBE;
2. Fungsionalitas dan kinerja SPBE; dan
3. Tingkat kepatuhan terhadap regulasi.



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

- c. Hal yang perlu diperhatikan dalam Perencanaan Audit TIK sebagai berikut:
1. Auditor harus menyusun perencanaan dan program Audit TIK berdasarkan pendekatan risiko (*risk approach*). Hasil penilaian risiko digunakan untuk mengatur prioritas dan pengalokasian sumber daya audit.
  2. Dalam melakukan penilaian risiko, Audit TIK paling sedikit melakukan beberapa hal sebagai berikut:
    - 1) Mengidentifikasi aset SPBE yang berupa data, aplikasi SPBE, sistem operasi, infrastruktur SPBE, fasilitas, dan personil;
    - 2) Mengidentifikasi kegiatan dan proses bisnis yang menggunakan SPBE; dan
    - 3) Mengidentifikasi tingkat dampak risiko SPBE dalam operasional layanan SPBE dan mempertimbangkan skala prioritas berdasarkan tingkat risiko.
  3. Program Audit TIK disusun sesuai dengan cakupan Audit TIK yang sudah ditetapkan dari hasil penilaian risiko TIK. Auditor dapat mengalokasikan sumber daya yang lebih fokus pada area yang berisiko tinggi dan mempunyai skala kepentingan yang tinggi pada Layanan TIK.
  4. Rencana kerja Audit TIK harus disusun untuk setiap penugasan Audit TIK. Dalam hal merencanakan Audit TIK, Auditor harus mengembangkan dan mendokumentasikan rencana untuk setiap pelaksanaan Audit, yang paling sedikit mencakup:
    - 1) Tujuan Audit TIK, jadwal, jumlah auditor, dan pelaporan;
    - 2) Lingkup Audit TIK sesuai hasil penilaian risiko;
    - 3) Pembagian tugas dan tanggung jawab dari auditor; dan
    - 4) Alokasi sumber daya.
  5. Rencana audit (*audit plan*) disusun dengan mempertimbangkan, antara lain:
    - 1) Sistem pengendalian internal dan kepatuhan Auditee terhadap kebijakan atau standar;
    - 2) Penetapan tujuan Audit TIK;
    - 3) Penetapan kecukupan lingkup; dan
    - 4) Penggunaan metodologi yang tepat.
  6. Ketua tim audit dan Auditee harus menyepakati rencana audit sebelum tahap pelaksanaan audit.
- d. Hal yang perlu diperhatikan dalam Pelaksanaan Audit TIK sebagai berikut:
1. Proses pelaksanaan Audit TIK mengacu pada program Audit TIK yang telah disusun pada tahap perencanaan
  2. Auditor menyiapkan kertas kerja Audit TIK untuk mendokumentasikan pelaksanaan Audit TIK. Dokumen kertas kerja Audit TIK, yang sekurangnya terdiri dari:



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

- 1) Dokumen rencana dan program audit;
  - 2) Surat Tugas Tim Audit;
  - 3) Laporan Hasil Audit; dan
  - 4) Laporan Tindak Lanjut Hasil Audit.
3. Dalam hal pelaksanaan audit TIK, Auditor TIK harus mengidentifikasi, menganalisis, mengevaluasi, dan mendokumentasikan informasi yang cukup untuk mencapai tujuan audit. Dalam melaksanakan audit tersebut, Auditor TIK harus:
- 1) Memperoleh bukti-bukti audit yang cukup, handal, dan relevan untuk mendukung penilaian audit dan kesimpulan audit;
  - 2) Mendasarkan temuan dan kesimpulan audit pada analisis dan interpretasi yang memadai atas bukti-bukti audit;
  - 3) Menyiapkan, mengelola dan menyimpan data dan informasi yang diperoleh selama pelaksanaan audit; dan
  - 4) Disupervisi dengan baik untuk memastikan terjaminnya kualitas dan meningkatnya kemampuan Auditor.
4. Dalam hal komunikasi atas hasil Audit TIK, Auditor TIK harus mengkomunikasikan hasil pelaksanaan audit kepada pihak-pihak yang berkepentingan. Komunikasi tersebut harus mencakup tujuan dan ruang lingkup pelaksanaan audit, selain kesimpulan yang terkait, rekomendasi dan rencana tindak lanjut. Jika komunikasi final berisi kesalahan atau penghilangan yang signifikan, ketua tim audit (*Lead Auditor*) harus mengkomunikasikan informasi yang telah diperbaiki kepada semua pihak yang menerima komunikasi.
- e. Monitoring dan evaluasi dilakukan oleh pengawas mutu dalam rangka memberikan informasi atas aktivitas audit yang sedang berjalan yang bertujuan untuk mengidentifikasi kemajuan dalam pelaksanaan audit, serta memastikan audit diimplementasikan secara efektif. Pengawas mutu menyampaikan hasil monitoring dan evaluasi aktivitas audit kepada Walikota dan koordinator SPBE.
- f. Evaluasi secara menyeluruh dilakukan setelah aktivitas audit selesai yang bertujuan untuk mengetahui kelebihan dan kekurangan aktivitas audit yang telah dilakukan dalam rangka meningkatkan kualitas pelaksanaan audit berikutnya.
- g. Aspek monitoring dalam aktivitas Audit TIK meliputi:
1. Kepatuhan terhadap Kode Etik dan Standar Audit;
  2. Kesesuaian terhadap Piagam Audit;
  3. Kesesuaian terhadap Rencana Audit; dan
  4. Kesesuaian terhadap Protokol Audit



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

### 1.3 Standar Pelaporan

- a. Laporan audit disampaikan oleh ketua Tim audit kepada Auditee dan pimpinan Aparat pengawasan Intern Pemerintah (APIP) untuk memutuskan apakah kesimpulan hasil pemeriksaan, termasuk temuan yang diperoleh selama Audit TIK berlangsung, serta rekomendasi yang diberikan dapat diterima oleh Auditee.
- b. Hal yang diperhatikan dalam pelaporan audit sebagai berikut:
  1. Laporan hasil audit dibuat dalam bentuk dokumen laporan audit dengan tepat waktu, lengkap, akurat, objektif, meyakinkan, jelas, dan ringkas;
  2. Auditor dapat meminta tanggapan atau pendapat terhadap temuan, kesimpulan dan rekomendasi yang diberikannya termasuk tindakan perbaikan yang direncanakan oleh auditee secara tertulis dari pejabat auditee yang bertanggung jawab;
  3. Setelah konfirmasi dilakukan, Tim Audit wajib menyampaikan laporan hasil audit yang berisikan antara lain:
    - 1) Tujuan Audit TIK;
    - 2) Lingkup Audit TIK;
    - 3) Periode pelaksanaan Audit TIK;
    - 4) Kriteria dan acuan Audit TIK;
    - 5) Metoda pengumpulan data dan metode analisa;
    - 6) Hasil analisis, kesimpulan, dan rekomendasi;
    - 7) Tanggapan Auditee terhadap hasil Audit TIK;
    - 8) Batasan dan kendala yang ditemui selama proses Audit TIK; dan
    - 9) Tata cara pendistribusian laporan sesuai dengan surat penugasan.
  4. Draft laporan diriviu oleh ketua tim audit untuk memastikan konsistensi dengan tujuan dan ruang lingkup audit.
  5. Laporan Audit diterbitkan dan dibuat rangkap dengan memberi identifikasi (nomor dokumen) untuk masing-masing salinan asli. Pada setiap halaman dokumen laporan hasil audit diberi identifikasi (nomor dokumen) yang menggambarkan sekurang kurangnya: tahun pelaksanaan audit, nomor urut atau nomor seri dokumen, domain Aplikasi atau Infrastruktur SPBE, Auditee dan kode pengendalian distribusi salinan dokumen.
  6. Laporan Audit didistribusikan kepada Bupati.
  7. Laporan Periodik yang berisi ringkasan hasil audit disampaikan oleh Bupati kepada Instansi Pemerintah Pusat, paling sedikit satu kali dalam 2 tahun.



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

#### 1.4 Standar Tindak Lanjut.

- a. Dalam kondisi pemantauan terhadap tindak lanjut akan dilaksanakan, ketua tim audit (*Lead Auditor*) harus menetapkan sebuah sistem pemantauan terhadap tindak lanjut temuan, kesimpulan dan rekomendasi audit oleh Auditee, mencakup cara berkomunikasi dengan Auditee, prosedur pemantauan, dan laporan status temuan.
- b. Untuk menjamin pelaksanaan tindak lanjut hasil audit TIK, APIP melakukan:
  1. pemantauan tindak lanjut hasil audit TIK;
  2. koordinasi dengan Koordinator SPBE, Dinas teknis terkait TIK, Auditee dan pihak terkait lainnya untuk mendorong penyelesaian Tindak Lanjut Hasil Audit;
  3. Tindak lanjut perbaikan dari Auditee perlu dievaluasi oleh auditor, untuk menilai apakah saran tindak lanjut yang diberikan dapat diimplementasikan dan memberikan manfaat bagi Auditee;
  4. APIP dan Auditee harus memelihara dokumentasi atas hasil tindak lanjut tersebut.

## BAB II

### PANDUAN TEKNIS AUDIT TIK

#### 2.1 Tata Cara Pelaksanaan Audit

Pelaksanaan Audit SPBE terbagi dalam tiga kelompok tahapan, yaitu:

- a. tahap Perencanaan (*Pre – Audit*);
- b. tahap Pelaksanaan Lapangan (*onsite audit*); dan
- c. tahap Analisa data dan pelaporan (*post audit*).

Tata laksana dalam tiga tahapan diatas sebagai berikut:

1. Penyiapan tim pelaksana meliputi penetapan personil tim audit.
2. *Quick Assessment* dilakukan untuk mengenali obyek audit dengan mengidentifikasi isu terkini (*current issue*), lokasi organisasi yang diaudit, struktur organisasi dari organisasi yang diaudit, proses bisnis dari organisasi, atau bagian yang diaudit, teknologi produk (bila relevan), teknologi proses (bila relevan), pengguna produk (bila relevan).
3. Penyiapan protocol audit  
 Penyiapan protocol audit dimulai dengan komunikasi dengan auditee untuk menjelaskan secara garis besar tentang audit TIK. Tim auditor menindaklanjuti dengan menyusun protokol audit yang berisi detail instrumen audit, meliputi tujuan, lingkup, kriteria, acuan, metode pengumpulan data, metoda Analisa, perkiraan jadwal pelaksanaan, Daftar data,



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

pertanyaan dan pengujian, Formulir untuk mencatat data, jawaban, hasil observasi dan hasil pengujian.

4. Penyepakatan protocol audit.

Komunikasi lanjutan dengan auditee dilakukan untuk menyepakati protocol yang disusun. Auditee dapat memberi masukan untuk memperbaiki protocol dan menunjuk personil di pihak auditee yang akan mendampingi auditor dalam pelaksanaan lapangan. Dokumen protocol ditandatangani oleh penanggung jawab tim auditor dan penanggung jawab tim auditee.

5. Penyiapan kertas kerja dan penyiapan *audit tools*

Setelah protocol audit disepakati, tim auditor menyiapkan secara rinci form-form yang diperlukan. Form tersebut dianggap sebagai kerja kerja formal dalam pengumpulan data.

6. Melakukan pertemuan pembukaan dengan auditee

Pelaksanaan lapangan diawasi dengan pertemuan pembukaan yang memaparkan rincian pelaksanaan lapangan audit aplikasi TIK dengan diawali dengan tata cara pelaksanaan audit melalui.

7. Melaksanakan audit lapangan, melalui:

- 1) Penelaahan dokumen;
- 2) Wawancara;
- 3) Observasi lapangan;
- 4) Pengujian; dan
- 5) Verifikasi bukti. Auditor dapat meminta data atau informasi guna keperluan pelaksanaan tugas, baik dalam bentuk salinan cetak maupun salinan lunak termasuk basis data dari Aplikasi SPBE

8. Melakukan analisis bukti;

9. Memberikan rekomendasi perbaikan untuk mengatasi temuan audit TIK. Temuan Audit TIK merupakan keadaan dimana fakta status penyelenggaraan SPBE Auditee tidak sesuai dengan ketentuan peraturan perundang-undangan serta standar penyelenggaraan SPBE.

10. Melakukan pertemuan penutupan dengan auditee;

11. Penyusunan laporan;

12. Proof-read laporan (memeriksa kembali laporan hasil audit);

13. Penyerahan laporan; dan

14. Evaluasi aktivitas



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

## 2.2 Pedoman Teknis Audit Infrastruktur SPBE

- a. Audit TIK Infrastruktur SPBE dengan obyek pusat data, jaringan intra dan sistem penghubung layanan, dilakukan pada aspek:
  1. Tata kelola infrastruktur SPBE, yang meliputi evaluasi, pengarahan, dan pemantauan;
  2. Manajemen Infrastruktur SPBE, yang meliputi
    - 1) Manajemen keamanan,
    - 2) Manajemen risiko,
    - 3) Manajemen asset,
    - 4) Manajemen pengetahuan,
    - 5) Manajemen sumber daya manusia (SDM),
    - 6) Manajemen layanan,
    - 7) Manajemen perubahan; dan
    - 8) Manajemen data.
- b. Fungsionalitas dan kinerja operasional dan pemeliharaan Infrastruktur SPBE, yang meliputi perencanaan, pengembangan, pengoperasian, dan pemeliharaan infrastruktur SPBE; dan
- c. Tingkat kepatuhan terhadap regulasi.
- b. Auditor melakukan pemeriksaan terhadap Infrastruktur SPBE untuk memastikan bahwa:
  1. Perubahan teknologi, ketentuan hukum, dan regulasi dipantau;
  2. Strategi Infrastruktur SPBE dan rencana Infrastruktur SPBE sudah selaras dengan kebutuhan Perangkat Daerah;
  3. Standar teknologi sudah ditetapkan dan diimplementasikan;
  4. Rekomendasi arsitektur Infrastruktur SPBE sudah dilaksanakan;
  5. Rencana pengadaan Infrastruktur SPBE sudah mempertimbangkan faktor risiko, biaya, manfaat, keamanan, dan kesesuaian teknis dengan Infrastruktur SPBE lainnya;
  6. Pengadaan Infrastruktur SPBE sesuai dengan rencana;
  7. Aset SPBE sudah diidentifikasi, ditentukan pemilik atau penanggung jawabnya, dan dicatat agar dapat dilindungi secara tepat;
  8. Penghapusan aset SPBE sudah dilakukan dengan tepat sehingga aset aman untuk dihapus dan/atau dimusnahkan;
  9. Kapasitas Infrastruktur SPBE sudah direncanakan dengan baik, dipantau, dianalisis dan dievaluasi penggunaannya;
  10. Insiden terkait Infrastruktur SPBE dicatat dan ditangani dengan baik sesuai dengan kesepakatan tingkat layanan;



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

11. Pemeliharaan Infrastruktur SPBE telah dilakukan secara reguler sesuai dengan petunjuk penggunaannya; dan
12. Setiap pegawai/petugas pengelola fasilitas, Infrastruktur SPBE harus memiliki kompetensi yang sesuai dengan bidang tugasnya.
- c. Audit dapat difokuskan pada penilaian fungsionalitas dan kinerja infrastruktur SPBE.
- d. Auditor harus melakukan pemeriksaan terhadap penyediaan layanan infrastruktur SPBE oleh pihak eksternal untuk memastikan bahwa :
  1. Pengendalian pemberian hak akses kepada pihak eksternal telah dilakukan;
  2. Pemantauan dan evaluasi layanan pihak eksternal telah ditinjau secara berkala;
  3. Evaluasi dan peninjauan layanan yang diberikan oleh pihak eksternal telah sesuai dengan pengendalian keamanan informasi yang ditetapkan dalam perjanjian atau kontrak; dan
  4. Perjanjian Kerahasiaan (*Non Disclosure Agreement*) telah ditandatangani oleh pihak eksternal.
- e. Panduan teknis dan kriteria penilaian pada audit infrastruktur SPBE dapat ditetapkan lebih lanjut oleh APIP, sesuai ketentuan peraturan perundang-undangan.

### 2.3 Pedoman Teknis Audit Aplikasi SPBE

- a. Audit Aplikasi SPBE dilakukan pada aspek:
  1. Penerapan tata kelola Aplikasi SPBE yang meliputi evaluasi, pengarahannya, dan pemantauan;
  2. Penerapan manajemen Aplikasi SPBE, yang meliputi
    - 1) Manajemen keamanan,
    - 2) Manajemen risiko,
    - 3) Manajemen asset,
    - 4) Manajemen pengetahuan,
    - 5) Manajemen sumber daya manusia,
    - 6) Manajemen layanan,
    - 7) Manajemen perubahan, dan
    - 8) Manajemen data;
  3. Fungsionalitas dan Kinerja Aplikasi SPBE yang meliputi perencanaan, pengembangan, pengoperasian, dan pemeliharaan aplikasi SPBE; dan
  4. Tingkat kepatuhan terhadap regulasi.
- b. Auditor harus melakukan pemeriksaan terhadap Arsitektur Aplikasi SPBE paling sedikit untuk memastikan bahwa:



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

1. Aplikasi direncanakan dalam suatu dokumen spesifikasi kemampuan aplikasi (*Software Requirements Specifications*) dengan mengacu kepada arsitektur SPBE Nasional, arsitektur SPBE Pemerintah Kabupaten Buleleng, dengan mempertimbangkan kebutuhan, peluang dan proses bisnis
  2. Perubahan kebutuhan dan proses bisnis dipantau;
  3. Standar pembangunan dan pengembangan Aplikasi SPBE sudah ditetapkan dan diimplementasikan;
  4. Rekomendasi arsitektur Aplikasi SPBE sudah dilaksanakan.
  5. Aplikasi SPBE sudah dibangun dan dikembangkan sesuai rencana dengan metodologi pembangunan dan pengembangan yang ada;
  6. Rancangan Aplikasi SPBE sudah mempertimbangkan kebutuhan keamanan dan ketersediaan;
  7. Aplikasi SPBE memiliki dokumentasi pembangunan dan pengembangan Aplikasi SPBE yang dibutuhkan;
  8. Aplikasi SPBE sudah diujicobakan sebelum dioperasikan sesuai dengan kebutuhannya. Uji coba terhadap aplikasi harus terdokumentasi.
  9. Pengendalian akses ke kode sumber (*source code*) Aplikasi SPBE sudah dilakukan;
  10. Pelatihan kepada pengguna dan pegawai/petugas pengelola Aplikasi SPBE telah dilakukan;
  11. Tinjauan pasca implementasi telah dilakukan ketika selesai implementasi Aplikasi SPBE.
  12. Kapasitas Aplikasi SPBE sudah direncanakan dengan baik, dipantau, dianalisis dan dievaluasi penggunaannya;
  13. Insiden terkait Aplikasi SPBE dicatat dan ditangani dengan baik sesuai dengan kesepakatan tingkat layanan;
  14. Pengoperasian dan pemeliharaan Aplikasi SPBE telah dilakukan secara rutin sesuai dengan pedoman; dan
  15. Setiap pegawai/petugas pengelola Aplikasi SPBE harus mempunyai kompetensi yang sesuai dengan bidang tugasnya.
- c. Auditor harus melakukan pemeriksaan terhadap penyediaan layanan pengembangan dan/atau pemeliharaan aplikasi SPBE oleh pihak ketiga, paling sedikit untuk memastikan bahwa:
1. Pengendalian pemberian hak akses kepada pihak eksternal telah dilakukan;
  2. Pemantauan dan evaluasi layanan pihak eksternal telah ditinjau secara berkala;
  3. Evaluasi dan peninjauan layanan yang diberikan oleh pihak eksternal telah sesuai dengan pengendalian keamanan informasi yang ditetapkan dalam perjanjian atau kontrak; dan



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

4. Perjanjian Kerahasiaan (*Non Disclosure Agreement*) telah ditandatangani oleh pihak eksternal.
- d. Panduan teknis dan kriteria penilaian pada audit aplikasi SPBE dapat ditetapkan lebih lanjut oleh APIP, sesuai ketentuan peraturan perundang-undangan.

#### 2.4 Pedoman Teknis Audit Keamanan SPBE

- a. Audit Keamanan SPBE dilakukan pada aspek:
  1. Penerapan tata kelola keamanan pada lingkup aplikasi dan infrastruktur SPBE, yang meliputi evaluasi, pengarahan, dan pemantauan;
  2. Penerapan manajemen keamanan SPBE, yang meliputi: kebijakan keamanan; organisasi keamanan; keamanan personil; keamanan aset; keamanan akses; keamanan kriptografi; keamanan fisik dan lingkungan; keamanan operasional; keamanan komunikasi; keamanan pengembangan dan pemeliharaan; keamanan rekanan; insiden keamanan; keamanan kontinuitas; dan/atau kepatuhan keamanan;
  3. Kinerja Keamanan Aplikasi SPBE dan Keamanan Infrastruktur SPBE; dan
  4. Tingkat kepatuhan terhadap regulasi.
- b. Auditor harus melakukan pemeriksaan terhadap Arsitektur Keamanan SPBE paling sedikit untuk memastikan bahwa:
  1. Perubahan ancaman, kerentanan, risiko, dan kendali SPBE dipantau;
  2. Strategi Keamanan SPBE dan rencana Keamanan SPBE sudah selaras dengan kebutuhan Pemerintah Kabupaten Buleleng;
  3. Standar keamanan informasi sudah ditetapkan dan diimplementasikan; dan
  4. Rekomendasi arsitektur Keamanan SPBE sudah dilaksanakan.
  5. Peta Rencana Keamanan SPBE telah disusun berdasarkan analisis risiko dan kesenjangan arsitektur Keamanan SPBE;
  6. Peta Rencana Keamanan SPBE disusun berdasarkan prioritas pengembangannya;
  7. Sejauh mana Peta Rencana Keamanan SPBE sudah diimplementasikan;
  8. Peta Rencana Keamanan SPBE ditinjau secara berkala berdasarkan kajian risiko, rencana anggaran, atau hasil evaluasi SPBE.
  9. Kebijakan dan pedoman keamanan informasi sudah disusun dan disosialisasikan secara berkala;
  10. Dilakukan pelatihan peningkatan kepedulian (*awareness training*) keamanan informasi secara berkala;
  11. Pengelola dan pelaksana keamanan informasi sudah ditetapkan; dan
  12. Setiap sistem, Aplikasi SPBE, dan data telah ditentukan tingkat kritikalitasnya;



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

13. Setiap sistem dan proses bisnis telah ditetapkan pemiliknya;
  14. Ada prosedur pengelolaan pengguna dan hak aksesnya untuk setiap pegawai dan pihak eksternal;
  15. Setiap pengguna sistem diberi hak akses sesuai dengan kebutuhan minimumnya dan disetujui oleh pemilik proses bisnis;
  16. Setiap pengguna sistem bisa diidentifikasi secara individual;
  17. Dilakukan tinjauan secara berkala terhadap pengguna dan hak aksesnya di setiap sistem;
  18. Dilakukan pemantauan keamanan sistem secara proaktif;
  19. Dilakukan pengujian keamanan sistem secara berkala;
  20. Insiden keamanan informasi ditangani secara efektif;
  21. Dilakukan perlindungan terhadap data yang bersifat rahasia;
  22. Terdapat kendali aplikasi paling sedikit pada:
    - 1) Identifikasi, otentikasi, dan otorisasi;
    - 2) Antarmuka sistem;
    - 3) Keakuratan dan kelengkapan transaksi; dan
    - 4) *Logging* dan *audit trail*.
  23. Terdapat kendali infrastruktur paling sedikit pada:
    - 1) Identifikasi, otentikasi, dan otorisasi penggunaan Infrastruktur SPBE sudah dikelola;
    - 2) Di setiap sistem dilakukan instalasi perangkat lunak untuk mencegah dan mendeteksi perangkat lunak berbahaya (virus, malware, dan lain-lain);
    - 3) Pengendalian keamanan pada jaringan telah dilakukan; dan
    - 4) Dilakukan identifikasi infrastruktur yang kritis untuk dipantau.
- c. Auditor harus melakukan pemeriksaan terhadap penyediaan layanan keamanan SPBE oleh pihak eksternal paling sedikit untuk memastikan bahwa:
1. Pengendalian pemberian hak akses kepada pihak eksternal telah dilakukan;
  2. Pemantauan dan evaluasi layanan pihak eksternal telah ditinjau secara berkala;
  3. Evaluasi dan peninjauan layanan yang diberikan oleh pihak eksternal telah sesuai dengan pengendalian keamanan informasi yang ditetapkan dalam perjanjian atau kontrak; dan
  4. Perjanjian Kerahasiaan (*Non Disclosure Agreement*) telah ditandatangani oleh pihak eksternal.
- d. Panduan teknis dan kriteria penilaian pada audit keamanan SPBE dapat ditetapkan lebih lanjut oleh APIP, sesuai ketentuan peraturan perundang-undangan.



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

**(1) Pembiayaan Audit TIK**

- a. Pembiayaan untuk pelaksanaan Audit TIK dapat ditanggung oleh:
  1. APIP;
  2. Dinas Teknis terkait TIK; dan/atau
  3. Auditee yang mengusulkan kegiatan audit TIK.
- b. Besaran biaya pelaksanaan audit didasarkan pada cakupan area audit sesuai dengan kompleksitas proses bisnis.
- c. Mekanisme penganggaran audit TIK dapat dilakukan melalui perjanjian kerja dengan pihak ketiga atau swakelola yang disesuaikan dengan ketentuan peraturan perundang-undangan.



Dokumen ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik, Badan Siber dan Sandi Negara

Lampiran 7. Standar Pelayanan DiskominfoSanti Tahun 2023



Lampiran II : Keputusan Kepala Dinas Komunikasi, Informatika,  
Persandian dan Statistik Kabupaten Buleleng  
Nomor : 800/ 73/II/KOMINFOSANTI/2023  
Tanggal : 27 Februari 2023  
Tentang : Penetapan Standar Pelayanan Pada Dinas Komunikasi, Informatika, Persandian  
Dan Statistik Kabupaten Buleleng

**REKAPITULASI STANDAR LAYANAN  
DINAS KOMUNIKASI, INFORMATIKA, PERSANDIAN DAN STATISTIK  
KABUPATEN BULELENG**

| No | Unit Kerja                                      | Jenis Layanan                                                                                                                                                      | Halaman |
|----|-------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|
| A  | Sekretariat                                     | 1. Pelayanan Surat Masuk                                                                                                                                           | 2       |
|    |                                                 | 2. Pelayanan Surat Keluar                                                                                                                                          | 4       |
|    |                                                 | 3. Pelayanan Kepegawaian (Naik Pangkat, Pensiun, Pembuatan Karpeg, Karis/Karsu, Pengajuan SLKS, Pengusulan CPNS menjadi PNS, Pengusulan Ujian Dinas, Ijin Belajar) | 6       |
|    |                                                 | 4. Pelayanan Pengajuan Cuti Pegawai                                                                                                                                | 8       |
| B  | Bidang Pengelolaan dan Layanan Informasi Publik | 1. Pelayanan Pemantauan Media Komunikasi                                                                                                                           | 10      |
|    |                                                 | 2. Pelayanan Data/ Informasi                                                                                                                                       | 12      |
|    |                                                 | 3. Pelayanan Multimedia                                                                                                                                            | 14      |
|    |                                                 | 4. Pelayanan Siaran Keliling                                                                                                                                       | 16      |
| C  | Bidang Pengelolaan Komunikasi Publik            | 1. Pelayanan Liputan dan Dokumentasi                                                                                                                               | 18      |
|    |                                                 | 2. Pelayanan Fasilitas Pameran Pembangunan                                                                                                                         | 20      |
| D  | Bidang Infrastruktur dan Layanan SPBE           | 1. Pelayanan Bandwidth Internet                                                                                                                                    | 22      |
|    |                                                 | 2. Pelayanan Domain/Subdomain                                                                                                                                      | 24      |
|    |                                                 | 3. Pelayanan <i>Government Cloud Computing</i>                                                                                                                     | 26      |
| E  | Bidang Tata Kelola dan SDM SPBE                 | 1. Pelayanan Pelatihan SDM bidang TIK                                                                                                                              | 28      |
|    |                                                 | 2. Pelayanan Pemberian Rekomendasi Pembuatan/ pengembangan Aplikasi                                                                                                | 30      |
|    |                                                 | 3. Pelayanan Pembuatan/ pengembangan Aplikasi                                                                                                                      | 32      |
|    |                                                 | 4. Pelayanan Pertemuan Virtual                                                                                                                                     | 34      |
| F  | Bidang Persandian dan Statistik                 | 1. Pelayanan Data Sektoral Pemkab                                                                                                                                  | 36      |
|    |                                                 | 2. Pelayanan Computer Scurity Incident Response Team                                                                                                               | 38      |
|    |                                                 | 3. Pelayanan Radio Komunikasi Bersandi                                                                                                                             | 40      |
|    |                                                 | 4. Pelayanan Pembuatan Tanda Tangan Elektronik (TTE)                                                                                                               | 42      |
|    |                                                 | 5. Pelayanan Pengintegrasian Sistem Informasi dengan Sertifikat Elektronik                                                                                         | 44      |
|    |                                                 | 6. Pelayanan Penanganan Insiden Siber                                                                                                                              | 46      |
|    |                                                 | 7. Pelayanan Pengamanan Sinyal                                                                                                                                     | 48      |

Lampiran 8. Hasil Uji Kuesioner Pertama untuk Identifikasi Risiko Layanan DiskominfoSanti oleh Ahli

| ID | ASPEK YANG DI UJI                                     |                                                                           |                                                                                                                                                                              |                                                                                                                                                                                                                                                      | BUTIR PENILAIAN |    | SARAN                                                                 |
|----|-------------------------------------------------------|---------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|----|-----------------------------------------------------------------------|
|    | KATEGORI                                              | PENGERTIAN                                                                | JUSTIFIKASI                                                                                                                                                                  | RISIKO                                                                                                                                                                                                                                               | R               | TR |                                                                       |
| 06 | Information (data breach: damage, leakage and access) | Informasi (peretasan data: kerusakan, kebocoran dan penyalahgunaan akses) | Risiko yang berhubungan dengan data dan informasi yang disebabkan oleh peretasan data, kerusakan, kebocoran informasi dan penyalahgunaan hak akses.<br>→ <i>Rahasia</i><br>→ | Data hilang atau rusak, Kegagalan backup data, Serangan manusia (hacker, cracker), Kebocoran data organisasi, Perusahaan mengalami limpahan data dan tidak dapat menyimpulkan informasi yang relevan dari data tersebut (misalnya, data bermasalah). | ✓               |    | <i>Perlu diklasifikasikan nanti data yang sifatnya Rahasia/public</i> |

| ID | ASPEK YANG DI UJI                                                                                                                         |                                                                                                                              |                                                                                                            |                                                                                                                                                                      | BUTIR<br>PENILAIAN |  | SARAN |
|----|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|--|-------|
| 08 | <i>Infrastructure (hardware, operating system and controlling technology) (selection/ implementation, operations and decommissioning)</i> | Infrastruktur (perangkat keras, sistem operasi dan teknologi pengontrolan) (pemilihan / implementasi, operasi dan penarikan) | Risiko yang berhubungan dengan infrastruktur (perangkat keras, sistem operasi, dan teknologi pengontrolan) | Kerusakan hardware, Koneksi internet tidak memadai, Koneksi jaringan terputus, Listrik padam, Server Down, Kondisi server, Perangkat mengalami Overheat dan overload | ✓                  |  |       |
| 09 | <i>software</i>                                                                                                                           | Perangkat lunak                                                                                                              | Risiko yang berhubungan dengan perangkat lunak                                                             | Pemakaian Software non orisinal, Dokumentasi atau                                                                                                                    | ✓                  |  |       |

| ID | ASPEK YANG DI UJI |  |  |                                                                                                                                                                                                                | BUTIR<br>PENILAIAN |  | SARAN |
|----|-------------------|--|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|--|-------|
|    |                   |  |  | tata cara<br>penggunaan<br>program / aplikasi<br>tidak lengkap,<br>Antar muka (user<br>interface) program<br>atau aplikasi susah<br>dipahami, Aplikasi<br>SPBE yang belum<br>stabil telah<br>diimplementasikan |                    |  |       |

**Keterangan**

R : Relevan

TR : Tidak Relevan

**Hasil Validasi Uji Kuesioner Oleh Ahli**  
**Dalam Rangka Penelitian Perancangan Manajemen Risiko Operasional SPBE**  
**Pada DiskominfoSanti Kabupaten Buleleng**

---

**Data Penguji Ahli**

|          |                                               |
|----------|-----------------------------------------------|
| Nama     | : Gede Arna Jude Saskara, S.T., M.T.          |
| Instansi | : Universitas Pendidikan Ganesha              |
| Jabatan  | : Asisten Ahli – Dosen Prodi Sistem Informasi |
| NIP      | : 199105152020121003                          |

**Hasil Kuesioner**

1. Pada ID 06 *Information* sudah RELEVAN akan tetapi perlu diklasifikasikan nanti data yang sifatnya rahasia atau sifatnya data publik

**Penguji Ahli,**



**Gede Arna Jude Saskara, S.T., M.T.**  
**NIP. 199105152020121003**

**Singaraja, 27 Maret 2024**

**Peneliti,**



**Vany Adelia Putri**  
**NIM. 2015091027**

| ID | ASPEK YANG DI UJI                                            |                                                                           |                                                                                                                                                     |                                                                                                                                                                                                                                                      | BUTIR PENILAIAN |    | SARAN |
|----|--------------------------------------------------------------|---------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|----|-------|
|    | KATEGORI                                                     | PENGERTIAN                                                                | JUSTIFIKASI                                                                                                                                         | RISIKO                                                                                                                                                                                                                                               | R               | TR |       |
| 06 | <i>Information (data breach: damage, leakage and access)</i> | Informasi (peretasan data: kerusakan, kebocoran dan penyalahgunaan akses) | Risiko yang berhubungan dengan data dan informasi yang disebabkan oleh peretasan data, kerusakan, kebocoran informasi dan penyalahgunaan hak akses. | Data hilang atau rusak, Kegagalan backup data, Serangan manusia (hacker, cracker), Kebocoran data organisasi, Perusahaan mengalami limpahan data dan tidak dapat menyimpulkan informasi yang relevan dari data tersebut (misalnya, data bermasalah). | ✓               |    |       |

| ID | ASPEK YANG DI UJI                                                                                                                         |                                                                                                                              |                                                                                                            |                                                                                                                                                                      | BUTIR PENILAIAN |   | SARAN                                                                                                                                                          |
|----|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|---|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 08 | <i>Infrastructure (hardware, operating system and controlling technology) (selection/ implementation, operations and decommissioning)</i> | Infrastruktur (perangkat keras, sistem operasi dan teknologi pengontrolan) (pemilihan / implementasi, operasi dan penarikan) | Risiko yang berhubungan dengan infrastruktur (perangkat keras, sistem operasi, dan teknologi pengontrolan) | Kerusakan hardware, Koneksi internet tidak memadai, Koneksi jaringan terputus, Listrik padam, Server Down, Kondisi server, Perangkat mengalami Overheat dan overload |                 | ✓ | <ul style="list-style-type: none"> <li>- kondisi ruang</li> <li>- kondisi instalasi kabel gantung</li> <li>(lebih rinci, etc: jarak akses pin, dll)</li> </ul> |
| 09 | <i>software</i>                                                                                                                           | Perangkat lunak                                                                                                              | Risiko yang berhubungan dengan perangkat lunak                                                             | Pemakaian Software non orisinal, Dokumentasi atau                                                                                                                    |                 |   |                                                                                                                                                                |

| ID | ASPEK YANG DI UJI |  |  |                                                                                                                                                                                  | BUTIR PENILAIAN |   | SARAN                                                  |
|----|-------------------|--|--|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|---|--------------------------------------------------------|
|    |                   |  |  | tata cara penggunaan program / aplikasi tidak lengkap, Antar muka (user interface) program atau aplikasi susah dipahami, Aplikasi SPBE yang belum stabil telah diimplementasikan |                 | ✓ | - tambahkan sosialisasi dan pelatihan pengguna sistem. |

**Keterangan**

R : Relevan

TR : Tidak Relevan

**Hasil Validasi Uji Kuesioner Oleh Ahli**  
**Dalam Rangka Penelitian Perancangan Manajemen Risiko Operasional SPBE**  
**Pada DiskominfoSanti Kabupaten Buleleng**

**Data Penguji Ahli**

|          |                                                  |
|----------|--------------------------------------------------|
| Nama     | : I Gusti Lanang Agung Raditya Putra, S.Pd.,M.T. |
| Instansi | : Universitas Pendidikan Ganesha                 |
| Jabatan  | : Asisten Ahli – Dosen Prodi Sistem Informasi    |
| NIP      | : 198908272019031008                             |

**Hasil Kuesioner**

1. Pada ID 08 *Infrastructure* TIDAK RELEVAN sebab perlu merincikan misalkan bagaimana kondisi ruangan objek penelitian, kondisi instalansi kabel jaringan seperti jarak, akses poin, dll.
2. Pada ID 09 *Software* TIDAK RELEVAN sebab disarankan perlu ditambahkan sosialisasi dan pelatihan pada pengguna sistem.

Penguji Ahli,



I Gusti Lanang Agung Raditya Putra, S.Pd.,M.T.  
NIP. 198908272019031008

Singaraja, 27 Maret 2024

Peneliti,



Vany Adelia Putri  
NIM. 2015091027

Lampiran 9. Hasil Uji Kuesioner Kedua (Revisi) untuk Identifikasi Risiko Layanan DiskominfoSanti oleh Ahli

| ID | ASPEK YANG DI UJI                                            |                                                                           |                                                                                                                                                                               |                                                                                                                                                                                                                                                               | BUTIR PENILAIAN |    | SARAN |
|----|--------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|----|-------|
|    | KATEGORI                                                     | PENGERTIAN                                                                | JUSTIFIKASI                                                                                                                                                                   | RISIKO                                                                                                                                                                                                                                                        | R               | TR |       |
| 06 | <i>Information (data breach: damage, leakage and access)</i> | Informasi (peretasan data: kerusakan, kebocoran dan penyalahgunaan akses) | Risiko yang berhubungan dengan data bersifat rahasia, internal dan terbatas yang disebabkan oleh peretasan data, kerusakan, kebocoran informasi dan penyalahgunaan hak akses. | Data hilang atau rusak, Kegagalan backup data, Serangan manusia ( <i>hacker, cracker</i> ), Kebocoran data organisasi, Perusahaan mengalami limpahan data dan tidak dapat menyimpulkan informasi yang relevan dari data tersebut (misalnya, data bermasalah). | ✓               |    |       |

| ID | ASPEK YANG DI UJI                                                                                                                        |                                                                                                                              |                                                                                                            |                                                                                                                                                                                                                                                                                  | BUTIR PENILAIAN |    | SARAN |
|----|------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|----|-------|
|    | KATEGORI                                                                                                                                 | PENGERTIAN                                                                                                                   | JUSTIFIKASI                                                                                                | RISIKO                                                                                                                                                                                                                                                                           | R               | TR |       |
| 08 | <i>Infrastructure (hardware, operating system and controlling technology) (selection/implementation, operations and decommissioning)</i> | Infrastruktur (perangkat keras, sistem operasi dan teknologi pengontrolan) (pemilihan / implementasi, operasi dan penarikan) | Risiko yang berhubungan dengan infrastruktur (perangkat keras, sistem operasi, dan teknologi pengontrolan) | Kerusakan <i>hardware</i> , Gangguan Koneksi Internet, Koneksi jaringan terputus, Listrik padam tiba-tiba, Ruangan <i>server</i> tidak menggunakan PAC ( <i>Precision Air Conditioning</i> ), <i>Server</i> mengalami kendala karena tidak adanya sumber energi listrik Cadangan | ✓               |    |       |

| ID | ASPEK YANG DI UJI |            |             |                                                                                                                                                                                                                                                                                 | BUTIR<br>PENILAIAN |    | SARAN |
|----|-------------------|------------|-------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|----|-------|
|    | KATEGORI          | PENGERTIAN | JUSTIFIKASI | RISIKO                                                                                                                                                                                                                                                                          | R                  | TR |       |
|    |                   |            |             | (Cth: UPS dan Genset), Akses masuk ke dalam ruangan <i>server</i> tidak dicatat dan tidak dibatasi, Ruangan <i>server</i> tidak dipantau melalui CCTV, Tidak tersedia pemadam api (Contoh: NOVEC) dalam ruangan <i>server</i> , Tidak ada tim monitoring khusus <i>server</i> , |                    |    |       |

| ID | ASPEK YANG DI UJI |            |             |                                                                                                                                                                                                                                                             | BUTIR PENILAIAN |    | SARAN |
|----|-------------------|------------|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|----|-------|
|    | KATEGORI          | PENGERTIAN | JUSTIFIKASI | RISIKO                                                                                                                                                                                                                                                      | R               | TR |       |
|    |                   |            |             | <p><i>Server mengalami down, Kondisi server yang tidak memadai/tidak layak (Contoh: Server Usang), Kondisi server yang tidak memadai/tidak layak (Contoh: Server Usang), Sistem operasi pada server tidak menyediakan interface untuk mengakses dan</i></p> |                 |    |       |

| ID | ASPEK YANG DI UJI |            |             |                                                                                                                                                                                                                                                                                                                          | BUTIR PENILAIAN |    | SARAN |
|----|-------------------|------------|-------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|----|-------|
|    | KATEGORI          | PENGERTIAN | JUSTIFIKASI | RISIKO                                                                                                                                                                                                                                                                                                                   | R               | TR |       |
|    |                   |            |             | <p>mengelola <i>server</i> (Contoh: CLI maupun GUI),</p> <p>Tidak melakukan <i>backup data</i> secara berkala atau otomatis, <i>Maintenance</i> tidak terjadwal, <i>Server</i> mengalami serangan (Contoh: Virus), <i>Backup failure</i>, <i>Data corrupt</i>, Tidak melakukan <i>back up data</i> dan <i>system</i></p> |                 |    |       |

| ID | ASPEK YANG DI UJI |                 |                                                |                                                                                                                                                                  | BUTIR PENILAIAN |    | SARAN |
|----|-------------------|-----------------|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|----|-------|
|    | KATEGORI          | PENGERTIAN      | JUSTIFIKASI                                    | RISIKO                                                                                                                                                           | R               | TR |       |
|    |                   |                 |                                                | server secara berkala, Tidak dilakukan kelola hak akses pengguna                                                                                                 |                 |    |       |
| 09 | software          | Perangkat lunak | Risiko yang berhubungan dengan perangkat lunak | Pemakaian Software non orisinal, Dokumentasi atau tata cara penggunaan program / aplikasi tidak lengkap, Antar muka (user interface) program atau aplikasi susah | ✓               |    |       |

| ID | ASPEK YANG DI UJI |            |             |                                                                                                          | BUTIR PENILAIAN |    | SARAN |
|----|-------------------|------------|-------------|----------------------------------------------------------------------------------------------------------|-----------------|----|-------|
|    | KATEGORI          | PENGERTIAN | JUSTIFIKASI | RISIKO                                                                                                   | R               | TR |       |
|    |                   |            |             | dipahami, Aplikasi SPBE yang belum stabil telah diimplementasikan                                        |                 |    |       |
|    |                   |            |             | Tidak ada sosialisasi dan pelatihan teknis sebelum perangkat lunak digunakan secara massif di organisasi | ✓               |    |       |

**Keterangan**

R : Relevan

TR : Tidak Relevan

**Hasil Validasi Uji Kuesioner Oleh Ahli**  
**Dalam Rangka Penelitian Perancangan Manajemen Risiko Operasional SPBE**  
**Pada DiskominfoSanti Kabupaten Buleleng**

---

**Data Penguji Ahli**

|          |                                               |
|----------|-----------------------------------------------|
| Nama     | : Gede Arna Jude Saskara, S.T., M.T.          |
| Instansi | : Universitas Pendidikan Ganesha              |
| Jabatan  | : Asisten Ahli – Dosen Prodi Sistem Informasi |
| NIP      | : 199105152020121003                          |

**Hasil Kuesioner**

1. -

**Penguji Ahli,**



**Gede Arna Jude Saskara, S.T., M.T.**

**NIP. 199105152020121003**

**Singaraja, 28 Maret 2024**

**Peneliti,**



**Vany Adelia Putri**

**NIM. 2015091027**

| ID | ASPEK YANG DI UJI                                            |                                                                           |                                                                                                                                                                               |                                                                                                                                                                                                                                                               | BUTIR PENILAIAN |    | SARAN |
|----|--------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|----|-------|
|    | KATEGORI                                                     | PENGERTIAN                                                                | JUSTIFIKASI                                                                                                                                                                   | RISIKO                                                                                                                                                                                                                                                        | R               | TR |       |
| 06 | <i>Information (data breach: damage, leakage and access)</i> | Informasi (peretasan data: kerusakan, kebocoran dan penyalahgunaan akses) | Risiko yang berhubungan dengan data bersifat rahasia, internal dan terbatas yang disebabkan oleh peretasan data, kerusakan, kebocoran informasi dan penyalahgunaan hak akses. | Data hilang atau rusak, Kegagalan backup data, Serangan manusia ( <i>hacker, cracker</i> ), Kebocoran data organisasi, Perusahaan mengalami limpahan data dan tidak dapat menyimpulkan informasi yang relevan dari data tersebut (misalnya, data bermasalah). | ✓               |    |       |

| ID | ASPEK YANG DI UJI |  |  |                                                                                                                                                                                                                                                                                                               | BUTIR PENILAIAN |  | SARAN |
|----|-------------------|--|--|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|--|-------|
|    |                   |  |  | Genset), Akses masuk ke dalam ruangan <i>server</i> tidak dicatat dan tidak dibatasi, Ruang <i>server</i> tidak dipantau melalui CCTV, Tidak tersedia pemadam api (Contoh: NOVEC) dalam ruangan <i>server</i> , Tidak ada tim monitoring khusus <i>server</i> , <i>Server</i> mengalami <i>down</i> , Kondisi |                 |  |       |

| ID | ASPEK YANG DI UJI |  |  |                                                                                                                                                                                                                                                                                                                   | BUTIR PENILAIAN |  | SARAN |
|----|-------------------|--|--|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|--|-------|
|    |                   |  |  | <p><i>server</i> yang tidak memadai/tidak layak (Contoh: <i>Server</i> Usang), Kondisi <i>server</i> yang tidak memadai/tidak layak (Contoh: <i>Server</i> Usang), Sistem operasi pada <i>server</i> tidak menyediakan <i>interface</i> untuk mengakses dan mengelola <i>server</i> (Contoh: CLI maupun GUI),</p> |                 |  |       |

| ID | ASPEK YANG DI UJI |  |  |                                                                                                                                                                                                                                                                                                                                | BUTIR<br>PENILAIAN |  | SARAN |
|----|-------------------|--|--|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|--|-------|
|    |                   |  |  | <p>Tidak melakukan <i>backup data</i> secara berkala atau otomatis, <i>Maintenance</i> tidak terjadwal, <i>Server</i> mengalami serangan (Contoh: <i>Virus</i>), <i>Backup failure</i>, <i>Data corrupt</i>, Tidak melakukan <i>back up</i> data dan <i>system server</i> secara berkala, Tidak dilakukan kelola hak akses</p> |                    |  |       |

| ID | ASPEK YANG DI UJI |                 |                                                |                                                                                                                                                                                                                                    | BUTIR PENILAIAN |  | SARAN |
|----|-------------------|-----------------|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------|--|-------|
|    |                   |                 |                                                | pengguna                                                                                                                                                                                                                           |                 |  |       |
| 09 | <i>software</i>   | Perangkat lunak | Risiko yang berhubungan dengan perangkat lunak | Pemakaian Software non orisinal, Dokumentasi atau tata cara penggunaan program / aplikasi tidak lengkap, Antar muka (user interface) program atau aplikasi susah dipahami, Aplikasi SPBE yang belum stabil telah diimplementasikan | ✓               |  |       |
|    |                   |                 |                                                | Tidak ada                                                                                                                                                                                                                          |                 |  |       |

| ID | ASPEK YANG DI UJI |  |  |                                                                                                               | BUTIR<br>PENILAIAN |  | SARAN |
|----|-------------------|--|--|---------------------------------------------------------------------------------------------------------------|--------------------|--|-------|
|    |                   |  |  |                                                                                                               |                    |  |       |
|    |                   |  |  | sosialisasi dan<br>pelatihan teknis<br>sebelum perangkat<br>lunak digunakan<br>secara massif di<br>organisasi |                    |  |       |

**Keterangan**

R : Relevan

TR : Tidak Relevan



**Hasil Validasi Uji Kuesioner Oleh Ahli**  
**Dalam Rangka Penelitian Perancangan Manajemen Risiko Operasional SPBE**  
**Pada DiskominfoSanti Kabupaten Buleleng**

---

**Data Penguji Ahli**

|          |                                                  |
|----------|--------------------------------------------------|
| Nama     | : I Gusti Lanang Agung Raditya Putra, S.Pd.,M.T. |
| Instansi | : Universitas Pendidikan Ganesha                 |
| Jabatan  | : Asisten Ahli – Dosen Prodi Sistem Informasi    |
| NIP      | : 198908272019031008                             |

**Hasil Kuesioner**

1. 

**Penguji Ahli,**



**I Gusti Lanang Agung Raditya Putra, S.Pd.,M.T.**

**NIP. 198908272019031008**

**Singaraja, 1 April 2024**

**Peneliti,**



**Vany Adelia Putri**

**NIM. 2015091027**

Lampiran 10. Pemilihan Layanan Berdasarkan Urgensi

Responden : Fransiskus Asisi Wawan Triyudhawianta

Jabatan/NIP : Staff Perencanaan Ahli Muda/197910052006041011

Instansi : Dinas Kominfosanti

Tempat/Tanggal : Singaraja / 28 Maret 2024

**IDENTIFIKASI RISIKO LAYANAN**

*Checklist (√) Pada Pernyataan Identifikasi Yang Sesuai*

| NO | UNIT KERJA  | JENIS LAYANAN            | PENGGUNA LAYANAN | IDENTIFIKASI LAYANAN                      |                                                               |                                                                           |                                                                   |                                                                |
|----|-------------|--------------------------|------------------|-------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |             |                          |                  | Layanan<br>Kerap<br>Mengalami<br>Gangguan | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
| 1  | SEKRETARIAT | Pelayanan Surat<br>Masuk | Kadis            |                                           | √                                                             |                                                                           |                                                                   |                                                                |

| NO | UNIT KERJA | JENIS LAYANAN                                                                                                             | PENGGUNA LAYANAN         | IDENTIFIKASI LAYANAN                                                                |                                                               |                                                                           |                                                                   |                                                                |
|----|------------|---------------------------------------------------------------------------------------------------------------------------|--------------------------|-------------------------------------------------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |            |                                                                                                                           |                          | Layanan<br>Kerap<br>Mengalami<br>Gangguan                                           | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
|    |            | Pelayanan Surat Keluar                                                                                                    | Pengaju Surat pada Kadis |  | √                                                             |                                                                           |                                                                   |                                                                |
|    |            | Pelayanan Kepegawaian (Naik Pangkat, Pensiun, Pembuatan Karpeg, Karis/Karsu, Pengajuan SLKS, Pengusulan CPNS menjadi PNS, | Pegawai                  |  | √                                                             |                                                                           |                                                                   |                                                                |

| NO | UNIT KERJA | JENIS LAYANAN                          | PENGGUNA LAYANAN | IDENTIFIKASI LAYANAN                      |                                                               |                                                                           |                                                                   |                                                                |
|----|------------|----------------------------------------|------------------|-------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |            |                                        |                  | Layanan<br>Kerap<br>Mengalami<br>Gangguan | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
|    |            | Pengusulan Ujian Dinas, Ijin Belajar). | Pegawai          |                                           | √                                                             |                                                                           |                                                                   |                                                                |
|    |            | Pelayanan Pengajuan Cuti Pegawai.      |                  |                                           |                                                               |                                                                           |                                                                   |                                                                |
|    | 2          | Pelayanan Pemantauan Media Komunikasi  |                  |                                           |                                                               | √                                                                         |                                                                   |                                                                |
|    |            | Pelayanan Data/ Informasi              |                  |                                           |                                                               | √                                                                         |                                                                   |                                                                |

| NO | UNIT KERJA                    | JENIS LAYANAN                     | PENGGUNA LAYANAN                                                   | IDENTIFIKASI LAYANAN                      |                                                               |                                                                           |                                                                   |                                                                |
|----|-------------------------------|-----------------------------------|--------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |                               |                                   |                                                                    | Layanan<br>Kerap<br>Mengalami<br>Gangguan | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
|    |                               | Pelayanan Multimedia.             |                                                                    |                                           |                                                               | √                                                                         |                                                                   |                                                                |
|    |                               | Pelayanan Siaran Keliling         |                                                                    |                                           |                                                               | √                                                                         |                                                                   |                                                                |
| 3  | PENGELOLAAN KOMUNIKASI PUBLIK | Pelayanan Liputan dan Dokumentasi | Instansi pemerintah yang membutuhkan peliputan ataupun dokumentasi |                                           |                                                               |                                                                           |                                                                   | √                                                              |

| NO | UNIT KERJA | JENIS LAYANAN                                  | PENGGUNA LAYANAN                                                                                                                                                 | IDENTIFIKASI LAYANAN                      |                                                               |                                                                           |                                                                   |                                                                |
|----|------------|------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |            |                                                |                                                                                                                                                                  | Layanan<br>Kerap<br>Mengalami<br>Gangguan | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
|    |            | Pelayanan Fasilitasi<br>Pameran<br>Pembangunan | Instansi<br>pemerintah<br>maupun instansi<br>swasta yang<br>akan mengikuti<br>Pameran<br>Pembangunan<br>yang<br>dilaksanakan<br>baik di tingkat<br>Provinsi Bali |                                           |                                                               | √                                                                         |                                                                   |                                                                |

| NO | UNIT KERJA                           | JENIS LAYANAN                   | PENGGUNA LAYANAN                                                                                           | IDENTIFIKASI LAYANAN                      |                                                               |                                                                           |                                                                   |                                                                |
|----|--------------------------------------|---------------------------------|------------------------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |                                      |                                 |                                                                                                            | Layanan<br>Kerap<br>Mengalami<br>Gangguan | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
|    |                                      |                                 | maupun tingkat<br>Kabupaten<br>Buleleng                                                                    |                                           |                                                               |                                                                           |                                                                   |                                                                |
| 4  | INFRASTRUKTUR<br>DAN LAYANAN<br>SPBE | Pelayanan<br>Bandwidth Internet | Perangkat<br>daerah lingkup<br>Pemkab<br>Buleleng dan<br>UPTD<br>dibawahnya,<br>Kantor Desa,<br>Desa Adat, |                                           | √                                                             | √                                                                         | √                                                                 | √                                                              |

| NO | UNIT KERJA | JENIS LAYANAN                 | PENGGUNA LAYANAN                                                                                                          | IDENTIFIKASI LAYANAN                      |                                                               |                                                                           |                                                                   |                                                                |
|----|------------|-------------------------------|---------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |            |                               |                                                                                                                           | Layanan<br>Kerap<br>Mengalami<br>Gangguan | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
|    |            |                               | Tempat wisata,<br>dan tempat-<br>tempat tertentu<br>lainnya yang<br>berada dalam<br>pengelolaan<br>instansi<br>pemerintah |                                           |                                                               |                                                                           |                                                                   |                                                                |
|    |            | Pelayanan<br>Domain/Subdomain | Instansi<br>pemerintah<br>ataupun panitia                                                                                 |                                           | √                                                             | √                                                                         | √                                                                 | √                                                              |

| NO | UNIT KERJA | JENIS LAYANAN                                  | PENGGUNA LAYANAN                                                               | IDENTIFIKASI LAYANAN                      |                                                               |                                                                           |                                                                   |                                                                |
|----|------------|------------------------------------------------|--------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |            |                                                |                                                                                | Layanan<br>Kerap<br>Mengalami<br>Gangguan | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
|    |            |                                                | pelaksana kegiatan yang merupakan kegiatan milik Pemerintah Kabupaten Buleleng |                                           |                                                               |                                                                           |                                                                   |                                                                |
|    |            | Pelayanan<br><i>Government Cloud Computing</i> | Perangkat daerah lingkup Pemkab Buleleng yang                                  |                                           | √                                                             | √                                                                         |                                                                   |                                                                |

| NO | UNIT KERJA               | JENIS LAYANAN                      | PENGGUNA LAYANAN                                                          | IDENTIFIKASI LAYANAN                      |                                                               |                                                                           |                                                                   |                                                                |
|----|--------------------------|------------------------------------|---------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |                          |                                    |                                                                           | Layanan<br>Kerap<br>Mengalami<br>Gangguan | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
|    |                          |                                    | memiliki sistem/aplikasi layanan yang membutuhkan sistem cloud computing. |                                           |                                                               |                                                                           |                                                                   |                                                                |
| 5  | TATA KELOLA DAN SDM SPBE | Pelayanan Pelatihan SDM bidang TIK | Instansi pemerintah maupun kelompok masyarakat yang                       |                                           |                                                               | √                                                                         |                                                                   | √                                                              |

| NO | UNIT KERJA | JENIS LAYANAN          | PENGGUNA LAYANAN                                                                                      | IDENTIFIKASI LAYANAN                      |                                                               |                                                                           |                                                                   |                                                                |
|----|------------|------------------------|-------------------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |            |                        |                                                                                                       | Layanan<br>Kerap<br>Mengalami<br>Gangguan | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
|    |            |                        | membutuhkan peningkatan pengetahuan sumber daya manusia di bidang Teknologi Informasi dan Komunikasi. |                                           |                                                               |                                                                           |                                                                   |                                                                |
|    |            | Pelayanan<br>Pemberian | Perangkat daerah lingkup                                                                              |                                           | √                                                             | √                                                                         |                                                                   |                                                                |

| NO | UNIT KERJA | JENIS LAYANAN                                          | PENGGUNA LAYANAN                                                                                                                 | IDENTIFIKASI LAYANAN                      |                                                               |                                                                           |                                                                   |                                                                |
|----|------------|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |            |                                                        |                                                                                                                                  | Layanan<br>Kerap<br>Mengalami<br>Gangguan | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
|    |            | Rekomendasi<br>Pembuatan/<br>pengembangan<br>Aplikasi. | Pemkab<br>Buleleng yang<br>akan melakukan<br>pembuatan<br>aplikasi baru<br>atau<br>pengembangan<br>aplikasi yang<br>sudah ada, y |                                           |                                                               |                                                                           |                                                                   |                                                                |
|    |            | Pelayanan<br>Pembuatan/                                | Perangkat<br>daerah lingkup                                                                                                      |                                           | √                                                             | √                                                                         |                                                                   |                                                                |

| NO | UNIT KERJA | JENIS LAYANAN          | PENGGUNA LAYANAN                                                                                                      | IDENTIFIKASI LAYANAN                      |                                                               |                                                                           |                                                                   |                                                                |
|----|------------|------------------------|-----------------------------------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |            |                        |                                                                                                                       | Layanan<br>Kerap<br>Mengalami<br>Gangguan | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
|    |            | pengembangan Aplikasi. | Pemkab Buleleng yang akan membuat atau mengembangkan aplikasi layanan pemerintah dan menyerahkannya kepada Diskominfo |                                           |                                                               |                                                                           |                                                                   |                                                                |

| NO | UNIT KERJA                  | JENIS LAYANAN                     | PENGGUNA LAYANAN                                                                            | IDENTIFIKASI LAYANAN                      |                                                               |                                                                           |                                                                   |                                                                |
|----|-----------------------------|-----------------------------------|---------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |                             |                                   |                                                                                             | Layanan<br>Kerap<br>Mengalami<br>Gangguan | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
|    |                             | Pelayanan<br>Pertemuan Virtual.   | Instansi<br>pemerintah yang<br>akan melakukan<br>pertemuan<br>virtual                       |                                           | √                                                             | √                                                                         | √                                                                 | √                                                              |
| 6. | PERSANDIAN<br>DAN STATISTIK | Pelayanan Data<br>Sektoral Pemkab | Siapa saja yang<br>membutuhkan<br>data sektoral<br>pemkab<br>Buleleng, baik<br>itu instansi |                                           | √                                                             | √                                                                         |                                                                   | √                                                              |

| NO | UNIT KERJA | JENIS LAYANAN                 | PENGGUNA LAYANAN                                                                                                            | IDENTIFIKASI LAYANAN                      |                                                               |                                                                           |                                                                   |                                                                |
|----|------------|-------------------------------|-----------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |            |                               |                                                                                                                             | Layanan<br>Kerap<br>Mengalami<br>Gangguan | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
|    |            |                               | pemerintah,<br>swasta, sekolah,<br>pelajar/<br>mahasiswa,<br>kelompok<br>masyarakat<br>ataupun<br>masyarakat<br>perorangan. |                                           |                                                               |                                                                           |                                                                   |                                                                |
|    |            | Pelayanan<br>Computer Scurity | Instansi<br>pemerintah,                                                                                                     |                                           | √                                                             | √                                                                         | √                                                                 |                                                                |

| NO | UNIT KERJA | JENIS LAYANAN          | PENGGUNA LAYANAN                                                                                   | IDENTIFIKASI LAYANAN                      |                                                               |                                                                           |                                                                   |                                                                |
|----|------------|------------------------|----------------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |            |                        |                                                                                                    | Layanan<br>Kerap<br>Mengalami<br>Gangguan | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
|    |            | Incident Response Team | kelompok masyarakat atau masyarakat perorangan yang mengalami gangguan keamanan berbasis komputer. |                                           |                                                               |                                                                           |                                                                   |                                                                |

| NO | UNIT KERJA | JENIS LAYANAN                       | PENGGUNA LAYANAN                                                                                                   | IDENTIFIKASI LAYANAN                      |                                                               |                                                                           |                                                                   |                                                                |
|----|------------|-------------------------------------|--------------------------------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |            |                                     |                                                                                                                    | Layanan<br>Kerap<br>Mengalami<br>Gangguan | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
|    |            | Pelayanan Radio Komunikasi Bersandi | Instansi pemerintah dan kelompok masyarakat yang membutuhkan radio komunikasi bersandi untuk menunjang pelaksanaan |                                           | √                                                             | √                                                                         | √                                                                 |                                                                |

| NO | UNIT KERJA | JENIS LAYANAN                                             | PENGGUNA LAYANAN                                                                                                                     | IDENTIFIKASI LAYANAN                      |                                                               |                                                                           |                                                                   |                                                                |
|----|------------|-----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |            |                                                           |                                                                                                                                      | Layanan<br>Kerap<br>Mengalami<br>Gangguan | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
|    |            |                                                           | kegiatan/ even<br>yang bersi                                                                                                         |                                           |                                                               |                                                                           |                                                                   |                                                                |
|    |            | Pelayanan<br>Pembutan Tanda<br>Tangan Elektronik<br>(TTE) | Perangkat<br>daerah lingkup<br>Pembkab<br>Buleleng yang<br>membutuhkan<br>Tanda Tangan<br>Elektronik<br>(TTE) yang akan<br>menunjang |                                           | √                                                             | √                                                                         |                                                                   |                                                                |

| NO | UNIT KERJA | JENIS LAYANAN                                                                       | PENGGUNA LAYANAN                                                                                                                 | IDENTIFIKASI LAYANAN                      |                                                               |                                                                           |                                                                   |                                                                |
|----|------------|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |            |                                                                                     |                                                                                                                                  | Layanan<br>Kerap<br>Mengalami<br>Gangguan | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
|    |            |                                                                                     | kinerja<br>perangkat<br>daerahnya.                                                                                               |                                           |                                                               |                                                                           |                                                                   |                                                                |
|    |            | Pelayanan<br>Pengintegrasian<br>Sistem Informasi<br>dengan Sertifikat<br>Elektronik | Perangkat<br>daerah lingkup<br>Pemkab<br>Buleleng yang<br>membutuhkan<br>integrasi sistem<br>informasi yang<br>telah dimilikinya |                                           | √                                                             | √                                                                         |                                                                   | √                                                              |

| NO | UNIT KERJA | JENIS LAYANAN                      | PENGGUNA LAYANAN                                                                                     | IDENTIFIKASI LAYANAN                      |                                                               |                                                                           |                                                                   |                                                                |
|----|------------|------------------------------------|------------------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |            |                                    |                                                                                                      | Layanan<br>Kerap<br>Mengalami<br>Gangguan | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
|    |            |                                    | dengan Tanda Tangan Elektronik. S                                                                    |                                           |                                                               |                                                                           |                                                                   |                                                                |
|    |            | Pelayanan Penanganan Insiden Siber | Instansi pemerintah yang mengalami gangguan terhadap akun resmi yang dimilikinya baik itu akun media |                                           | √                                                             | √                                                                         |                                                                   | √                                                              |

| NO | UNIT KERJA | JENIS LAYANAN                      | PENGGUNA LAYANAN                                                                                                        | IDENTIFIKASI LAYANAN                      |                                                               |                                                                           |                                                                   |                                                                |
|----|------------|------------------------------------|-------------------------------------------------------------------------------------------------------------------------|-------------------------------------------|---------------------------------------------------------------|---------------------------------------------------------------------------|-------------------------------------------------------------------|----------------------------------------------------------------|
|    |            |                                    |                                                                                                                         | Layanan<br>Kerap<br>Mengalami<br>Gangguan | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Kinerja | Dampak<br>Gangguan<br>Pada Layanan<br>Mempengaruhi<br>Penilaian<br>Publik | Layanan<br>Menjadi<br>Prioritas<br>Apabila<br>Terjadi<br>Gangguan | Layanan<br>Menjadi<br>Prioritas<br>Pada<br>Periode<br>Tertentu |
|    |            |                                    | sosial maupun<br>website resmi.                                                                                         |                                           |                                                               |                                                                           |                                                                   |                                                                |
|    |            | Pelayanan<br>Pengamanan<br>Sinyal. | Instansi<br>pemerintah atau<br>panitia<br>pelaksana<br>kegiatan/even<br>penting<br>Pemerintah<br>Kabupaten<br>Buleleng. |                                           | √                                                             | √                                                                         |                                                                   |                                                                |

## Lampiran 11. Penetapan Pemilihan Layanan

**Narasumber** : Fransiskus Asisi Wawan Triyudawanto, ST, M.Kom  
**Jabatan** : Staff Perencanaan  
**Instansi** : Dinas Komunikasi, Informatika, Persandian dan Statistik  
**Tempat/Tanggal** : Singaraja/22 April 2024

| NO. | PERTANYAAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | JAWABAN                                                                                                                                                                                           |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.  | <p>Terkait hasil kuesioner identifikasi layanan risiko milik Diskominfosanti yang sebelumnya telah didapatkan dari bantuan bagian perencanaan, menghasilkan bahwa terdapat 3 layanan dengan poin urgensi risiko 4 yakni:</p> <p style="margin-left: 40px;">A. Pelayanan Bandwidth Internet</p> <p style="margin-left: 40px;">B. Pelayanan Domain/Subdomain</p> <p style="margin-left: 40px;">C. Pelayanan Pertemuan Virtual</p> <p>dari ketiga layanan tersebut, mana kah layanan yang akan diprioritaskan untuk ditindaklanjuti dalam manajemen risiko operasional SPBE Layanan Diskominfosanti?</p> | <p>Yang diprioritaskan adalah layanan bandwidth internet sebab dia sebagai pintu masuk untuk mengakses semua layanan yang dioperasikan oleh Diskominfosanti atau dipergunakan oleh SKPD lain.</p> |

**Narasumber,**



**Fransiskus Asisi Wawan Triyudawanto, ST, M.Kom**  
 NIP. 197910052006041011

**Singaraja, 22 April 2024**  
**Peneliti,**



**Vany Adelia Putri**  
 NIM. 2015091027

Narasumber : Luh Putu Adi Ariwati, SE, M.Pd  
 Jabatan : Sekretaris Dinas  
 Instansi : Dinas Komunikasi, Informatika, Persandian dan Statistik  
 Tempat/Tanggal : Singaraja/22 April 2024

| NO. | PERTANYAAN                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | JAWABAN                                                                                                                                                                                                                                                                                                                                                    |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.  | <p>Terkait hasil kuesioner identifikasi layanan risiko milik DiskominfoSanti yang sebelumnya telah didapatkan dari bantuan bagian perencanaan, menghasilkan bahwa terdapat 3 layanan dengan poin urgensi risiko 4 yakni:</p> <p>A. Pelayanan Bandwidth Internet</p> <p>B. Pelayanan Domain/Subdomain</p> <p>C. Pelayanan Pertemuan Virtual</p> <p>dari ketiga layanan tersebut, mana kah layanan yang akan diprioritaskan untuk ditindaklanjuti dalam manajemen risiko operasional SPBE Layanan DiskominfoSanti?</p> | <p>Dari ketiga layanan tersebut, yang paling di prioritaskan adalah Pelayanan Bandwidth Internet sebab layanan tersebut seringkali mengalami gangguan yang tentunya berdampak besar bagi kinerja organisasi DiskominfoSanti bahkan SKPD pengguna layanan tersebut. Jadi, sebagai awal dalam Manajemen Risiko Operasional SPBE Layanan DiskominfoSanti.</p> |

Narasumber,



Luh Putu Adi Ariwati, SE, M.Pd  
 NIP. 198107112001121002

Singaraja. 22 April 2024

Peneliti,



Vany Adelia Putri  
 NIM. 2015091027

Lampiran 12. Data Aset Layanan Bandwidth Internet DiskominfoSanti Kab.  
Buleleng

| SARANA DAN PRASARANA                                                       | KETERANGAN                                         |
|----------------------------------------------------------------------------|----------------------------------------------------|
| Kecepatan Akses Unduh (Mbps atau Gbps)                                     | 2 Gbps                                             |
| Kecepatan Akses Upload (Mbps atau Gbps)                                    | 2 Gbps                                             |
| Akses poin                                                                 | 14 di Dinas Kominfosanti dan 2 di tiap2 SKPD       |
| IP Adress                                                                  | 103.168.29.0/24                                    |
| Provider                                                                   | Dewata telematika dan Biznet                       |
| Topologi Jaringan                                                          | (terlampir)                                        |
| Kebijakan Penggunaan                                                       | Maksimal 10 Mbps per perangkat                     |
| Skema Pembagian Bandwith                                                   | Kecepatan maksimal per SKPD 150 Mbps               |
| Jenis Layanan Bandwith                                                     | Dedicated                                          |
| Pengukuran Bandwith                                                        | Latensi 5 milisecon                                |
| Biaya Operasional :                                                        |                                                    |
| 1. Biaya Perangkat Keras ( <i>Hardware Cost</i> )                          | (termasuk dalam biaya penyedia layanan internet)   |
| 2. Biaya Perangkat Lunak ( <i>Software Costs</i> )                         | -                                                  |
| 3. Biaya Infrastruktur                                                     | - (termasuk dalam biaya penyedia layanan internet) |
| 4. Biaya Pekerjaan (Misal: Tenaga Kerja untuk instalasi, konfigurasi, dll) | -                                                  |

| <b>SARANA DAN PRASARANA</b>                | <b>KETERANGAN</b>                  |                                             |
|--------------------------------------------|------------------------------------|---------------------------------------------|
| 5. Biaya Penyedia Layanan Internet         | Rp. 3.500.496.000                  |                                             |
| 6. Biaya Penyimpanan dan Pemeliharaan      | -                                  |                                             |
| 7. Biaya Cadangan dan Kontingensi          | —                                  |                                             |
| Perangkat Keras<br>( <i>Hardware</i> )     | <b>JUMLAH</b>                      | <b>KETERANGAN</b>                           |
|                                            | 1. Router                          | 2 unit di dinas kominfo dan 39 unit di skpd |
|                                            | 2. Switch                          |                                             |
|                                            | 3. Akses Point                     | 14 unit di dinas kominfo                    |
| Perangkat Lunak ( <i>Software</i> )        | <b>JUMLAH</b>                      | <b>KETERANGAN</b>                           |
|                                            | 1. Mikrotik Router OS = 2          | Software pada router                        |
|                                            | 2. Network Monitoring System (NMS) | Aplikasi untuk memonitor jaringan           |
|                                            | 3. Ruijie Cloud                    | Aplikasi untuk control semua akses poin     |
| Infrastruktur (Misal: Kabel, Konektor dll) | <b>JUMLAH</b>                      | <b>KETERANGAN</b>                           |
|                                            | 1. Kabel fiber optik               | Dari dinak kominfo ke skpd                  |
|                                            | 2. Kabel UTP                       | Dari router ke akses poin                   |
|                                            | 3. Konektor rj 45                  |                                             |

### Lampiran 13. Perbup Buleleng Nomor 52 Tahun 2021

- g. melaksanakan pemberdayaan dan penyediaan akses informasi bagi media dan lembaga komunikasi publik;
- h. penyelenggaraan hubungan masyarakat, media dan kemitraan komunitas;
- i. mengevaluasi dan melaporkan pelaksanaan tugasnya kepada atasan; dan
- j. melaksanakan tugas kedinasan lain yang diberikan oleh atasan.

#### 4.3. SUBSTANSI PELIPUTAN DAN DOKUMENTASI

Substansi Peliputan dan Dokumentasi mempunyai tugas dan fungsi :

- a. menyusun rencana kegiatan Substansi Peliputan dan Dokumentasi berdasarkan data dan program Bidang Pengelolaan Komunikasi Publik serta ketentuan Peraturan Perundang-undangan;
- b. memimpin dan mendistribusikan tugas kepada bawahan;
- c. mengevaluasi dan menilai prestasi hasil kerja bawahan;
- d. melakukan kajian terkait pemberian rekomendasi terhadap permohonan perizinan di bidang komunikasi;
- e. melaksanakan peliputan dan pendokumentasian kegiatan Pemerintahan dan pembangunan daerah dalam bentuk tulisan, rekaman audio dan video;
- f. memproses berita hasil liputan untuk ditayangkan pada situs dan media sosial resmi Pemerintah Daerah serta dinas;
- g. menyediakan bahan publikasi bagi pimpinan daerah;
- h. mengemas ulang konten nasional dan membuat konten lokal;
- i. mengevaluasi dan melaporkan pelaksanaan tugasnya kepada atasan; dan
- j. melaksanakan tugas kedinasan lain yang diberikan oleh atasan.

#### 5. BIDANG INFRASTRUKTUR DAN LAYANAN SISTEM PEMERINTAHAN BERBASIS ELEKTRONIK (SPBE)

Bidang Infrastruktur dan Layanan Sistem Pemerintahan Berbasis Elektronik (SPBE) mempunyai tugas dan fungsi :

- a. menyusun rencana kegiatan Bidang Infrastruktur dan Layanan Sistem Pemerintahan Berbasis Elektronik (SPBE), berdasarkan data dan program Dinas Komunikasi, Informatika, Persandian dan Statistik serta ketentuan Peraturan Perundang-undangan;
- b. memimpin dan mendistribusikan tugas kepada bawahan;
- c. mengevaluasi dan menilai prestasi hasil kerja bawahan;
- d. memberikan layanan nama domain dan sub domain bagi lembaga, pelayanan publik dan kegiatan Provinsi/Kabupaten/Kota;
- e. memfasilitasi dan melaksanakan koordinasi layanan pengembangan intranet dan penggunaan akses internet;
- f. memfasilitasi dan melaksanakan koordinasi layanan interkoneksi jaringan Intra Pemerintah;
- g. mengevaluasi dan melaporkan pelaksanaan tugasnya kepada atasan; dan
- h. melaksanakan tugas kedinasan lain yang diberikan oleh atasan.

## Lampiran 14. Renstra DiskominfoSanti Kab. Buleleng Tahun 2023-2026

Tabel 4.1  
Tujuan dan Sasaran Jangka Menengah  
Pelayanan Dinas Komunikasi, Informatika, Persandian dan Statistik Kabupaten Buleleng

| NO | TUJUAN                                                                                                                  | SASARAN                                                                     | INDIKATOR SASARAN                                           | TARGET KINERJA SASARAN PADA TAHUN KE- |         |         |         |
|----|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|-------------------------------------------------------------|---------------------------------------|---------|---------|---------|
|    |                                                                                                                         |                                                                             |                                                             | 1                                     | 2       | 3       | 4       |
| 1  | 2                                                                                                                       | 3                                                                           | 4                                                           | 5                                     | 6       | 7       | 8       |
| 1. | Meningkatnya layanan pemerintahan dibidang komunikasi, informatika, persandian serta statistik yang efektif dan efisien | 1. Terwujudnya pelayanan informasi publik sesuai standar                    | Persentase layanan informasi publik yang sesuai standar     | 100,00%                               | 100,00% | 100,00% | 100,00% |
|    |                                                                                                                         | 2. Terwujudnya e-government Pemkab Buleleng sesuai dengan ketentuan         | Predikat Sistem Pemerintahan Berbasis Elektronik (SPBE)     | Baik                                  | Baik    | Baik    | Baik    |
|    |                                                                                                                         | 3. Terwujudnya peningkatan pelayanan kebutuhan data sektoral sesuai standar | Persentase peningkatan layanan data sektoral sesuai standar | 10,00%                                | 11,36%  | 12,24%  | 13,64%  |
|    |                                                                                                                         | 4. Terwujudnya pengamanan informasi sesuai standar                          | Persentase pengamanan persandian sesuai standar             | 100,00%                               | 100,00% | 100,00% | 100,00% |

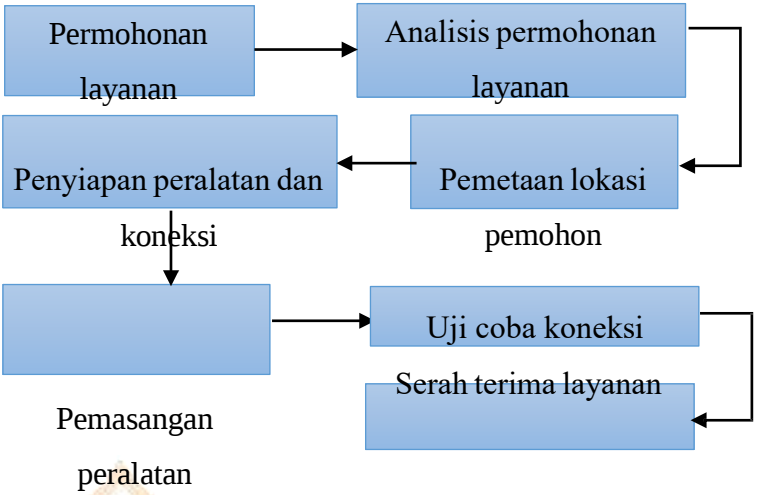
Renstra Dinas Komunikasi, Informatika, Persandian dan Statistik Kabupaten Buleleng - Tahun 2023-2026

Hal: 47



Lampiran 15. Peraturan Perundang-Undangan Layanan Bandwith Internet

|                                                                                                                            |                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  <p>Pemerintah Kabupaten<br/>Buleleng</p> | <p>STANDAR PELAYANAN</p> <p>DINAS KOMUNIKASI, INFORMATIKA,<br/>PERSANDIAN, DAN STATISTIK</p> <p>Unit Kerja: Infrastruktur dan Layanan SPBE</p> |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| A                                                                                                                          | Pelayanan Bandwidth Internet                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| 1                                                                                                                          | Dasar Hukum                                                                                                                                    | <p>: 1. Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik;</p> <p>2. Undang-Undang Nomor 25 Tahun 2009 tentang Pelayanan Publik;</p> <p>3. Undang-Undang Republik Indonesia Nomor: 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi Dan Transaksi Elektronik;</p> <p>4. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik</p> |
| 2                                                                                                                          | Persyaratan Pelayanan                                                                                                                          | <p>: 1. Yang dapat mengajukan adalah instansi pemerintah</p> <p>2. Permohonan disampaikan secara resmi kepada Kepala Dinas Kominfosanti.</p>                                                                                                                                                                                                                                                                                    |

|   |                                     |                                                                                                                                                                                                                                                                                                                                                                                                                    |
|---|-------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3 | Sistem, Mekanisme dan Prosedur      | :  <pre> graph LR     A[Permohonan layanan] --&gt; B[Analisis permohonan layanan]     B --&gt; C[Pemetaan lokasi pemohon]     C --&gt; D[Penyiapan peralatan dan koneksi]     D --&gt; E[Pemasangan peralatan]     E --&gt; F[Uji coba koneksi]     F --&gt; G[Serah terima layanan]     B --&gt; C     F --&gt; G </pre>        |
| 4 | Jangka Waktu Penyelesaian           | : 2 Hari                                                                                                                                                                                                                                                                                                                                                                                                           |
| 5 | Biaya/ Tarif                        | : Tidak ada                                                                                                                                                                                                                                                                                                                                                                                                        |
| 6 | Produk layanan                      | : 1. Wifi dan koneksi internet                                                                                                                                                                                                                                                                                                                                                                                     |
| 7 | Penanganan Pengaduan                | : 1. Melalui Kotak Saran<br>2. Pada jam Kerja melalui: <ul style="list-style-type: none"> <li>- Datang langsung</li> <li>- Telpon: (0362) 21146</li> <li>- Website: <a href="http://www.kominfosanti.bulelengkab.go.id">www.kominfosanti.bulelengkab.go.id</a></li> <li>- Facebook: <a href="https://www.facebook.com/kominfosanti.bulelengkab/">https://www.facebook.com/kominfosanti.bulelengkab/</a></li> </ul> |
| 8 | Sarana prasarana dan atau fasilitas | : 1. Komputer<br>2. Perangkat wifi<br>3. Jaringan internet                                                                                                                                                                                                                                                                                                                                                         |

Lampiran 16. Hasil Kuesioner Identifikasi Kemungkinan Risiko SPBE pada Layanan Bandwith Internet DiskominfoSanti

Kab. Buleleng

|                          |                                                                      |
|--------------------------|----------------------------------------------------------------------|
| Nama Responden           | : Made Kunayanti, SE, M.A.P                                          |
| Jabatan / NIP (Opsional) | : Kepala Bidang Infrastruktur dan Layanan SPBE / 1980009221999032001 |

*Silakan checklist/centang (✓) pada salah satu kolom dalam Frekuensi Kejadian dan Mohon isikan penyebab terjadinya risiko. Ada pun keterangan penjelas sebagai berikut.*

1. Hampir Tidak Terjadi (HTT) mengindikasikan risiko terjadi 1 kali dalam 1 tahun
2. Jarang Terjadi (JT) mengindikasikan risiko terjadi 2 s/d 5 kali dalam 1 tahun
3. Kadang-Kadang Terjadi (KKT) mengindikasikan risiko terjadi 6 s/d 9 kali dalam 1 tahun
4. Sering Terjadi (ST) mengindikasikan risiko terjadi 10 s/d 12 kali dalam 1 tahun
5. Hampir Pasti Terjadi (HPT) mengindikasikan risiko terjadi lebih dari 12 kali dalam 1 tahun

| No.                                                      | RISIKO                                                              | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|----------------------------------------------------------|---------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|                                                          |                                                                     | HTT                                    | JT  | KKT | ST    | HPT |               |
|                                                          |                                                                     | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 06. INFORMATION (DATA BREACH: DAMAGE, LEAKAGE AND ACCES) |                                                                     |                                        |     |     |       |     |               |
| 1.                                                       | Data hilang atau rusak                                              | ✓                                      |     |     |       |     |               |
| 2.                                                       | Kegagalan <i>backup</i> data                                        | ✓                                      |     |     |       |     |               |
| 3.                                                       | Serangan manusia ( <i>hacker, cracker</i> )                         | ✓                                      |     |     |       |     |               |
| 4.                                                       | Kebocoran data organisasi                                           | ✓                                      |     |     |       |     |               |
| 5.                                                       | Organisasi mengalami limpahan data tetapi tidak mampu mengolah data | ✓                                      |     |     |       |     |               |

| No. | RISIKO                                                                                                                                    | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|     |                                                                                                                                           | HTT                                    | JT  | KKT | ST    | HPT |               |
|     |                                                                                                                                           | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 14. | Tidak tersedia pemadam api (Contoh: NOVEC) dalam ruangan <i>server</i>                                                                    | √                                      |     |     |       |     |               |
| 15. | Tidak ada tim monitoring khusus <i>server</i>                                                                                             | ✓                                      |     |     |       |     |               |
| 16. | <i>Server</i> mengalami <i>down</i>                                                                                                       | √                                      |     |     |       |     |               |
| 17. | Kondisi <i>server</i> yang tidak memadai/tidak layak (Contoh: <i>Server</i> usang)                                                        | √                                      |     |     |       |     |               |
| 18. | Perangkat mengalami <i>overheat</i> dan <i>overload</i>                                                                                   | ✓                                      |     |     |       |     |               |
| 19. | Sistem operasi pada <i>server</i> tidak menyediakan <i>interface</i> untuk mengakses dan mengelola <i>server</i> (Contoh: CLI maupun GUI) | ✓                                      |     |     |       |     |               |
| 20. | Tidak melakukan <i>backup data</i> secara berkala atau otomatis                                                                           | ✓                                      |     |     |       |     |               |

| No.                 | RISIKO                                                                      | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|---------------------|-----------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|                     |                                                                             | HTT                                    | JT  | KKT | ST    | HPT |               |
|                     |                                                                             | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 21.                 | <i>Maintenance</i> tidak terjadwal                                          | ✓                                      |     |     |       |     |               |
| 22.                 | <i>Server</i> mengalami serangan (Contoh: Virus)                            | ✓                                      |     |     |       |     |               |
| 23.                 | <i>Data corrupt</i>                                                         | ✓                                      |     |     |       |     |               |
| 24.                 | Tidak melakukan <i>back up</i> data dan <i>system server</i> secara berkala | ✓                                      |     |     |       |     |               |
| 25.                 | Tidak dilakukan kelola hak akses pengguna                                   | ✓                                      |     |     |       |     |               |
| <b>09. SOFTWARE</b> |                                                                             |                                        |     |     |       |     |               |
| 26.                 | Pemakaian <i>software</i> non orisinal                                      | ✓                                      |     |     |       |     |               |
| 27.                 | Dokumentasi atau tata cara penggunaan program / aplikasi tidak lengkap      | ✓                                      |     |     |       |     |               |
| 28.                 | Antar muka ( <i>user interface</i> ) program atau aplikasi susah dipahami   | ✓                                      |     |     |       |     |               |

| No. | RISIKO                                                                                                   | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|-----|----------------------------------------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|     |                                                                                                          | TT                                     | JT  | KT  | ST    | PT  |               |
|     |                                                                                                          | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 29. | Layanan berbasis elektronik yang belum stabil tetapi digunakan                                           | ✓                                      |     |     |       |     |               |
| 30. | Tidak ada sosialisasi dan pelatihan teknis sebelum perangkat lunak digunakan secara massif di organisasi | ✓                                      |     |     |       |     |               |

Responden,



**Made Kunayanti, SE, M.A.P**  
NIP. 198009221555032001

Singaraja, 16 Mei  
Peneliti,

2024



**Vany Adelia Putri**  
NIM. 2015091027

|                          |                                        |
|--------------------------|----------------------------------------|
| Nama Responden           | : Nyoman Budarsa, M.Kom                |
| Jabatan / NIP (Opsional) | : JFT Komputer / NIP. 1982080420091002 |

Silakan *checklist/centang* (✓) pada salah satu kolom dalam Frekuensi Kejadian dan Mohon isikan penyebab terjadinya risiko dengan keterangan sebagai berikut.

- Hampir Tidak Terjadi (HTT) mengindikasikan risiko terjadi 1 kali dalam 1 tahun
- Jarang Terjadi (JT) mengindikasikan risiko terjadi 2 s/d 5 kali dalam 1 tahun
- Kadang Terjadi (KT) mengindikasikan risiko terjadi 6 s/d 9 kali dalam 1 tahun
- Sering Terjadi (ST) mengindikasikan risiko terjadi 10 s/d 12 kali dalam 1 tahun
- Pasti Terjadi (PT) mengindikasikan risiko terjadi lebih dari 12 kali dalam 1 tahun

| No.                                                      | RISIKO                                      | FREKUENSI KEJADIAN (KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO      |
|----------------------------------------------------------|---------------------------------------------|-------------------------------------|-----|-----|-------|-----|--------------------|
|                                                          |                                             | HTT                                 | JT  | KT  | ST    | PT  |                    |
|                                                          |                                             | 1                                   | 2-5 | 6-9 | 10-12 | >12 |                    |
| 06. INFORMATION (DATA BREACH: DAMAGE, LEAKAGE AND ACCES) |                                             |                                     |     |     |       |     |                    |
| 1.                                                       | Data hilang atau rusak                      |                                     | ✓   |     |       |     | Hardisk Error      |
| 2.                                                       | Kegagalan <i>backup</i> data                |                                     | ✓   |     |       |     | Konfigurasi Backup |
| 3.                                                       | Serangan manusia ( <i>hacker, cracker</i> ) |                                     |     | ✓   |       |     | Update aplikasi    |
| 4.                                                       | Kebocoran data organisasi                   | ✓                                   |     |     |       |     | Data di server     |

|                          |                                        |
|--------------------------|----------------------------------------|
| Nama Responden           | : Nyoman Budarsa, M.Kom                |
| Jabatan / NIP (Opsional) | : JFT Komputer / NIP. 1982080420091002 |

Silakan checklist/centang (✓) pada salah satu kolom dalam Frekuensi Kejadian dan Mohon isikan penyebab terjadinya risiko dengan keterangan sebagai berikut.

- Hampir Tidak Terjadi (HTT) mengindikasikan risiko terjadi 1 kali dalam 1 tahun
- Jarang Terjadi (JT) mengindikasikan risiko terjadi 2 s/d 5 kali dalam 1 tahun
- Kadang Terjadi (KT) mengindikasikan risiko terjadi 6 s/d 9 kali dalam 1 tahun
- Sering Terjadi (ST) mengindikasikan risiko terjadi 10 s/d 12 kali dalam 1 tahun
- Pasti Terjadi (PT) mengindikasikan risiko terjadi lebih dari 12 kali dalam 1 tahun

| No.                                                      | RISIKO                                      | FREKUENSI KEJADIAN (KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO             |
|----------------------------------------------------------|---------------------------------------------|-------------------------------------|-----|-----|-------|-----|---------------------------|
|                                                          |                                             | HTT                                 | JT  | KT  | ST    | PT  |                           |
|                                                          |                                             | 1                                   | 2-5 | 6-9 | 10-12 | >12 |                           |
| 06. INFORMATION (DATA BREACH: DAMAGE, LEAKAGE AND ACCES) |                                             |                                     |     |     |       |     |                           |
| 1.                                                       | Data hilang atau rusak                      |                                     | ✓   |     |       |     | Hardisk Error             |
| 2.                                                       | Kegagalan <i>backup</i> data                |                                     | ✓   |     |       |     | Konfigurasi <i>Backup</i> |
| 3.                                                       | Serangan manusia ( <i>hacker, cracker</i> ) |                                     |     | ✓   |       |     | Update aplikasi           |
| 4.                                                       | Kebocoran data organisasi                   | ✓                                   |     |     |       |     | Data di server            |

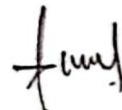
| No.                                                                                                                                          | RISIKO                                                                                                      | FREKUENSI KEJADIAN (KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO        |
|----------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|-------------------------------------|-----|-----|-------|-----|----------------------|
|                                                                                                                                              |                                                                                                             | HTT                                 | JT  | KT  | ST    | PT  |                      |
|                                                                                                                                              |                                                                                                             | 1                                   | 2-5 | 6-9 | 10-12 | >12 |                      |
| 5.                                                                                                                                           | Organisasi mengalami limpahan data tetapi tidak mampu mengolah data                                         |                                     | ✓   |     |       |     |                      |
| <b>08. INFRASTRUCTURE (HARDWARE, OPERATING SYSTEM AND CONTROLLING TECHNOLOGY) (SELECTION/IMPLEMENTATION, OPERATIONS AND DECOMMISSIONING)</b> |                                                                                                             |                                     |     |     |       |     |                      |
| 6.                                                                                                                                           | Kerusakan <i>hardware</i>                                                                                   |                                     |     | ✓   |       |     | UPS, Router          |
| 7.                                                                                                                                           | Gangguan Koneksi Internet                                                                                   |                                     |     | ✓   |       |     | ISP atau kabel       |
| 8.                                                                                                                                           | Koneksi jaringan terputus                                                                                   |                                     |     | ✓   |       |     | ISP atau kabel putus |
| 9.                                                                                                                                           | Listrik padam tiba-tiba                                                                                     |                                     | ✓   |     |       |     | PLN                  |
| 10.                                                                                                                                          | Ruangan <i>server</i> tidak menggunakan PAC ( <i>Precision Air Conditioning</i> )                           | ✓                                   |     |     |       |     | Sudah pakai PAC      |
| 11.                                                                                                                                          | <i>Server</i> mengalami kendala karena tidak adanya sumber energi listrik Cadangan (Contoh: UPS dan Genset) |                                     | ✓   |     |       |     | Kendala UPS          |

| No. | RISIKO                                                                                                                                    | FREKUENSI KEJADIAN (KALI<br>PER TAHUN) |     |     |       |     | SUMBER RISIKO                  |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|--------------------------------|
|     |                                                                                                                                           | HTT                                    | JT  | KT  | ST    | PT  |                                |
|     |                                                                                                                                           | 1                                      | 2-5 | 6-9 | 10-12 | >12 |                                |
| 12. | Akses masuk ke dalam ruangan <i>server</i> tidak dicatat dan tidak dibatasi                                                               |                                        | ✓   |     |       |     | Tata kelola data <i>center</i> |
| 13. | Ruangan <i>server</i> tidak dipantau melalui CCTV                                                                                         | ✓                                      |     |     |       |     | Sudah ada CCTV                 |
| 14. | Tidak tersedia pemadam api (Contoh: NOVEC) dalam ruangan <i>server</i>                                                                    | ✓                                      |     |     |       |     | Sudah ada apar                 |
| 15. | Tidak ada tim monitoring khusus <i>server</i>                                                                                             | ✓                                      |     |     |       |     | Ada                            |
| 16. | <i>Server</i> mengalami <i>down</i>                                                                                                       |                                        |     | ✓   |       |     | Hardware / Konfigurasi         |
| 17. | Kondisi <i>server</i> yang tidak memadai/tidak layak (Contoh: <i>Server</i> usang)                                                        |                                        | ✓   |     |       |     | Server lambat                  |
| 18. | Perangkat mengalami <i>overheat</i> dan <i>overload</i>                                                                                   |                                        | ✓   |     |       |     | Server Hardware                |
| 19. | Sistem operasi pada <i>server</i> tidak menyediakan <i>interface</i> untuk mengakses dan mengelola <i>server</i> (Contoh: CLI maupun GUI) | ✓                                      |     |     |       |     |                                |

| No.                 | RISIKO                                                                      | FREKUENSI KEJADIAN (KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO            |
|---------------------|-----------------------------------------------------------------------------|-------------------------------------|-----|-----|-------|-----|--------------------------|
|                     |                                                                             | HTT                                 | JT  | KT  | ST    | PT  |                          |
|                     |                                                                             | 1                                   | 2-5 | 6-9 | 10-12 | >12 |                          |
| 20.                 | Tidak melakukan <i>backup data</i> secara berkala atau otomatis             |                                     | ✓   |     |       |     | Kekurangan NAS           |
| 21.                 | <i>Maintenance</i> tidak terjadwal                                          |                                     | ✓   |     |       |     | Tata kelola              |
| 22.                 | <i>Server</i> mengalami serangan (Contoh: Virus)                            |                                     | ✓   |     |       |     | <i>Deface website</i>    |
| 23.                 | <i>Data corrupt</i>                                                         | ✓                                   |     |     |       |     | Kerusakan <i>hardisk</i> |
| 24.                 | Tidak melakukan <i>back up data</i> dan <i>system server</i> secara berkala |                                     | ✓   |     |       |     |                          |
| 25.                 | Tidak dilakukan kelola hak akses pengguna                                   |                                     | ✓   |     |       |     | Tata kelola server       |
| <b>09. SOFTWARE</b> |                                                                             |                                     |     |     |       |     |                          |
| 26.                 | Pemakaian <i>software</i> non orisinal                                      |                                     | ✓   |     |       |     | Kekurangan lisensi       |
| 27.                 | Dokumentasi atau tata cara penggunaan program / aplikasi tidak lengkap      |                                     | ✓   |     |       |     | Proses pengaduan         |

| No. | RISIKO                                                                                                   | FREKUENSI KEJADIAN (KALI<br>PER TAHUN) |     |     |       |     | SUMBER RISIKO                     |
|-----|----------------------------------------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|-----------------------------------|
|     |                                                                                                          | HTT                                    | JT  | KT  | ST    | PT  |                                   |
|     |                                                                                                          | 1                                      | 2-5 | 6-9 | 10-12 | >12 |                                   |
| 28. | Antar muka ( <i>user interface</i> ) program atau aplikasi susah dipahami                                |                                        | ✓   |     |       |     | Aplikasi                          |
| 29. | Layanan berbasis elektronik yang belum stabil tetapi digunakan                                           |                                        | ✓   |     |       |     | Ada aplikasi yang wajib digunakan |
| 30. | Tidak ada sosialisasi dan pelatihan teknis sebelum perangkat lunak digunakan secara massif di organisasi |                                        | ✓   |     |       |     | Aplikasi                          |

Responden,



Nyoman Budarsa, M.Kom  
NIP. 1982080420091002

Singaraja, 22 Mei 2024

Peneliti,



Vany Adelia Putri  
NIM. 2015091027

|                          |                                           |
|--------------------------|-------------------------------------------|
| Nama Responden           | : Angelina Sagita Sastrawan, S.T., M.Kom. |
| Jabatan / NIP (Opsional) | : JFT Komputer / NIP. 198612022009022001  |

*Silakan checklist/centang (✓) pada salah satu kolom dalam Frekuensi Kejadian dan Mohon isikan penyebab terjadinya risiko. Ada pun keterangan penjelas sebagai berikut.*

1. Hampir Tidak Terjadi (HTT) mengindikasikan risiko terjadi 1 kali dalam 1 tahun
2. Jarang Terjadi (JT) mengindikasikan risiko terjadi 2 s/d 5 kali dalam 1 tahun
3. Kadang-Kadang Terjadi (KKT) mengindikasikan risiko terjadi 6 s/d 9 kali dalam 1 tahun
4. Sering Terjadi (ST) mengindikasikan risiko terjadi 10 s/d 12 kali dalam 1 tahun
5. Hampir Pasti Terjadi (HPT) mengindikasikan risiko terjadi lebih dari 12 kali dalam 1 tahun

| No.                                                      | RISIKO                                                              | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|----------------------------------------------------------|---------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|                                                          |                                                                     | HTT                                    | JT  | KKT | ST    | HPT |               |
|                                                          |                                                                     | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 06. INFORMATION (DATA BREACH: DAMAGE, LEAKAGE AND ACCES) |                                                                     |                                        |     |     |       |     |               |
| 1.                                                       | Data hilang atau rusak                                              | ✓                                      |     |     |       |     |               |
| 2.                                                       | Kegagalan <i>backup</i> data                                        | ✓                                      |     |     |       |     |               |
| 3.                                                       | Serangan manusia ( <i>hacker, cracker</i> )                         | ✓                                      |     |     |       |     |               |
| 4.                                                       | Kebocoran data organisasi                                           | ✓                                      |     |     |       |     |               |
| 5.                                                       | Organisasi mengalami limpahan data tetapi tidak mampu mengolah data | ✓                                      |     |     |       |     |               |

| No.                                                                                                                                       | RISIKO                                                                                                      | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO                                                    |
|-------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|------------------------------------------------------------------|
|                                                                                                                                           |                                                                                                             | HTT                                    | JT  | KKT | ST    | HPT |                                                                  |
|                                                                                                                                           |                                                                                                             | 1                                      | 2-5 | 6-9 | 10-12 | >12 |                                                                  |
| 08. INFRASTRUCTURE (HARDWARE, OPERATING SYSTEM AND CONTROLLING TECHNOLOGY)<br>(SELECTION/ IMPLEMENTATION, OPERATIONS AND DECOMMISSIONING) |                                                                                                             |                                        |     |     |       |     |                                                                  |
| 6.                                                                                                                                        | Kerusakan <i>hardware</i>                                                                                   | ✓                                      |     |     |       |     |                                                                  |
| 7.                                                                                                                                        | Gangguan Koneksi Internet                                                                                   |                                        | ✓   |     |       |     | Hujan deras mengakibatkan infrastruktur terganggu (bencana alam) |
| 8.                                                                                                                                        | Koneksi jaringan terputus                                                                                   |                                        | ✓   |     |       |     | Kabel jaringan putus karena beberapa faktor                      |
| 9.                                                                                                                                        | Listrik padam tiba-tiba                                                                                     |                                        | ✓   |     |       |     |                                                                  |
| 10.                                                                                                                                       | Ruangan <i>server</i> tidak menggunakan PAC ( <i>Precision Air Conditioning</i> )                           | ✓                                      |     |     |       |     |                                                                  |
| 11.                                                                                                                                       | <i>Server</i> mengalami kendala karena tidak adanya sumber energi listrik Cadangan (Contoh: UPS dan Genset) | ✓                                      |     |     |       |     |                                                                  |
| 12.                                                                                                                                       | Akses masuk ke dalam ruangan <i>server</i> tidak dicatat dan tidak dibatasi                                 | ✓                                      |     |     |       |     |                                                                  |
| 13.                                                                                                                                       | Ruangan <i>server</i> tidak dipantau melalui CCTV                                                           | ✓                                      |     |     |       |     |                                                                  |

| No. | RISIKO                                                                                                                                    | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO                                                                                  |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|------------------------------------------------------------------------------------------------|
|     |                                                                                                                                           | HTT                                    | JT  | KKT | ST    | HPT |                                                                                                |
|     |                                                                                                                                           | 1                                      | 2-5 | 6-9 | 10-12 | >12 |                                                                                                |
| 14. | Tidak tersedia pemadam api (Contoh: NOVEC) dalam ruangan <i>server</i>                                                                    | ✓                                      |     |     |       |     |                                                                                                |
| 15. | Tidak ada tim monitoring khusus <i>server</i>                                                                                             | ✓                                      |     |     |       |     |                                                                                                |
| 16. | <i>Server</i> mengalami <i>down</i>                                                                                                       |                                        | ✓   |     |       |     | Pengelola aplikasi pada <i>server</i> dari pihak ke-3 yang kurang koordinasi dgn komprofasanti |
| 17. | Kondisi <i>server</i> yang tidak memadai/tidak layak (Contoh: <i>Server</i> usang)                                                        | ✓                                      |     |     |       |     |                                                                                                |
| 18. | Perangkat mengalami <i>overheat</i> dan <i>overload</i>                                                                                   | ✓                                      |     |     |       |     |                                                                                                |
| 19. | Sistem operasi pada <i>server</i> tidak menyediakan <i>interface</i> untuk mengakses dan mengelola <i>server</i> (Contoh: CLI maupun GUI) | ✓                                      |     |     |       |     |                                                                                                |
| 20. | Tidak melakukan <i>backup data</i> secara berkala atau otomatis                                                                           | ✓                                      |     |     |       |     |                                                                                                |

| No.                 | RISIKO                                                                      | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|---------------------|-----------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|                     |                                                                             | HTT                                    | JT  | KKT | ST    | HPT |               |
|                     |                                                                             | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 21.                 | <i>Maintenance</i> tidak terjadwal                                          | ✓                                      |     |     |       |     |               |
| 22.                 | <i>Server</i> mengalami serangan (Contoh: Virus)                            | ✓                                      |     |     |       |     |               |
| 23.                 | <i>Data corrupt</i>                                                         | ✓                                      |     |     |       |     |               |
| 24.                 | Tidak melakukan <i>back up</i> data dan <i>system server</i> secara berkala | ✓                                      |     |     |       |     |               |
| 25.                 | Tidak dilakukan kelola hak akses pengguna                                   | ✓                                      |     |     |       |     |               |
| <b>09. SOFTWARE</b> |                                                                             |                                        |     |     |       |     |               |
| 26.                 | Pemakaian <i>software</i> non orisinal                                      | ✓                                      |     |     |       |     |               |
| 27.                 | Dokumentasi atau tata cara penggunaan program / aplikasi tidak lengkap      | ✓                                      |     |     |       |     |               |
| 28.                 | Antar muka ( <i>user interface</i> ) program atau aplikasi susah dipahami   | ✓                                      |     |     |       |     |               |

| No. | RISIKO                                                                                                   | FREKUENSI KEJADIAN (KALI<br>PER TAHUN |     |     |       |     | SUMBER RISIKO |
|-----|----------------------------------------------------------------------------------------------------------|---------------------------------------|-----|-----|-------|-----|---------------|
|     |                                                                                                          | HTT                                   | JT  | KKT | ST    | HPT |               |
|     |                                                                                                          | 1                                     | 2-5 | 6-9 | 10-12 | >12 |               |
| 29. | Layanan berbasis elektronik yang belum stabil tetapi digunakan                                           | ✓                                     |     |     |       |     |               |
| 30. | Tidak ada sosialisasi dan pelatihan teknis sebelum perangkat lunak digunakan secara massif di organisasi | ✓                                     |     |     |       |     |               |

Responden,



Angelina Sagita Sastrawan, S.T., M.Kom.

NIP. 198612022009022001

Singaraja, 16 Mei 2024

Peneliti,



Vany Adelia Putri

|                          |                                                      |
|--------------------------|------------------------------------------------------|
| Nama Responden           | : Gede Adi Widiastawa, SE.                           |
| Jabatan / NIP (Opsional) | : Jasa Tenaga Teknisi atau Tenaga Teknis Lainnya / - |

*Silakan checklist/centang (✓) pada salah satu kolom dalam Frekuensi Kejadian dan Mohon isikan penyebab terjadinya risiko. Ada pun keterangan penjelas sebagai berikut.*

1. Hampir Tidak Terjadi (HTT) mengindikasikan risiko terjadi 1 kali dalam 1 tahun
2. Jarang Terjadi (JT) mengindikasikan risiko terjadi 2 s/d 5 kali dalam 1 tahun
3. Kadang-Kadang Terjadi (KKT) mengindikasikan risiko terjadi 6 s/d 9 kali dalam 1 tahun
4. Sering Terjadi (ST) mengindikasikan risiko terjadi 10 s/d 12 kali dalam 1 tahun
5. Hampir Pasti Terjadi (HPT) mengindikasikan risiko terjadi lebih dari 12 kali dalam 1 tahun

| No.                                                      | RISIKO                                                              | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|----------------------------------------------------------|---------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|                                                          |                                                                     | HTT                                    | JT  | KKT | ST    | HPT |               |
|                                                          |                                                                     | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 06. INFORMATION (DATA BREACH: DAMAGE, LEAKAGE AND ACCES) |                                                                     |                                        |     |     |       |     |               |
| 1.                                                       | Data hilang atau rusak                                              | ✓                                      |     |     |       |     |               |
| 2.                                                       | Kegagalan <i>backup</i> data                                        | ✓                                      |     |     |       |     |               |
| 3.                                                       | Serangan manusia ( <i>hacker, cracker</i> )                         |                                        | ✓   |     |       |     |               |
| 4.                                                       | Kebocoran data organisasi                                           | ✓                                      |     |     |       |     |               |
| 5.                                                       | Organisasi mengalami limpahan data tetapi tidak mampu mengolah data | ✓                                      |     |     |       |     |               |

| No.                                                                                                                                       | RISIKO                                                                                                      | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|-------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|                                                                                                                                           |                                                                                                             | HTT                                    | JT  | KKT | ST    | HPT |               |
|                                                                                                                                           |                                                                                                             | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 08. INFRASTRUCTURE (HARDWARE, OPERATING SYSTEM AND CONTROLLING TECHNOLOGY)<br>(SELECTION/ IMPLEMENTATION, OPERATIONS AND DECOMMISSIONING) |                                                                                                             |                                        |     |     |       |     |               |
| 6.                                                                                                                                        | Kerusakan <i>hardware</i>                                                                                   |                                        | ✓   |     |       |     |               |
| 7.                                                                                                                                        | Gangguan Koneksi Internet                                                                                   |                                        | ✓   |     |       |     |               |
| 8.                                                                                                                                        | Koneksi jaringan terputus                                                                                   | ✓                                      |     |     |       |     |               |
| 9.                                                                                                                                        | Listrik padam tiba-tiba                                                                                     |                                        | ✓   |     |       |     |               |
| 10.                                                                                                                                       | Ruangan <i>server</i> tidak menggunakan PAC ( <i>Precision Air Conditioning</i> )                           | ✓                                      |     |     |       |     |               |
| 11.                                                                                                                                       | <i>Server</i> mengalami kendala karena tidak adanya sumber energi listrik Cadangan (Contoh: UPS dan Genset) | ✓<br>✓<br>✓                            |     |     |       |     |               |
| 12.                                                                                                                                       | Akses masuk ke dalam ruangan <i>server</i> tidak dicatat dan tidak dibatasi                                 |                                        | ✓   |     |       |     |               |
| 13.                                                                                                                                       | Ruangan <i>server</i> tidak dipantau melalui CCTV                                                           | ✓                                      |     |     |       |     |               |

| No. | RISIKO                                                                                                                                    | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|     |                                                                                                                                           | HTT                                    | JT  | KKT | ST    | HPT |               |
|     |                                                                                                                                           | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 14. | Tidak tersedia pemadam api (Contoh: NOVEC) dalam ruangan <i>server</i>                                                                    | ✓                                      |     |     |       |     |               |
| 15. | Tidak ada tim monitoring khusus <i>server</i>                                                                                             | ✓                                      |     |     |       |     |               |
| 16. | <i>Server</i> mengalami <i>down</i>                                                                                                       | ✓                                      |     |     |       |     |               |
| 17. | Kondisi <i>server</i> yang tidak memadai/tidak layak (Contoh: <i>Server</i> usang)                                                        | ✓                                      |     |     |       |     |               |
| 18. | Perangkat mengalami <i>overheat</i> dan <i>overload</i>                                                                                   | ✓                                      |     |     |       |     |               |
| 19. | Sistem operasi pada <i>server</i> tidak menyediakan <i>interface</i> untuk mengakses dan mengelola <i>server</i> (Contoh: CLI maupun GUI) | ✓                                      |     |     |       |     |               |
| 20. | Tidak melakukan <i>backup data</i> secara berkala atau otomatis                                                                           | ✓                                      |     |     |       |     |               |

| No.                 | RISIKO                                                                      | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|---------------------|-----------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|                     |                                                                             | HTT                                    | JT  | KKT | ST    | HPT |               |
|                     |                                                                             | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 21.                 | <i>Maintenance</i> tidak terjadwal                                          |                                        | ✓   |     |       |     |               |
| 22.                 | <i>Server</i> mengalami serangan (Contoh: Virus)                            |                                        | ✓   |     |       |     |               |
| 23.                 | <i>Data corrupt</i>                                                         |                                        | ✓   |     |       |     |               |
| 24.                 | Tidak melakukan <i>back up</i> data dan <i>system server</i> secara berkala |                                        | ✓   |     |       |     |               |
| 25.                 | Tidak dilakukan kelola hak akses pengguna                                   | ✓                                      |     |     |       |     |               |
| <b>09. SOFTWARE</b> |                                                                             |                                        |     |     |       |     |               |
| 26.                 | Pemakaian <i>software</i> non orisinal                                      | ✓                                      |     |     |       |     |               |
| 27.                 | Dokumentasi atau tata cara penggunaan program / aplikasi tidak lengkap      | ✓                                      | ✓   |     |       |     |               |
| 28.                 | Antar muka ( <i>user interface</i> ) program atau aplikasi susah dipahami   | ✓                                      |     |     |       |     |               |

| No. | RISIKO                                                                                                   | FREKUENSI KEJADIAN (KALI<br>PER TAHUN |     |     |       |     | SUMBER RISIKO |
|-----|----------------------------------------------------------------------------------------------------------|---------------------------------------|-----|-----|-------|-----|---------------|
|     |                                                                                                          | HTT                                   | JT  | KKT | ST    | HPT |               |
|     |                                                                                                          | 1                                     | 2-5 | 6-9 | 10-12 | >12 |               |
| 29. | Layanan berbasis elektronik yang belum stabil tetapi digunakan                                           |                                       | ✓   |     |       |     |               |
| 30. | Tidak ada sosialisasi dan pelatihan teknis sebelum perangkat lunak digunakan secara massif di organisasi | ✓                                     |     |     |       |     |               |

Responden,



Gede Adi Widiastawa, SE.

Singaraja, 21 Mei 2024

Peneliti,



Vany Adelia Putri

|                          |                                                      |
|--------------------------|------------------------------------------------------|
| Nama Responden           | : Kadek Adi Suartawan, SE.                           |
| Jabatan / NIP (Opsional) | : Jasa Tenaga Teknisi atau Tenaga Teknis Lainnya / - |

*Silakan checklist/centang (✓) pada salah satu kolom dalam Frekuensi Kejadian dan Mohon isikan penyebab terjadinya risiko. Ada pun keterangan penjelas sebagai berikut.*

1. Hampir Tidak Terjadi (HTT) mengindikasikan risiko terjadi 1 kali dalam 1 tahun
2. Jarang Terjadi (JT) mengindikasikan risiko terjadi 2 s/d 5 kali dalam 1 tahun
3. Kadang-Kadang Terjadi (KKT) mengindikasikan risiko terjadi 6 s/d 9 kali dalam 1 tahun
4. Sering Terjadi (ST) mengindikasikan risiko terjadi 10 s/d 12 kali dalam 1 tahun
5. Hampir Pasti Terjadi (HPT) mengindikasikan risiko terjadi lebih dari 12 kali dalam 1 tahun

| No.                                                      | RISIKO                                                              | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|----------------------------------------------------------|---------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|                                                          |                                                                     | HTT                                    | JT  | KKT | ST    | HPT |               |
|                                                          |                                                                     | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 06. INFORMATION (DATA BREACH: DAMAGE, LEAKAGE AND ACCES) |                                                                     |                                        |     |     |       |     |               |
| 1.                                                       | Data hilang atau rusak                                              | ✓                                      | .   |     |       |     |               |
| 2.                                                       | Kegagalan <i>backup</i> data                                        | ✓                                      |     |     |       |     |               |
| 3.                                                       | Serangan manusia ( <i>hacker, cracker</i> )                         |                                        | ✓   |     |       |     |               |
| 4.                                                       | Kebocoran data organisasi                                           | ✓                                      |     |     |       |     |               |
| 5.                                                       | Organisasi mengalami limpahan data tetapi tidak mampu mengolah data | ✓                                      |     |     |       |     |               |

| No.                                                                                                                                                    | RISIKO                                                                                                      | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|--------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|                                                                                                                                                        |                                                                                                             | HTT                                    | JT  | KKT | ST    | HPT |               |
|                                                                                                                                                        |                                                                                                             | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| <b>18. INFRASTRUCTURE (HARDWARE, OPERATING SYSTEM AND CONTROLLING TECHNOLOGY)</b><br><b>(SELECTION IMPLEMENTATION, OPERATIONS AND DECOMMISSIONING)</b> |                                                                                                             |                                        |     |     |       |     |               |
| 6.                                                                                                                                                     | Kerusakan <i>hardware</i>                                                                                   |                                        | ✓   |     |       |     |               |
| 7.                                                                                                                                                     | Gangguan Koneksi Internet                                                                                   |                                        | ✓   |     |       |     |               |
| 8.                                                                                                                                                     | Koneksi jaringan terputus                                                                                   | ✓                                      |     |     |       |     |               |
| 9.                                                                                                                                                     | Listrik padam tiba-tiba                                                                                     |                                        | ✓   |     |       |     |               |
| 10.                                                                                                                                                    | Ruangan <i>server</i> tidak menggunakan PAC ( <i>Precision Air Conditioning</i> )                           | ✓                                      |     |     |       |     |               |
| 11.                                                                                                                                                    | <i>Server</i> mengalami kendala karena tidak adanya sumber energi listrik Cadangan (Contoh: UPS dan Genset) | ✓                                      |     |     |       |     |               |
| 12.                                                                                                                                                    | Akses masuk ke dalam ruangan <i>server</i> tidak dicatat dan tidak dibatasi                                 | ✓                                      |     |     |       |     |               |
| 13.                                                                                                                                                    | Ruangan <i>server</i> tidak dipantau melalui CCTV                                                           | ✓                                      |     |     |       |     |               |

| No. | RISIKO                                                                                                                                    | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|     |                                                                                                                                           | HTT                                    | JT  | KKT | ST    | HPT |               |
|     |                                                                                                                                           | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 14. | Tidak tersedia pemadam api (Contoh: NOVEC) dalam ruangan <i>server</i>                                                                    | ✓                                      |     |     |       |     |               |
| 15. | Tidak ada tim monitoring khusus <i>server</i>                                                                                             | ✓                                      |     |     |       |     |               |
| 16. | <i>Server</i> mengalami <i>down</i>                                                                                                       | ✓                                      |     |     |       |     |               |
| 17. | Kondisi <i>server</i> yang tidak memadai/tidak layak (Contoh: <i>Server</i> usang)                                                        | ✓                                      |     |     |       |     |               |
| 18. | Perangkat mengalami <i>overheat</i> dan <i>overload</i>                                                                                   | ✓                                      |     |     |       |     |               |
| 19. | Sistem operasi pada <i>server</i> tidak menyediakan <i>interface</i> untuk mengakses dan mengelola <i>server</i> (Contoh: CLI maupun GUI) | ✓                                      |     |     |       |     |               |
| 20. | Tidak melakukan <i>backup data</i> secara berkala atau otomatis                                                                           | ✓                                      |     |     |       |     |               |

| No.                 | RISIKO                                                                      | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|---------------------|-----------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|                     |                                                                             | HTT                                    | JT  | KKT | ST    | HPT |               |
|                     |                                                                             | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 21.                 | <i>Maintenance</i> tidak terjadwal                                          |                                        | ✓   |     |       |     |               |
| 22.                 | <i>Server</i> mengalami serangan (Contoh: Virus)                            |                                        | ✓   |     |       |     |               |
| 23.                 | <i>Data corrupt</i>                                                         | ✓                                      |     |     |       |     |               |
| 24.                 | Tidak melakukan <i>back up</i> data dan <i>system server</i> secara berkala |                                        | ✓   |     |       |     |               |
| 25.                 | Tidak dilakukan kelola hak akses pengguna                                   | ✓                                      |     |     |       |     |               |
| <b>09. SOFTWARE</b> |                                                                             |                                        |     |     |       |     |               |
| 26.                 | Pemakaian <i>software</i> non orisinal                                      | ✓                                      |     |     |       |     |               |
| 27.                 | Dokumentasi atau tata cara penggunaan program / aplikasi tidak lengkap      | ✓                                      |     |     |       |     |               |
| 28.                 | Antar muka ( <i>user interface</i> ) program atau aplikasi susah dipahami   | ✓                                      |     |     |       |     |               |

| No. | RISIKO                                                                                                   | FREKUENSI KEJADIAN (KALI<br>PER TAHUN |     |     |       |     | SUMBER RISIKO |
|-----|----------------------------------------------------------------------------------------------------------|---------------------------------------|-----|-----|-------|-----|---------------|
|     |                                                                                                          | HTT                                   | JT  | KKT | ST    | HPT |               |
|     |                                                                                                          | 1                                     | 2-5 | 6-9 | 10-12 | >12 |               |
| 29. | Layanan berbasis elektronik yang belum stabil tetapi digunakan                                           | ✓                                     |     |     |       |     |               |
| 30. | Tidak ada sosialisasi dan pelatihan teknis sebelum perangkat lunak digunakan secara massif di organisasi | ✓                                     |     |     |       |     |               |

Singaraja, 28 Mei 2024

Responden,



Kadek Adi Suartawan

Peneliti,



Vany Adelia Putri

|                          |                                                  |
|--------------------------|--------------------------------------------------|
| Nama Responden           | : Ni Luh Maherni, SE.                            |
| Jabatan / NIP (Opsional) | : Jasa Tenaga Administrasi Umum SKPD Lainnya / - |

Silakan *checklist/centang* (✓) pada salah satu kolom dalam Frekuensi Kejadian dan Mohon isikan penyebab terjadinya risiko. Ada pun keterangan penjelas sebagai berikut.

1. Hampir Tidak Terjadi (HTT) mengindikasikan risiko terjadi 1 kali dalam 1 tahun
2. Jarang Terjadi (JT) mengindikasikan risiko terjadi 2 s/d 5 kali dalam 1 tahun
3. Kadang-Kadang Terjadi (KKT) mengindikasikan risiko terjadi 6 s/d 9 kali dalam 1 tahun
4. Sering Terjadi (ST) mengindikasikan risiko terjadi 10 s/d 12 kali dalam 1 tahun
5. Hampir Pasti Terjadi (HPT) mengindikasikan risiko terjadi lebih dari 12 kali dalam 1 tahun

| No.                                                      | RISIKO                                                              | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|----------------------------------------------------------|---------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|                                                          |                                                                     | HTT                                    | JT  | KKT | ST    | HPT |               |
|                                                          |                                                                     | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 06. INFORMATION (DATA BREACH: DAMAGE, LEAKAGE AND ACCES) |                                                                     |                                        |     |     |       |     |               |
| 1.                                                       | Data hilang atau rusak                                              | ✓                                      |     |     |       |     |               |
| 2.                                                       | Kegagalan <i>backup</i> data                                        | ✓                                      |     |     |       |     |               |
| 3.                                                       | Serangan manusia ( <i>hacker, cracker</i> )                         | ✓                                      |     |     |       |     |               |
| 4.                                                       | Kebocoran data organisasi                                           | ✓                                      |     |     |       |     |               |
| 5.                                                       | Organisasi mengalami limpahan data tetapi tidak mampu mengolah data |                                        | ✓   |     |       |     |               |

| No.                                                                                                                                       | RISIKO                                                                                                      | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|-------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|                                                                                                                                           |                                                                                                             | HTT                                    | JT  | KKT | ST    | HPT |               |
|                                                                                                                                           |                                                                                                             | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 08. INFRASTRUCTURE (HARDWARE, OPERATING SYSTEM AND CONTROLLING TECHNOLOGY)<br>(SELECTION/ IMPLEMENTATION, OPERATIONS AND DECOMMISSIONING) |                                                                                                             |                                        |     |     |       |     |               |
| 6.                                                                                                                                        | Kerusakan <i>hardware</i>                                                                                   | ✓                                      |     |     |       |     |               |
| 7.                                                                                                                                        | Gangguan Koneksi Internet                                                                                   | ✓                                      |     |     |       |     |               |
| 8.                                                                                                                                        | Koneksi jaringan terputus                                                                                   | ✓                                      |     |     |       |     |               |
| 9.                                                                                                                                        | Listrik padam tiba-tiba                                                                                     | ✓                                      |     |     |       |     |               |
| 10.                                                                                                                                       | Ruangan <i>server</i> tidak menggunakan PAC ( <i>Precision Air Conditioning</i> )                           | ✓                                      |     |     |       |     |               |
| 11.                                                                                                                                       | <i>Server</i> mengalami kendala karena tidak adanya sumber energi listrik Cadangan (Contoh: UPS dan Genset) | ✓                                      |     |     |       |     |               |
| 12.                                                                                                                                       | Akses masuk ke dalam ruangan <i>server</i> tidak dicatat dan tidak dibatasi                                 | ✓                                      |     |     |       |     |               |
| 13.                                                                                                                                       | Ruangan <i>server</i> tidak dipantau melalui CCTV                                                           | ✓                                      |     |     |       |     |               |

| No. | RISIKO                                                                                                                                    | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|     |                                                                                                                                           | HTT                                    | JT  | KKT | ST    | HPT |               |
|     |                                                                                                                                           | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 14. | Tidak tersedia pemadam api (Contoh: NOVEC) dalam ruangan <i>server</i>                                                                    | ✓                                      |     |     |       |     |               |
| 15. | Tidak ada tim monitoring khusus <i>server</i>                                                                                             | ✓                                      |     |     |       |     |               |
| 16. | <i>Server</i> mengalami <i>down</i>                                                                                                       | ✓                                      |     |     |       |     |               |
| 17. | Kondisi <i>server</i> yang tidak memadai/tidak layak (Contoh: <i>Server</i> usang)                                                        | ✓                                      |     |     |       |     |               |
| 18. | Perangkat mengalami <i>overheat</i> dan <i>overload</i>                                                                                   | ✓                                      |     |     |       |     |               |
| 19. | Sistem operasi pada <i>server</i> tidak menyediakan <i>interface</i> untuk mengakses dan mengelola <i>server</i> (Contoh: CLI maupun GUI) | ✓                                      |     |     |       |     |               |
| 20. | Tidak melakukan <i>backup data</i> secara berkala atau otomatis                                                                           | ✓                                      |     |     |       |     |               |

| No.                 | RISIKO                                                                      | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|---------------------|-----------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|                     |                                                                             | HTT                                    | JT  | KKT | ST    | HPT |               |
|                     |                                                                             | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 21.                 | <i>Maintenance</i> tidak terjadwal                                          | ✓                                      |     |     |       |     |               |
| 22.                 | <i>Server</i> mengalami serangan (Contoh: Virus)                            | ✓                                      |     |     |       |     |               |
| 23.                 | <i>Data corrupt</i>                                                         | ✓                                      |     |     |       |     |               |
| 24.                 | Tidak melakukan <i>back up</i> data dan <i>system server</i> secara berkala | ✓                                      |     |     |       |     |               |
| 25.                 | Tidak dilakukan kelola hak akses pengguna                                   | ✓                                      |     |     |       |     |               |
| <b>09. SOFTWARE</b> |                                                                             |                                        |     |     |       |     |               |
| 26.                 | Pemakaian <i>software</i> non orisinal                                      | ✓                                      |     |     |       |     |               |
| 27.                 | Dokumentasi atau tata cara penggunaan program / aplikasi tidak lengkap      | ✓                                      |     |     |       |     |               |
| 28.                 | Antar muka ( <i>user interface</i> ) program atau aplikasi susah dipahami   | ✓                                      |     |     |       |     |               |

| No. | RISIKO                                                                                                   | FREKUENSI KEJADIAN (KALI<br>PER TAHUN |     |     |       |     | SUMBER RISIKO |
|-----|----------------------------------------------------------------------------------------------------------|---------------------------------------|-----|-----|-------|-----|---------------|
|     |                                                                                                          | HTT                                   | JT  | KKT | ST    | HPT |               |
|     |                                                                                                          | 1                                     | 2-5 | 6-9 | 10-12 | >12 |               |
| 29. | Layanan berbasis elektronik yang belum stabil tetapi digunakan                                           | ✓                                     |     |     |       |     |               |
| 30. | Tidak ada sosialisasi dan pelatihan teknis sebelum perangkat lunak digunakan secara massif di organisasi | ✓                                     |     |     |       |     |               |

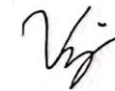
Responden,



Ni Luh Maherni

Singaraja, 21 Mei 2024

Peneliti,



Vany Adelia Putri

|                          |                                             |
|--------------------------|---------------------------------------------|
| Nama Responden           | : Indah Nur Fitriyani, A.Md                 |
| Jabatan / NIP (Opsional) | : Fungsional Umum / NIP. 199601302019022003 |

*Silakan checklist/centang (✓) pada salah satu kolom dalam Frekuensi Kejadian dan Mohon isikan penyebab terjadinya risiko. Ada pun keterangan penjelas sebagai berikut.*

1. Hampir Tidak Terjadi (HTT) mengindikasikan risiko terjadi 1 kali dalam 1 tahun
2. Jarang Terjadi (JT) mengindikasikan risiko terjadi 2 s/d 5 kali dalam 1 tahun
3. Kadang-Kadang Terjadi (KKT) mengindikasikan risiko terjadi 6 s/d 9 kali dalam 1 tahun
4. Sering Terjadi (ST) mengindikasikan risiko terjadi 10 s/d 12 kali dalam 1 tahun
5. Hampir Pasti Terjadi (HPT) mengindikasikan risiko terjadi lebih dari 12 kali dalam 1 tahun

| No.                                                      | RISIKO                                                              | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|----------------------------------------------------------|---------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|                                                          |                                                                     | HTT                                    | JT  | KKT | ST    | HPT |               |
|                                                          |                                                                     | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 06. INFORMATION (DATA BREACH: DAMAGE, LEAKAGE AND ACCES) |                                                                     |                                        |     |     |       |     |               |
| 1.                                                       | Data hilang atau rusak                                              | ✓                                      |     |     |       |     |               |
| 2.                                                       | Kegagalan <i>backup</i> data                                        |                                        | ✓   |     |       |     |               |
| 3.                                                       | Serangan manusia ( <i>hacker, cracker</i> )                         |                                        |     | ✓   |       |     |               |
| 4.                                                       | Kebocoran data organisasi                                           | ✓                                      |     |     |       |     |               |
| 5.                                                       | Organisasi mengalami limpahan data tetapi tidak mampu mengolah data | ✓                                      |     |     |       |     |               |

| No.                                                                                                                                       | RISIKO                                                                                                      | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|-------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|                                                                                                                                           |                                                                                                             | HTT                                    | JT  | KKT | ST    | HPT |               |
|                                                                                                                                           |                                                                                                             | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 08. INFRASTRUCTURE (HARDWARE, OPERATING SYSTEM AND CONTROLLING TECHNOLOGY)<br>(SELECTION/ IMPLEMENTATION, OPERATIONS AND DECOMMISSIONING) |                                                                                                             |                                        |     |     |       |     |               |
| 6.                                                                                                                                        | Kerusakan <i>hardware</i>                                                                                   |                                        | ✓   |     |       |     |               |
| 7.                                                                                                                                        | Gangguan Koneksi Internet                                                                                   |                                        | ✓   |     |       |     |               |
| 8.                                                                                                                                        | Koneksi jaringan terputus                                                                                   | ✓                                      |     |     |       |     |               |
| 9.                                                                                                                                        | Listrik padam tiba-tiba                                                                                     | ✓                                      |     |     |       |     |               |
| 10.                                                                                                                                       | Ruangan <i>server</i> tidak menggunakan PAC ( <i>Precision Air Conditioning</i> )                           | ✓                                      |     |     |       |     |               |
| 11.                                                                                                                                       | <i>Server</i> mengalami kendala karena tidak adanya sumber energi listrik Cadangan (Contoh: UPS dan Genset) | ✓                                      |     |     |       |     |               |
| 12.                                                                                                                                       | Akses masuk ke dalam ruangan <i>server</i> tidak dicatat dan tidak dibatasi                                 | ✓                                      |     |     |       |     |               |
| 13.                                                                                                                                       | Ruangan <i>server</i> tidak dipantau melalui CCTV                                                           | ✓                                      |     |     |       |     |               |

| No. | RISIKO                                                                                                                                    | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|-----|-------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|     |                                                                                                                                           | HTT                                    | JT  | KKT | ST    | HPT |               |
|     |                                                                                                                                           | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 14. | Tidak tersedia pemadam api (Contoh: NOVEC) dalam ruangan <i>server</i>                                                                    | ✓                                      |     |     |       |     |               |
| 15. | Tidak ada tim monitoring khusus <i>server</i>                                                                                             | ✓                                      |     |     |       |     |               |
| 16. | <i>Server</i> mengalami <i>down</i>                                                                                                       | ✓                                      |     |     |       |     |               |
| 17. | Kondisi <i>server</i> yang tidak memadai/tidak layak (Contoh: <i>Server</i> usang)                                                        | ✓                                      |     |     |       |     |               |
| 18. | Perangkat mengalami <i>overheat</i> dan <i>overload</i>                                                                                   | ✓                                      |     |     |       |     |               |
| 19. | Sistem operasi pada <i>server</i> tidak menyediakan <i>interface</i> untuk mengakses dan mengelola <i>server</i> (Contoh: CLI maupun GUI) | ✓                                      |     |     |       |     |               |
| 20. | Tidak melakukan <i>backup data</i> secara berkala atau otomatis                                                                           | ✓                                      |     |     |       |     |               |

| No.                 | RISIKO                                                                      | FREKUENSI KEJADIAN<br>(KALI PER TAHUN) |     |     |       |     | SUMBER RISIKO |
|---------------------|-----------------------------------------------------------------------------|----------------------------------------|-----|-----|-------|-----|---------------|
|                     |                                                                             | HTT                                    | JT  | KKT | ST    | HPT |               |
|                     |                                                                             | 1                                      | 2-5 | 6-9 | 10-12 | >12 |               |
| 21.                 | <i>Maintenance</i> tidak terjadwal                                          | ✓                                      |     |     |       |     |               |
| 22.                 | <i>Server</i> mengalami serangan (Contoh: Virus)                            |                                        | ✓   |     |       |     |               |
| 23.                 | <i>Data corrupt</i>                                                         | ✓                                      |     |     |       |     |               |
| 24.                 | Tidak melakukan <i>back up</i> data dan <i>system server</i> secara berkala | ✓                                      |     |     |       |     |               |
| 25.                 | Tidak dilakukan kelola hak akses pengguna                                   | ✓                                      |     |     |       |     |               |
| <b>09. SOFTWARE</b> |                                                                             |                                        |     |     |       |     |               |
| 26.                 | Pemakaian <i>software</i> non orisinal                                      | ✓                                      |     |     |       |     |               |
| 27.                 | Dokumentasi atau tata cara penggunaan program / aplikasi tidak lengkap      | ✓                                      |     |     |       |     |               |
| 28.                 | Antar muka ( <i>user interface</i> ) program atau aplikasi susah dipahami   | ✓                                      |     |     |       |     |               |

| No. | RISIKO                                                                                                   | FREKUENSI KEJADIAN (KALI<br>PER TAHUN |     |     |       |     | SUMBER RISIKO |
|-----|----------------------------------------------------------------------------------------------------------|---------------------------------------|-----|-----|-------|-----|---------------|
|     |                                                                                                          | HTT                                   | JT  | KKT | ST    | HPT |               |
|     |                                                                                                          | 1                                     | 2-5 | 6-9 | 10-12 | >12 |               |
| 29. | Layanan berbasis elektronik yang belum stabil tetapi digunakan                                           | ✓                                     |     |     |       |     |               |
| 30. | Tidak ada sosialisasi dan pelatihan teknis sebelum perangkat lunak digunakan secara massif di organisasi | ✓                                     |     |     |       |     |               |

Responden,



Indah Nur Fitriyani, A.Md

NIP. 199601302019022003

Singaraja, 16 Mei 2024

Peneliti,



Vany Adelia Putri

Lampiran 17. Wawancara Persetujuan Rancangan Karakteristik Area Dampak  
Risiko SPBE

Narasumber : Luh Putu Adi Ariwati, SE, M.Pd  
Jabatan : Sekretaris Dinas  
Instansi : Dinas Komunikasi, Informatika, Persandian dan Statistik  
Tempat/Tanggal : Kantor DiskominfoSanti/ 4 Juni 2024

Untuk dapat melakukan perhitungan risiko, maka instansi perlu mendefinisikan **Kriteria Area Dampak Risiko SPBE** dan menentukan level dampak risiko dari masing-masing kemungkinan risiko SPBE, berdasarkan wawancara yang dilakukan dengan Ibu Luh Putu Adi Ariwati, SE, M.Pd pada Selasa, 4 Juni 2024, bahwa instansi DiskominfoSanti Kab. Buleleng belum memiliki pendefinisian kriteria Area Dampak Risiko SPBE, maka diputuskan untuk menggunakan contoh pada panduan Permen PAN RB Nomor 5 Tahun 2020 serta mempertimbangkan berbagai contoh dari literatur sejumlah penelitian serupa. Berikut pendefinisian masing-masing level dampak pada sisi positif maupun negatif pada setiap area dampak (Terlampir)

| NO. | PERTANYAAN                                                                                                 | JAWABAN       |
|-----|------------------------------------------------------------------------------------------------------------|---------------|
| 1.  | Apakah rancangan dari pendefinisian area dampak (terlampir) disetujui untuk digunakan pada penelitian ini? | Iya, silakan. |

Sekretaris DiskominfoSanti,



**Luh Putu Adi Ariwati, SE, M.Pd**  
NIP. 198107112001121002

Singaraja. 4 Juni 2024  
Peneliti,



**Vany Adelia Putri**  
NIM. 2015091027

Narasumber : Made Kunayanti, SE, M.A.P  
Jabatan : Kepala Bidang Infrastruktur dan Layanan SPBE  
Instansi : Dinas Komunikasi, Informatika, Persandian dan Statistik  
Tempat/Tanggal : Kantor Diskominfosanti/ 4 Juni 2024

Untuk dapat melakukan perhitungan risiko, maka instansi perlu mendefinisikan **Kriteria Area Dampak Risiko SPBE** dan menentukan level dampak risiko dari masing-masing kemungkinan risiko SPBE, berdasarkan wawancara yang dilakukan dengan Ibu Luh Putu Adi Ariwati, SE, M.Pd pada Selasa, 4 Juni 2024, bahwa instansi Diskominfosanti Kab. Buleleng belum memiliki pendefinisian kriteria Area Dampak Risiko SPBE, maka diputuskan untuk menggunakan contoh pada panduan Permen PAN RB Nomor 5 Tahun 2020 serta mempertimbangkan berbagai contoh dari literatur sejumlah penelitian serupa. Berikut pendefinisian masing-masing level dampak pada sisi positif maupun negatif pada setiap area dampak (Terlampir)

| NO. | PERTANYAAN                                                                                                 | JAWABAN       |
|-----|------------------------------------------------------------------------------------------------------------|---------------|
| 1.  | Apakah rancangan dari pendefinisian area dampak (terlampir) disetujui untuk digunakan pada penelitian ini? | Iya, silakan. |

Kabid Infrastruktur & Layanan  
SPBE,



Made Kunayanti, SE, M.A.P  
NIP. 1980009221999032001

Singaraja. 4 Juni 2024  
Peneliti,



Vany Adelia Putri  
NIM. 2015091027

| AREA DAMPAK |         | LEVEL DAMPAK                                                                            |                                                                                         |                                                                                                           |                                                                                                            |                                                                                  |
|-------------|---------|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------|
|             |         | 1                                                                                       | 2                                                                                       | 3                                                                                                         | 4                                                                                                          | 5                                                                                |
|             |         | TIDAK SIGNIFIKAN                                                                        | KURANG SIGNIFIKAN                                                                       | CUKUP SIGNIFIKAN                                                                                          | SIGNIFIKAN                                                                                                 | SANGAT SIGNIFIKAN                                                                |
| FINANSIAL   | POSITIF | Peningkatan Efisiensi <20%                                                              | Peningkatan Efisiensi 20% s.d <40%                                                      | Peningkatan Efisiensi 40% s.d <60%                                                                        | Peningkatan Efisiensi 60% s.d <80%                                                                         | Peningkatan Efisiensi ≤80%                                                       |
|             | NEGATIF | Penurunan Efisiensi <20%                                                                | Penurunan Efisiensi 20% s.d <40%                                                        | Penurunan Efisiensi 40% s.d <60%                                                                          | Penurunan Efisiensi 60% s.d <80%                                                                           | Penurunan Efisiensi ≤80%                                                         |
| REPUTASI    | POSITIF | Terdapat pemberitaan positif namun tidak mengakibatkan kenaikan kepercayaan stakeholder | Terdapat pemberitaan positif namun tidak mengakibatkan kenaikan kepercayaan stakeholder | Terdapat pemberitaan positif yang dapat mempengaruhi kenaikan kepercayaan sebagian kecil dari stakeholder | Terdapat pemberitaan positif yang dapat mengakibatkan kenaikan kepercayaan sebagian besar dari stakeholder | Terdapat pemberitaan positif yang dapat menumbuhkan kepercayaan dari stakeholder |

|                     |         |                                                                                          |                                                                                          |                                                                                                  |                                                                                                             |                                                                                    |
|---------------------|---------|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
|                     | NEGATIF | Terdapat pemberitaan negatif namun tidak mengakibatkan penurunan kepercayaan stakeholder | Terdapat pemberitaan negatif namun tidak mengakibatkan penurunan kepercayaan stakeholder | Terdapat pemberitaan negatif yang dapat mempengaruhi kepercayaan sebagian kecil dari stakeholder | Terdapat pemberitaan negatif yang dapat mengakibatkan penurunan kepercayaan sebagian besar dari stakeholder | Terdapat pemberitaan negatif yang dapat menghilangkan kepercayaan dari stakeholder |
| KINERJA             | POSITIF | Peningkatan kinerja <20%                                                                 | Peningkatan kinerja 20% s.d <40%                                                         | Peningkatan kinerja 40% s.d <60%                                                                 | Peningkatan kinerja 60% s.d <80%                                                                            | Peningkatan kinerja ≤80%                                                           |
|                     | NEGATIF | Penurunan kinerja <20%                                                                   | Penurunan kinerja 20% s.d <40%                                                           | Penurunan kinerja 40% s.d <60%                                                                   | Penurunan kinerja 60% s.d <80%                                                                              | Penurunan kinerja ≤80%                                                             |
| LAYANAN ORGANISASAI | POSITIF | Peningkatan Kepuasan Pelanggan Meningkat <20%                                            | Peningkatan Kepuasan Pelanggan Meningkat 20% s.d <40%                                    | Peningkatan Kepuasan Pelanggan Meningkat 40% s.d <60%                                            | Peningkatan Kepuasan Pelanggan Meningkat 60% s.d <80%                                                       | Peningkatan Kepuasan Pelanggan Meningkat ≤80%                                      |
|                     | NEGATIF | Peningkatan Kepuasan Pelanggan Menurun <20%                                              | Peningkatan Kepuasan Pelanggan Menurun 20% s.d <40%                                      | Peningkatan Kepuasan Pelanggan Menurun 40% s.d <60%                                              | Peningkatan Kepuasan Pelanggan Menurun 60% s.d <80%                                                         | Peningkatan Kepuasan Pelanggan Menurun ≤80%                                        |

|                          |         |                                                                             |                                                                             |                                            |                                                           |                                                                                 |
|--------------------------|---------|-----------------------------------------------------------------------------|-----------------------------------------------------------------------------|--------------------------------------------|-----------------------------------------------------------|---------------------------------------------------------------------------------|
| OPERASIONAL DAN ASET TIK | POSITIF | Memangkas Proses Bisnis selama beberapa jam                                 | Memangkas Proses Bisnis 1 Hari                                              | Memangkas Proses Bisnis 2-3 Hari           | Memangkas Proses Bisnis 4-7 Hari                          | Memangkas Proses Bisnis lebih dari 7 hari                                       |
|                          | NEGATIF | Menghambat Proses Bisnis selama beberapa jam                                | Menghambat Proses Bisnis 1 Hari                                             | Menghambat Proses Bisnis 2-3 Hari          | Menghambat Proses Bisnis 4-7 Hari                         | Menghambat Proses Bisnis lebih dari 7 hari                                      |
| HUKUM DAN REGULASI       | POSITIF | Tidak terdapat permasalahan hukum                                           | Tidak terdapat permasalahan hukum                                           | Tidak terdapat permasalahan hukum          | Tidak terdapat permasalahan hukum                         | Tidak terdapat permasalahan hukum                                               |
|                          | NEGATIF | Terdapat permasalahan hukum(misal pelanggaran) namun belum menjadi tuntutan | Terdapat permasalahan hukum(misal pelanggaran) namun belum menjadi tuntutan | Tuntutan hukum dengan dampak relatif kecil | Tuntutan hukum berdampak pada kinerja/performa organisasi | Tuntutan hukum mengancam eksistensi organisasi atau manajemen puncak organisasi |
| SDM                      | POSITIF | Peningkatan Loyalitas <20%                                                  | Peningkatan Loyalitas 20% s.d <40%                                          | Peningkatan Loyalitas 40% s.d <60%         | Peningkatan Loyalitas 60% s.d <80%                        | Peningkatan Loyalitas ≤80%                                                      |

|  |         |                                |                                           |                                           |                                           |                                |
|--|---------|--------------------------------|-------------------------------------------|-------------------------------------------|-------------------------------------------|--------------------------------|
|  | NEGATIF | Penurunan<br>Loyalitas<br><20% | Penurunan<br>Loyalitas<br>20% s.d<br><40% | Penurunan<br>Loyalitas<br>40% s.d<br><60% | Penurunan<br>Loyalitas<br>60% s.d<br><80% | Penurunan<br>Loyalitas<br>≤80% |
|--|---------|--------------------------------|-------------------------------------------|-------------------------------------------|-------------------------------------------|--------------------------------|



## Lampiran 18. Penetapan Level Area Dampak Risiko

### **PENETAPAN LEVEL DAMPAK DARI MASING-MASING RISIKO**

Narasumber : Made Kunayanti, SE, M.A.P  
Jabatan : Kepala Bidang Infrastruktur dan Layanan SPBE  
Instansi : Dinas Komunikasi, Informatika, Persandian dan Statistik  
Tempat/Tanggal : Singaraja/10 Juli 2024

Berikut ini adalah form kuesioner yang digunakan guna mengidentifikasi level dampak dari tiap risiko dimasa depan akan memberikan dampak sejauh mana. Pada kolom *Level Dampak* silakan menuliskan level 1 – 5.

#### ***Keterangan:***

Level 1: Tidak Signifikan  
Level 2: Kurang Signifikan  
Level 3: Cukup Signifikan  
Level 4: Signifikan  
Level 5: Sangat Signifikan



| NO. | AREA DAMPAK | ID RISIKO |                                                                     | LEVEL DAMPAK | ALASAN LEVEL DAMPAK                                                                                                                 |
|-----|-------------|-----------|---------------------------------------------------------------------|--------------|-------------------------------------------------------------------------------------------------------------------------------------|
| 1.  | Finansial   | R1        | Data hilang atau rusak                                              | 5            | Berpengaruh besar pada operasional layanan ketika kehilangan informasi penting                                                      |
|     |             | R2        | Kegagalan backup data                                               | 4            | Mengakibatkan gangguan operasional dan kerugian besar sebab membutuhkan waktu pemulihan yang panjang                                |
|     |             | R5        | Organisasi mengalami limpahan data tetapi tidak mampu mengolah data | 3            | Dapat menghambat operasional bisnis tetapi masih dapat diatasi dengan penyesuaian operasional                                       |
| 2.  | Reputasi    | R3        | Serangan manusia (hacker, cracker)                                  | 5            | Penurunan reputasi dari masyarakat dan instansi                                                                                     |
|     |             | R16       | Server mengalami down                                               | 5            | Memberikan gangguan total atau keseluruhan pada kinerja operasional, bahkan kehilangan data dan berpotensi kerugian finansial besar |
|     |             | R29       | Layanan berbasis elektronik yang belum stabil tetapi digunakan      | 3            | Menyebabkan ketidaknyamanan pengguna dan gangguan operasional                                                                       |

| NO. | AREA DAMPAK              | ID RISIKO |                                                                      | LEVEL DAMPAK | ALASAN LEVEL DAMPAK                                                                                  |
|-----|--------------------------|-----------|----------------------------------------------------------------------|--------------|------------------------------------------------------------------------------------------------------|
| 3.  | Kinerja                  | R7        | Gangguan koneksi internet                                            | 4            | Menghambat kinerja yang menyebabkan tidak optimalnya pelayanan                                       |
|     |                          | R8        | Koneksi jaringan terputus                                            | 5            | Menghambat kelancaran operasional dan aksesibilitas vital layanan                                    |
|     |                          | R9        | Listrik padam tiba-tiba                                              | 4            | Berdampak pada kontinuitas operasional dan ketersediaan layanan yang membutuhkan daya listrik stabil |
| 4.  | Layanan                  | R27       | Dokumentasi atau tata cara penggunaan program/aplikasi tidak lengkap | 3            | Mengganggu efisiensi dan kehandalan penggunaan program tersebut.                                     |
|     |                          | R28       | Antar muka (user interface) program atau aplikasi susah dipahami     | 3            | Menghambat efektivitas pengguna dalam mengoperasikan program atau aplikasi                           |
| 5.  | Operasional dan Aset TIK | R6        | Kerusakan hardware                                                   | 5            | Menghambat kinerja operasional sebagai faktor eksternal dari layanan                                 |

| NO. | AREA DAMPAK | ID RISIKO |                                                                                                      | LEVEL DAMPAK | ALASAN LEVEL DAMPAK                                                                                                                                            |
|-----|-------------|-----------|------------------------------------------------------------------------------------------------------|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------|
|     |             | R10       | Ruangan server tidak menggunakan PAC (Precision Air Conditioning)                                    | 4            | Menyebabkan <i>overheating</i> dan kerusakan pada perangkat keras server, yang pada gilirannya dapat mengganggu ketersediaan layanan sistem secara signifikan. |
|     |             | R11       | Server mengalami kendala karena tidak adanya sumber energi listrik cadangan (Contoh: UPS dan Genset) | 4            | Mengakibatkan gangguan operasional yang luas                                                                                                                   |
|     |             | R12       | Akses masuk dan mengoperasikan layanan di dalam ruangan server tidak dicatat dan tidak dibatasi      | 5            | Berdampak kehilangan data bersifat sensitive/rahasia, gangguan operasional dan masalah hukum yang serius                                                       |
|     |             | R13       | Ruangan server tidak dipantau melalui CCTV                                                           | 5            | Berdampak kehilangan data bersifat sensitive/rahasia, gangguan operasional, pencurian aset seperti <i>hardware</i> dan masalah hukum yang serius               |

| NO. | AREA DAMPAK | ID RISIKO |                                                                                                                      | LEVEL DAMPAK | ALASAN LEVEL DAMPAK                                                                                                                                |
|-----|-------------|-----------|----------------------------------------------------------------------------------------------------------------------|--------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
|     |             | R14       | Tidak tersedia pemadam api (Contoh: NOVEC) dalam ruangan server                                                      | 5            | Mengakibatkan kebakaran besar sehingga memicu kehilangan hingga kerusakan data organisasi baik yang berifat data public atau data sesnitif/rahasia |
|     |             | R15       | Tidak ada tim monitoring khusus server                                                                               | 4            | Penanganan terhamabt akibat deteksi dan penanganan pada server yang lambat                                                                         |
|     |             | R17       | Kondisi server yang tidak memadai/tidak layak (Contoh: Server usang)                                                 | 4            | Kinerja server melambat/menurun hingga mengalami error atau <i>downtime</i> layanan                                                                |
|     |             | R18       | Perangkat mengalami overheat dan overload                                                                            | 4            | Mengakibatkan kerusakan perangkat dan <i>downtime</i> serta gangguan operasional                                                                   |
|     |             | R19       | Sistem operasi pada server tidak menyediakan interface untuk mengakses dan mengelola server (Contoh: CLI maupun GUI) | 2            | Dampak yang minimal dan tidak berakibat langsung pada operasi bisnis                                                                               |

| NO. | AREA DAMPAK | ID RISIKO |                                                                                 | LEVEL DAMPAK | ALASAN LEVEL DAMPAK                                                                                                                                 |
|-----|-------------|-----------|---------------------------------------------------------------------------------|--------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
|     |             | R20       | Tidak melakukan backup data secara berkala atau otomatis                        | 4            | Kehilangan data penting dan gangguan operasional yang signifikan jika terjadi kerusakan <i>hardware</i> , serangan virus, bahkan <i>human error</i> |
|     |             | R21       | Maintenance tidak terjadwal                                                     | 3            | Kemungkinan besar kehilangan data dan menyebabkan <i>downtime</i> pada layanan saat melakukan <i>backup data</i>                                    |
|     |             | R22       | Server mengalami serangan (Contoh: Virus)                                       | 4            | Menyebabkan <i>downtime</i> layanan dan potensi pelanggaran data                                                                                    |
|     |             | R23       | Data corrupt                                                                    | 4            | Mengakibatkan gangguan operasional layanan dan operasional bisnis serta potensi kehilangan data                                                     |
|     |             | R24       | Tidak melakukan back up data dan system server secara berkala                   | 4            | Kehilangan data penting dan gangguan operasional yang signifikan jika terjadi kerusakan <i>hardware</i> , serangan virus, bahkan <i>human error</i> |
|     |             | R25       | Tidak dilakukan kelola hak akses pengguna dalam hal ini hak akses yang dimaksud | 4            | Mengakibatkan akses tidak sah yang signifikan ke data sensitif, potensi pelanggaran data, dan kerusakan reputasi                                    |

| NO. | AREA DAMPAK         | ID RISIKO |                                                                                                          | LEVEL DAMPAK | ALASAN LEVEL DAMPAK                                     |
|-----|---------------------|-----------|----------------------------------------------------------------------------------------------------------|--------------|---------------------------------------------------------|
|     |                     |           | adalah hak masuk dan mengoperasikan infrastruktur server ( <i>hardware</i> dan <i>software</i> )         |              |                                                         |
|     |                     | R26       | Pemakaian software non orisinal                                                                          | 4            | Kerentanan keamanan                                     |
| 6.  | Hukum dan Regulasi  | R4        | Kebocoran data organisasi                                                                                | 4            | Penurunan reputasi dan penuntutan hukum atau regulasi   |
| 7.  | Sumber Daya Manusia | R30       | Tidak ada sosialisasi dan pelatihan teknis sebelum perangkat lunak digunakan secara massif di organisasi | 3            | Kerugian produktivitas dan potensi pada risiko keamanan |

## Lampiran 19. Rancangan Rekomendasi Menggunakan SWOT

### R1. Data Hilang atau Rusak

| INTERNAL<br>EKSTERNAL                                                                                                                                                                                                                                                                                                                                | STRENGTH                                                                                                                                                                                                                                                                                                                                                                                                                                       | WEAKNESS                                                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                                                                                      | <ol style="list-style-type: none"> <li>1. Surat Edaran nomor 400.13.53/1853/T.Kelola.Kominfosanti/VII/2023 mengenai Pedoman Penyelenggaraan Audit Teknologi Informasi Dan Komunikasi (TIK) Lingkup Pemerintah Kabupaten Buleleng</li> <li>2. Peta rencana pemkab buleleng</li> <li>3. SOP Penyediaan Layanan <i>Government Cloud Computing</i></li> <li>4. Memiliki tim IT yang cukup baik untuk Melakukan backup data secara rutin</li> </ol> | <ol style="list-style-type: none"> <li>1. Belum ada pedoman manajemen data SPBE</li> <li>2. Kegagalan sistem perangkat keras seperti kerusakan infrastruktur seperti dengan terjadinya hardisk error</li> <li>3. Tidak ada SOP pemulihan data rusak atau data hilang</li> </ol>                                        |
| OPPORTUNITY                                                                                                                                                                                                                                                                                                                                          | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                                                                                                                  | STRATEGIC W-O                                                                                                                                                                                                                                                                                                          |
| <ol style="list-style-type: none"> <li>1. Pemkab Buleleng memiliki Perbup Nomor 49 Tahun 2022 tentang Satu Data Daerah, pada pasal 13 bagian keempat tentang penyebarluasan data, ayat (5)</li> <li>2. Perbup Buleleng Nomor 79 Tahun 2017 tentang SOP Manajemen Pengamanan Informasi Digital di Lingkungan Pemerintah Kabupaten Buleleng</li> </ol> | <ol style="list-style-type: none"> <li>9. Memanfaatkan tim IT yang cukup baik untuk meningkatkan implementasi SOP Manajemen Pengamanan Informasi Digital (Perbup Nomor 79 Tahun 2017)</li> <li>10. Menggunakan Peta rencana Pemkab Buleleng untuk mendukung penerapan Perbup Nomor 49 Tahun 2022 tentang Satu Data Daerah.</li> </ol>                                                                                                          | <ol style="list-style-type: none"> <li>1. Mengembangkan dan mengimplementasikan pedoman manajemen data SPBE dengan merujuk pada Perbup Nomor 49 Tahun 2022 tentang Satu Data Daerah.</li> <li>2. Menyusun SOP pemulihan data yang rusak atau hilang, memanfaatkan Perbup Nomor 79 Tahun 2017 sebagai acuan.</li> </ol> |
| THREAT                                                                                                                                                                                                                                                                                                                                               | STRATEGIC S-T                                                                                                                                                                                                                                                                                                                                                                                                                                  | STRATEGIC W-T                                                                                                                                                                                                                                                                                                          |
| <ol style="list-style-type: none"> <li>1. Bencana Alam (Contoh: Banjir, Kebakaran, dll)</li> <li>2. <i>Cyber Crime (Hacking, cracking, virus, malware, phishing, cyber espionage, cyber terrorism)</i></li> </ol>                                                                                                                                    | <ol style="list-style-type: none"> <li>1. Memperkuat tim IT untuk menghadapi ancaman <i>cyber crime</i> dengan pelatihan dan alat keamanan yang memadai.</li> <li>2. Menggunakan SOP Penyediaan Layanan <i>Government Cloud Computing</i> untuk mitigasi risiko bencana alam dengan melakukan <i>backup data</i> secara <i>cloud-based</i>.</li> </ol>                                                                                         | <ol style="list-style-type: none"> <li>1. Mengembangkan infrastruktur yang lebih handal untuk mengurangi risiko kegagalan sistem perangkat keras.</li> <li>2. Menerapkan SOP pemulihan data yang hilang untuk mengurangi dampak dari ancaman bencana alam dan <i>cyber crime</i>.</li> </ol>                           |

## R2. Kegagalan backup data

| INTERNAL<br>EKSTERNAL                                                                                                                                                                                                                                                                        | STRENGTH                                                                                                                                                                                                                                                                                                                                                                                                       | WEAKNESS                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                              | <ol style="list-style-type: none"> <li>1. Pemkab Buleleng sudah memiliki peta rencana SPBE yang berisikan kriteria manajemen data SPBE</li> <li>2. SOP Penyediaan Layanan <i>Government Cloud Computing</i></li> <li>3. Di dukung dengan hardware yang baik</li> <li>4. Memiliki tim IT yang cukup baik untuk Melakukan backup data secara rutin</li> </ol>                                                    | <ol style="list-style-type: none"> <li>1. Belum ada pedoman manajemen data SPBE</li> <li>2. Terjadi kesalahan konfigurasi backup</li> <li>3. Tidak ada SOP backup data</li> <li>4. Belum ada jadwal yang dibuat khusus untuk melakukan backup data secara rutin</li> </ol>             |
| OPPORTUNITY                                                                                                                                                                                                                                                                                  | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                                                                                  | STRATEGIC W-O                                                                                                                                                                                                                                                                          |
| <ol style="list-style-type: none"> <li>1. Pemkab Buleleng memiliki Perbup Nomor 49 Tahun 2022 tentang Satu Data Daerah, pada pasal 13 bagian keempat tentang penyebaran data, ayat (5)</li> <li>2. Perbup Buleleng Nomor 79 Tahun 2017 tentang SOP Manajemen Pengamanan Informasi</li> </ol> | <ol style="list-style-type: none"> <li>1. Mengoptimalkan hardware yang sudah baik dan tim IT yang kompeten untuk menerapkan Perbup Nomor 49 Tahun 2022 dan Perbup Nomor 79 Tahun 2017 dalam manajemen data SPBE dan pengamanan informasi digital.</li> <li>2. Menggunakan SOP Penyediaan Layanan <i>Government Cloud Computing</i> untuk meningkatkan manajemen data sesuai dengan Perbup yang ada.</li> </ol> | <ol style="list-style-type: none"> <li>1. Membuat pedoman manajemen data SPBE dengan merujuk pada Perbup Nomor 49 Tahun 2022 dan Perbup Nomor 79 Tahun 2017.</li> <li>2. Mengembangkan SOP backup data dan menjadwalkan backup rutin dengan bimbingan dari Perbup yang ada.</li> </ol> |

|                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Digital di Lingkungan Pemerintah Kabupaten Buleleng                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                         |
| <b>THREAT</b>                                                                                                                                                                                                                                                            | <b>STRATEGIC S-T</b>                                                                                                                                                                                                                                                                                                                          | <b>STRATEGIC W-T</b>                                                                                                                                                                                                                                                                                                                                    |
| <ol style="list-style-type: none"> <li>1. Kehilangan data atau kerusakan data</li> <li>2. <i>Cyber Crime</i> (<i>Hacking, cracking, virus, malware, phishing, cyber espionage, cyber terrorism</i>)</li> <li>3. Bencana Alam (Contoh: Banjir, Kebakaran, dll)</li> </ol> | <ol style="list-style-type: none"> <li>1. Menggunakan hardware yang baik dan tim IT yang kompeten untuk memperkuat keamanan terhadap cyber crime dengan menerapkan SOP Manajemen Pengamanan Informasi Digital.</li> <li>2. Memanfaatkan SOP Penyediaan Layanan Government Cloud Computing untuk melindungi data dari bencana alam.</li> </ol> | <ol style="list-style-type: none"> <li>1. Menyusun pedoman dan SOP backup data serta menjadwalkan backup rutin untuk meminimalisir kehilangan atau kerusakan data.</li> <li>2. Meningkatkan pelatihan dan kesadaran akan cyber crime untuk tim IT dan staf terkait, serta memastikan konfigurasi backup yang benar untuk mencegah kesalahan.</li> </ol> |

### R3. Serangan manusia (hacker, cracker)

| INTERNAL<br>EKSTERNAL                                                                                  | STRENGTH                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | WEAKNESS                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                        | <ol style="list-style-type: none"> <li>1. Telah memiliki Cyber Incident Response Team (CIRT) Kabupaten Buleleng yang memberikan edukasi kesadaran keamanan SPBE yang dapat diakses melalui : <a href="https://csirt.bulelengkab.go.id/">https://csirt.bulelengkab.go.id/</a></li> <li>2. Pemkab Buleleng sudah memiliki draft peta rencana SPBE yang berisikan kriteria manajemen keamanan informasi SPBE</li> <li>3. BSSN memverifikasi laporan perbaikan IT Security Assesment oleh Diskominfosanti dengan Nomor Laporan Dok. 013/D21/LAP/03/2022</li> <li>4. Telah melakukan sosialisasi pada staff tentang kesadaran pentingnya keamanan informasi dan data</li> <li>5. Memiliki tim IT yang cukup baik untuk Melakukan backup data secara rutin</li> <li>6. Rutin melakukan audit berkala untuk menemukan celah keamanan, misalkan dengan penggunaan Honeyptot</li> </ol> | <ol style="list-style-type: none"> <li>1. Belum memiliki pedoman manajemen keamanan informasi SPBE</li> <li>2. Belum dilaksanakannya dokumentasi penanganan insiden keamanan SPBE</li> <li>3. Belum dilaksanakannya audit keamanan SPBE</li> <li>4. Di akibatkan tidak update <i>software</i></li> <li>5. Belum menggunakan teknologi enkripsi data untuk melindungi informasi data dan sensitive</li> <li>6. Tidak ada SOP untuk menindak serangan manusia</li> </ol> |
| OPPORTUNITY                                                                                            | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | STRATEGIC W-O                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <ol style="list-style-type: none"> <li>1. Pemkab Buleleng memiliki Perbub Buleleng Nomor 20</li> </ol> | <ol style="list-style-type: none"> <li>17. Memanfaatkan keberadaan Cyber Incident Response Team (CIRT) untuk mengimplementasikan Perbup Buleleng</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | <ol style="list-style-type: none"> <li>1. Mengembangkan pedoman manajemen keamanan informasi</li> </ol>                                                                                                                                                                                                                                                                                                                                                                |

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Tahun 2019 tentang Penyelenggaraan Persandian untuk pengamanan informasi, pada Pasal 3 Pengelolaan dan Perlindungan Informasi, ayat (2)</p> <p>2. Perbup Buleleng Nomor 79 Tahun 2017 tentang SOP Manajemen Pengamanan Informasi Digital di Lingkungan Pemerintah Kabupaten Buleleng</p> <p>3. Serah Terima perangkat Honeypot (honeypot adalah sistem tidak terlindungi yang menarik peretas dan mengumpulkan data tentang taktik dan teknik mereka) kepada Dinas Kominfosanti pada 24 September 2019 berdasarkan PKS</p> | <p>Nomor 79 Tahun 2017 tentang SOP Manajemen Pengamanan Informasi Digital.</p> <p>18. Menggunakan hasil verifikasi dari BSSN untuk mendapatkan dukungan implementasi Perbub Buleleng Nomor 20 Tahun 2019 tentang Pengelolaan dan Perlindungan Informasi.</p> <p>19. Memanfaatkan sosialisasi kesadaran keamanan untuk mendukung implementasi perangkat Honeypot yang diterima dari BSSN.</p> <p>20. Rutin melakukan audit berkala dengan memanfaatkan perangkat Honeypot untuk meningkatkan keamanan SPBE.</p> | <p>SPBE dengan dasar hukum Perbup Buleleng Nomor 79 Tahun 2017</p> <p>2. Meningkatkan dokumentasi penanganan insiden keamanan SPBE sesuai dengan Perbub Buleleng Nomor 79 Tahun 2017</p> <p>3. Melakukan audit keamanan SPBE dengan mengacu pada Perbub Buleleng Nomor 79 Tahun 2017.</p> <p>4. Menggunakan dukungan dari BSSN untuk memperbarui software dan menerapkan teknologi enkripsi data</p> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| BSSN Nomor<br>075/18/PKS/PEM/2019                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>THREAT</b>                                                                                                                                                                                                                                                               | <b>STRATEGIC S-T</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <b>STRATEGIC W-T</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <ol style="list-style-type: none"> <li>1. Cyber Crime (Hacking, cracking, virus, malware, phishing, cyber espionage, cyber terrorism)</li> <li>2. Kerugian finansial akibat kehilangan informasi/data</li> <li>3. Kerugian reputasi penurunan kepercayaan publik</li> </ol> | <ol style="list-style-type: none"> <li>1. Memanfaatkan tim IT yang kompeten dan rutin melakukan backup data untuk mengurangi dampak serangan cyber crime</li> <li>2. Melakukan sosialisasi dan edukasi keamanan informasi untuk mengurangi risiko kerugian reputasi akibat kehilangan data</li> <li>3. Menggunakan Honeypot untuk mendeteksi dan menganalisis serangan cyber sehingga dapat mencegah kerugian finansial</li> <li>4. Mengimplementasikan verifikasi laporan IT Security Assessment untuk mengurangi risiko serangan malware dan phishing</li> </ol> | <ol style="list-style-type: none"> <li>1. Mengembangkan dan menerapkan SOP penanganan serangan manusia untuk meningkatkan respons terhadap ancaman cyber crime</li> <li>2. Meningkatkan kesadaran dan pelatihan staf untuk memitigasi kerugian finansial akibat kehilangan data</li> <li>3. Menerapkan enkripsi data untuk melindungi informasi sensitif dan mengurangi risiko kerugian reputasi</li> <li>4. Memperbarui dan memelihara software secara berkala untuk mengurangi risiko serangan cyber espionage dan cyber terrorism</li> </ol> |

#### R4. Kebocoran data organisasi

| INTERNAL<br>EKSTERNAL                                                                                                                                                                                                                                                                                              | STRENGTH                                                                                                                                                                                                                                                                                                                                                             | WEAKNESS                                                                                                                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                                                    | <ol style="list-style-type: none"> <li>1. Pemkab Buleleng sudah memiliki peta rencana SPBE yang berisikan kriteria manajemen data SPBE</li> <li>2. Di dukung dengan hardware yang baik</li> <li>3. SOP Penyediaan Layanan <i>Government Cloud Computing</i></li> <li>4. Memiliki tim IT yang cukup baik untuk Melakukan backup data secara rutin</li> </ol>          | <ol style="list-style-type: none"> <li>1. Belum ada pedoman manajemen data SPBE</li> <li>2. Belum ada pedoman manajemen keamanan informasi SPBE</li> <li>3. Terjadi kesalahan konfigurasi backup</li> <li>4. Tim IT atau ahli dalam melakukan backup data hanya sedikit, perlu untuk penambahan SDM</li> </ol>          |
| OPPORTUNITY                                                                                                                                                                                                                                                                                                        | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                                        | STRATEGIC W-O                                                                                                                                                                                                                                                                                                           |
| <ol style="list-style-type: none"> <li>1. Pemkab Buleleng memiliki Perbup Nomor 49 Tahun 2022 tentang Satu Data Daerah, pada pasal 13 bagian keempat tentang penyebaran data, ayat (5)</li> <li>2. Perbup Buleleng Nomor 79 Tahun 2017 tentang SOP Manajemen Pengamanan Informasi Digital di Lingkungan</li> </ol> | <ol style="list-style-type: none"> <li>9. Memanfaatkan peta rencana SPBE dan hardware yang baik untuk mendukung implementasi Perbup No. 49 Tahun 2022 dan Perbup No. 79 Tahun 2017.</li> <li>10. Menggunakan SOP penyediaan layanan <i>Government Cloud Computing</i> bersama dengan tim IT yang handal untuk menjalankan program sertifikasi TI support.</li> </ol> | <ol style="list-style-type: none"> <li>1. Mengembangkan pedoman manajemen data dan keamanan informasi SPBE sesuai dengan Perbup No. 49 Tahun 2022 dan Perbup No. 79 Tahun 2017.</li> <li>2. Meningkatkan jumlah SDM IT melalui program sertifikasi TI support dan meminimalkan kesalahan konfigurasi backup.</li> </ol> |

|                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                    |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>Pemerintah Kabupaten Buleleng</p> <p>3. Serah Terima perangkat Honeypot (honeypot adalah sistem tidak terlindungi yang menarik peretas dan mengumpulkan data tentang taktik dan teknik mereka) kepada Dinas Kominfo pada 24 September 2019 berdasarkan PKS BSSN Nomor 075/18/PKS/PEM/2019</p> <p>4. Program sertifikasi TI <i>support</i> kepada tim TI dan atau calon pegawai/staff</p> |                                                                                                                                                                                                      |                                                                                                                                                                                                                                    |
| <p><b>THREAT</b></p>                                                                                                                                                                                                                                                                                                                                                                        | <p><b>STRATEGIC S-T</b></p>                                                                                                                                                                                                                                                             | <p><b>STRATEGIC W-T</b></p>                                                                                                                                                                                                        |
| <p>1. Bencana Alam (Contoh: Banjir, Kebakaran, dll)</p> <p>2. <i>Cyber Crime (Hacking, cracking, virus, malware, phishing, cyber espionage, cyber terrorism)</i></p>                                                                                                                                                                                                                        | <p>1. Menggunakan peta rencana SPBE, hardware yang baik, dan SOP Government Cloud Computing untuk mengurangi risiko bencana alam dan cyber crime.</p> <p>2. Mengoptimalkan kemampuan tim IT dalam melakukan backup data secara rutin untuk mencegah kehilangan atau kerusakan data.</p> | <p>1. Mengembangkan dan menerapkan pedoman manajemen data dan keamanan informasi SPBE untuk mengurangi risiko human error dan cyber crime.</p> <p>2. Meningkatkan jumlah dan kapasitas SDM IT untuk menghadapi ancaman bencana</p> |

|                                                |  |                                                     |
|------------------------------------------------|--|-----------------------------------------------------|
| 3. Kehilangan data atau kerusakan data         |  | alam dan meminimalkan kesalahan konfigurasi backup. |
| 4. Kesalahan manusia<br>( <i>Human error</i> ) |  |                                                     |



### R5. Organisasi mengalami limpahan data tetapi tidak mampu mengolah data

| INTERNAL<br>EKSTERNAL                                                                                                                                     | STRENGTH                                                                                                                                                                                            | WEAKNESS                                                                                                                        |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                           | Limpahan data terjadi menysar ke bidang yang berkolaborasi saja, tidak terjadi pada layanan <i>bandwith</i> internet                                                                                | Kemungkinan terjadinya limpahan data                                                                                            |
| OPPORTUNITY                                                                                                                                               | STRATEGIC S-O                                                                                                                                                                                       | STRATEGIC W-O                                                                                                                   |
| Pemkab Buleleng memiliki dokumen yang mengatur tentang standar dan mekanisme interoperabilitas sesuai Perbup Nomor 58 Tahun 2019 tentang Tata Kelola SPBE | 6. Memanfaatkan standar dan mekanisme interoperabilitas yang diatur dalam Perbup Nomor 58 Tahun 2019 untuk memastikan data kolaborasi<br>7. Aman dan tidak mempengaruhi layanan bandwidth internet. | Menggunakan standar dan mekanisme interoperabilitas yang diatur dalam Perbup Nomor 58 Tahun 2019 untuk mengurangi limpahan data |
| THREAT                                                                                                                                                    | STRATEGIC S-T                                                                                                                                                                                       | STRATEGIC W-T                                                                                                                   |
| Kehilangan data atau kerusakan data                                                                                                                       | Menggunakan kekuatan dalam pengelolaan limpahan data untuk memastikan data tidak hilang atau rusak selama proses kolaborasi.                                                                        | Mengembangkan sistem backup dan recovery untuk mengatasi risiko kehilangan atau kerusakan data akibat limpahan data.            |

## R6. Kerusakan Hardware

| INTERNAL<br>EKSTERNAL                                                                                                                                                  | STRENGTH                                                                                                                                                                                                                                                                                                                                         | WEAKNESS                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                        | <ol style="list-style-type: none"> <li>Memiliki hardware dengan kondisi baik, hal ini terdapat dalam RENSTRA Diskominfosanti 2023-2026</li> <li>Memiliki hardware cadangan yang siap digunakan</li> <li>Pemkab Buleleng sudah memiliki peta rencana SPBE yang berisikan kriteria manajemen aset TIK</li> </ol>                                   | <ol style="list-style-type: none"> <li>Masih ada hardware yang telah usang beroperasi, tetapi tetap diberikan pemeliharaan</li> <li>Tidak ada SOP untuk melakukan pemeliharaan dan perbaikan hardware</li> <li>Belum memiliki pedoman manajemen aset TIK</li> </ol>        |
| OPPORTUNITY                                                                                                                                                            | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                    | STRATEGIC W-O                                                                                                                                                                                                                                                              |
| <ol style="list-style-type: none"> <li>Pemkab Buleleng memiliki kebijakan internal berupa Perda Nomor 6 Tahun 2017 tentang Pengelolaan Barang Milik Daerah.</li> </ol> | <ol style="list-style-type: none"> <li>Memanfaatkan hardware dalam kondisi baik dan hardware cadangan untuk mendukung implementasi Perda No. 6 Tahun 2017 tentang Pengelolaan Barang Milik Daerah.</li> <li>Menggunakan peta rencana SPBE untuk mengembangkan dan memperluas infrastruktur TIK yang sesuai dengan kebijakan internal.</li> </ol> | <ol style="list-style-type: none"> <li>Membuat dan menerapkan SOP untuk pemeliharaan dan perbaikan hardware berdasarkan panduan Perda No. 6 Tahun 2017.</li> <li>Mengembangkan pedoman manajemen aset TIK dengan memanfaatkan kebijakan internal sebagai acuan.</li> </ol> |
| THREAT                                                                                                                                                                 | STRATEGIC S-T                                                                                                                                                                                                                                                                                                                                    | STRATEGIC W-T                                                                                                                                                                                                                                                              |
| <ol style="list-style-type: none"> <li><i>Downtime</i> akibat kegagalan daya</li> </ol>                                                                                | <ol style="list-style-type: none"> <li>Menggunakan hardware dalam kondisi baik dan hardware cadangan untuk meminimalisir downtime akibat kegagalan daya.</li> </ol>                                                                                                                                                                              | <ol style="list-style-type: none"> <li>Mengurangi risiko menggunakan hardware usang dengan meningkatkan pengadaan dan</li> </ol>                                                                                                                                           |

|                                                                                                                                                                                     |                                                                                                               |                                                                                                                                                                                                                            |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>2. Bencana Alam<br/>(Contoh: Banjir, Kebakaran, dll)</p> <p>3. <i>Cyber Crime</i><br/>(<i>Hacking, cracking, virus, malware, phishing, cyber espionage, cyber terrorism</i>)</p> | <p>2. Mengimplementasikan peta rencana SPBE yang mencakup strategi mitigasi bencana alam dan cyber crime.</p> | <p>perawatan yang lebih baik sesuai dengan pedoman yang baru dibuat.</p> <p>2. Membuat SOP yang kuat dan teruji untuk pemeliharaan dan perbaikan hardware guna mengurangi dampak ancaman bencana alam dan cyber crime.</p> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



### R7. Gangguan Koneksi Internet

|                                          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div>INTERNAL</div> <div>EKSTERNAL</div> | <b>STRENGTH</b> <ol style="list-style-type: none"> <li>1. Surat Edaran Nomor 800/1302/Kominfosanti/2020 mengenai pengadaan bandwidth internet khususnya pada semua SKPD pada Tahun Anggaran 2021 dipusatkan di Dinas Komunikasi Informatika Persandian, dan Statistik Kabupaten Buleleng</li> <li>2. SOP Penyediaan <i>Bandwith</i> Internet</li> <li>3. Dinas Komunikasi, Informatika, Persandian dan Statistik selaku pengelola jaringan intranet di Kabupaten Buleleng telah menyusun dokumen topologi jaringan intra pemerintah daerah</li> <li>4. Kondisi jaringan internet tergolong baik</li> </ol> | <b>WEAKNESS</b> <ol style="list-style-type: none"> <li>1. Berdampak besar pada operasional harian instansi</li> <li>2. Tidak ada SOP untuk pemeliharaan jaringan</li> <li>3. Putusnya kabel fiber <i>optic</i></li> <li>4. Kurangnya koordinasi dengan Internet Service Provider (ISP)</li> </ol>                                                                                       |
|                                          | <b>OPPORTUNITY</b> <ol style="list-style-type: none"> <li>1. <i>Internet Service Provider</i> (ISP) yang lebih andal</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | <b>STRATEGIC S-O</b> <ol style="list-style-type: none"> <li>9. Memanfaatkan dokumen topologi jaringan intra pemerintah daerah untuk menarik ISP yang lebih andal dan memastikan cakupan jaringan yang lebih luas dan stabil</li> <li>10. Dengan jaringan internet yang tergolong baik, mengadakan negosiasi dengan ISP untuk peningkatan layanan internet agar semakin andal</li> </ol> |
|                                          | <b>THREAT</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <b>STRATEGIC W-O</b> <ol style="list-style-type: none"> <li>1. Mengembangkan SOP untuk pemeliharaan jaringan dengan melibatkan ISP yang lebih andal.</li> <li>2. Meningkatkan koordinasi dengan ISP baru yang lebih andal untuk mencegah dan menangani putusnya kabel fiber optic.</li> </ol>                                                                                           |
|                                          | <b>STRATEGIC S-T</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | <b>STRATEGIC W-T</b>                                                                                                                                                                                                                                                                                                                                                                    |

|                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                              |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. Akibat penanganan masalah yang tertunda</li> <li>2. <i>Cyber Crime</i> (<i>Hacking, cracking, virus, malware,</i> Penurunan reputasi</li> <li>3. <i>phising, cyber espionage, cyber terrorism</i>)</li> </ol> | <ol style="list-style-type: none"> <li>1. Menggunakan SOP Penyediaan Bandwidth Internet dan dokumen topologi jaringan untuk cepat tanggap dalam menangani masalah jaringan sehingga tidak terjadi penanganan masalah yang tertunda.</li> <li>2. Memastikan kondisi jaringan internet yang baik untuk meminimalisir risiko serangan cyber.</li> </ol> | <ol style="list-style-type: none"> <li>1. Mengembangkan dan menerapkan SOP pemeliharaan jaringan untuk mengurangi dampak operasional harian akibat putusnya kabel fiber optic.</li> <li>2. Meningkatkan koordinasi internal dan eksternal dengan ISP untuk mencegah dan menangani serangan cyber.</li> </ol> |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



### R8. Koneksi jaringan terputus

| INTERNAL<br>EKSTERNAL                                                                                        | STRENGTH                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | WEAKNESS                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                              | <ol style="list-style-type: none"> <li>1. Surat Edaran Nomor 800/1302/Kominfosanti/2020 mengenai pengadaan bandwidth internet khususnya pada semua SKPD pada Tahun Anggaran 2021 dipusatkan di Dinas Komunikasi Informatika Persandian, dan Statistik Kabupaten Buleleng</li> <li>2. SOP Penyediaan <i>Bandwith</i> dengan tujuan pengelolaan jaringan untuk akses intranet dan internet bagi setiap perangkat daerah</li> <li>3. Dinas Komunikasi, Informatika, Persandian dan Statistik selaku pengelola jaringan intranet di Kabupaten Buleleng telah menyusun dokumen topologi jaringan intra pemerintah daerah</li> <li>4. Kondisi jaringan internet tergolong baik</li> </ol> | <ol style="list-style-type: none"> <li>1. Berdampak besar pada operasional harian instansi</li> <li>2. Tidak ada SOP untuk pemeliharaan jaringan</li> <li>3. Putusnya kabel fiber optic</li> <li>4. Kurangnya koordinasi dengan <i>Internet Service Provider</i> (ISP)</li> </ol> |
| OPPORTUNITY                                                                                                  | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | STRATEGIC W-O                                                                                                                                                                                                                                                                     |
| <ol style="list-style-type: none"> <li>1. <i>Internet Service Provider</i> (ISP) yang lebih andal</li> </ol> | <ol style="list-style-type: none"> <li>10. Memanfaatkan Surat Edaran dan SOP yang ada untuk menjalin kerjasama dengan ISP yang lebih andal, guna meningkatkan kualitas dan kehandalan jaringan internet.</li> <li>11. Menggunakan dokumen topologi jaringan untuk mengoptimalkan pengelolaan dan</li> </ol>                                                                                                                                                                                                                                                                                                                                                                         | <ol style="list-style-type: none"> <li>1. Mengembangkan SOP pemeliharaan jaringan dengan melibatkan ISP yang lebih andal untuk memastikan operasional harian instansi tidak terganggu.</li> <li>2. Meningkatkan koordinasi dengan ISP untuk penanganan masalah</li> </ol>         |

|                                                                                                                                                                                   |                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                   | <p>peningkatan jaringan dengan ISP yang lebih andal.</p> <p>12. Meningkatkan kondisi jaringan internet yang sudah baik dengan dukungan dari ISP yang lebih andal.</p>                                                                                                       | <p>kabel fiber optic yang putus sehingga dapat mengurangi dampak besar pada operasional instansi.</p>                                                                                                                                                          |
| <b>THREAT</b>                                                                                                                                                                     | <b>STRATEGIC S-T</b>                                                                                                                                                                                                                                                        | <b>STRATEGIC W-T</b>                                                                                                                                                                                                                                           |
| <p>1. Penurunan reputasi akibat penanganan masalah yang tertunda</p> <p>2. <i>Cyber Crime (Hacking, cracking, virus, malware, phishing, cyber espionage, cyber terrorism)</i></p> | <p>1. Menggunakan SOP yang ada dan dokumen topologi jaringan untuk menanggulangi dan memitigasi ancaman cyber crime secara efektif.</p> <p>2. Menjaga kondisi jaringan internet yang baik untuk menghindari penurunan reputasi akibat penanganan masalah yang tertunda.</p> | <p>1. Menyusun SOP pemeliharaan jaringan untuk mencegah penurunan reputasi akibat penanganan masalah yang tertunda.</p> <p>2. Meningkatkan koordinasi dengan ISP dan mengembangkan rencana cadangan untuk menangani ancaman cyber crime dengan lebih baik.</p> |

### R9. Listrik padam tiba-tiba

| INTERNAL<br>EKSTERNAL                                                                                    | STRENGTH                                                                                                                                                                           | WEAKNESS                                                                                                                                                              |
|----------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                          | Memiliki cadangan listrik selain listrik utama yang disediakan oleh PLN, yakni dengan pengadaan Genset yang dapat beroperasi langsung sesaat listrik PLN padam                     | Berdampak pada operasional harian instansi secara tidak signifikan                                                                                                    |
| OPPORTUNITY                                                                                              | STRATEGIC S-O                                                                                                                                                                      | STRATEGIC W-O                                                                                                                                                         |
| Penambahan daya listrik PLN untuk mengurangi kejadian listrik padam saat operasional organisasi berjalan | Memanfaatkan cadangan listrik dari genset untuk mendukung penambahan daya listrik PLN sehingga operasional organisasi tetap berjalan lancar tanpa terganggu oleh pemadaman listrik | Mengurangi dampak operasional harian yang tidak signifikan dengan meningkatkan penambahan daya listrik PLN agar operasional berjalan lebih efisien dan efektif        |
| THREAT                                                                                                   | STRATEGIC S-T                                                                                                                                                                      | STRATEGIC W-T                                                                                                                                                         |
| Kehilangan data atau kerusakan data                                                                      | Menggunakan genset sebagai backup untuk melindungi data dan mengurangi risiko kehilangan atau kerusakan data selama pemadaman listrik PLN                                          | Meminimalkan dampak negatif pada operasional harian dan melindungi data dengan menambah daya listrik PLN serta mengimplementasikan sistem backup data yang lebih baik |

**R10. Ruang server tidak menggunakan PAC (Precision Air Conditioning)**

| INTERNAL<br>EKSTERNAL                                                                                                                                                                                                                                                                              | STRENGTH                                                                                                                                                                                                                                                                                             | WEAKNESS                                                                                                                                                                                                                                    |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                                    | Sudah menggunakan PAC (PAC berfungsi untuk pengendalian suhu & kelembapan, operasional stabil, hemat energi, dan penghambatan downtime)                                                                                                                                                              | Anggaran pengadaan PAC lebih mahal                                                                                                                                                                                                          |
| OPPORTUNITY                                                                                                                                                                                                                                                                                        | STRATEGIC S-O                                                                                                                                                                                                                                                                                        | STRATEGIC W-O                                                                                                                                                                                                                               |
| Perbup Buleleng Nomor 79 Tahun 2018 Tentang Standar Operasional Dan Prosedur Manajemen Data Center Pada Pemerintah Kabupaten Buleleng, pada BAB 2, Bagian Kesatu tentang ruang server dan perangkat pendukung, Pasal 5 ayat (1) tentang Ruang server wajib memenuhi standar pendukung bagian a,b,c | <ol style="list-style-type: none"> <li>1. Manfaatkan PAC untuk memenuhi standar operasional dan prosedur dalam Perbup Buleleng Nomor 79 Tahun 2018</li> <li>2. Promosikan stabilitas operasional dan efisiensi energi dari PAC kepada pihak berwenang untuk mendapatkan dukungan tambahan</li> </ol> | <ol style="list-style-type: none"> <li>1. Ajukan anggaran tambahan dengan menunjukkan bagaimana PAC membantu memenuhi standar Perbup Buleleng</li> <li>2. Carilah subsidi atau bantuan dana untuk pengadaan PAC yang lebih mahal</li> </ol> |
| THREAT                                                                                                                                                                                                                                                                                             | STRATEGIC S-T                                                                                                                                                                                                                                                                                        | STRATEGIC W-T                                                                                                                                                                                                                               |
| Berdampak signifikan bagi operasional server ketika terjadi gangguan misalkan kehilangan data dan kerugian finansial                                                                                                                                                                               | <ol style="list-style-type: none"> <li>1. Gunakan stabilitas dan efisiensi energi PAC untuk mengurangi risiko downtime dan kehilangan data</li> <li>2. Implementasikan prosedur keamanan tambahan untuk meminimalkan risiko finansial dari gangguan operasional</li> </ol>                           | <ol style="list-style-type: none"> <li>1. Buat rencana kontingensi untuk mengatasi gangguan operasional meskipun anggaran PAC lebih tinggi</li> <li>2. Kembangkan pelatihan dan sistem pemantauan untuk mendeteksi dan</li> </ol>           |

|  |  |                                     |
|--|--|-------------------------------------|
|  |  | mencegah gangguan seawal<br>mungkin |
|--|--|-------------------------------------|



**R11. Server mengalami kendala karena tidak adanya sumber energi listrik cadangan (Contoh: UPS dan Genset)**

| INTERNAL<br>EKSTERNAL                                                                                                                                                                                                                                                 | STRENGTH                                                                                                                                                                                                                                                                                                                                         | WEAKNESS                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                       | Sudah menggunakan 5 UPS dan 1 Genset                                                                                                                                                                                                                                                                                                             | Kendala UPS                                                                                                                                                                                                                                                                                                                                                    |
| OPPORTUNITY                                                                                                                                                                                                                                                           | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                    | STRATEGIC W-O                                                                                                                                                                                                                                                                                                                                                  |
| Perbup Buleleng Nomor 79 Tahun 2018 Tentang Standar Operasional Dan Prosedur Manajemen Data Center Pada Pemerintah Kabupaten Buleleng, pada BAB 2, Bagian Kesatu tentang ruang server dan perangkat pendukung, Pasal 5 ayat (5) tentang Kelistrikan bagian b,c,dan d. | <ol style="list-style-type: none"> <li>9. Memanfaatkan keberadaan 5 UPS dan 1 genset untuk memastikan kesesuaian dengan Perbup Buleleng Nomor 79 Tahun 2018 dalam hal kelistrikan.</li> <li>10. Menggunakan kekuatan kelistrikan yang ada untuk mematuhi standar operasional dan prosedur manajemen data center di Kabupaten Buleleng</li> </ol> | <ol style="list-style-type: none"> <li>1. Memanfaatkan peluang dari Perbup Buleleng Nomor 79 Tahun 2018 untuk mengatasi kendala UPS dengan memperbaiki atau meningkatkan infrastruktur UPS sesuai dengan standar yang ditetapkan.</li> <li>2. Menggunakan regulasi sebagai panduan untuk meningkatkan sistem UPS dan mengurangi kelemahan yang ada.</li> </ol> |
| THREAT                                                                                                                                                                                                                                                                | STRATEGIC S-T                                                                                                                                                                                                                                                                                                                                    | STRATEGIC W-T                                                                                                                                                                                                                                                                                                                                                  |
| Penurunan reputasi akibat penanganan masalah yang tertunda                                                                                                                                                                                                            | <ol style="list-style-type: none"> <li>1. Menggunakan 5 UPS dan 1 genset yang ada untuk memastikan tidak ada penurunan reputasi akibat penanganan masalah yang tertunda, dengan selalu siap menghadapi kemungkinan gangguan listrik</li> <li>2. Memanfaatkan kekuatan kelistrikan yang ada untuk merespons dengan cepat setiap</li> </ol>        | <ol style="list-style-type: none"> <li>1. Meningkatkan pemeliharaan dan monitoring UPS untuk menghindari kendala yang dapat menyebabkan penanganan masalah yang tertunda, yang dapat merusak reputasi</li> </ol>                                                                                                                                               |

|  |                                                               |                                                                                                                                                                 |
|--|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|
|  | masalah teknis, sehingga mengurangi risiko penurunan reputasi | 2. Menggunakan standar dari Perbup Buleleng sebagai panduan untuk mengatasi kelemahan UPS, sehingga dapat mengurangi risiko terhadap ancaman penurunan reputasi |
|--|---------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------|



**R12. Akses masuk ke dalam ruangan server tidak dicatat dan tidak dibatasi**

| INTERNAL<br>EKSTERNAL                                                                                                                                                                                                                                               | STRENGTH                                                                                                                                                                                                                 | WEAKNESS                                                                                                                                                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                     | Memiliki kebijakan tidak tertulis bahwa yang bisa masuk ke dalam ruang server hanya yang berkepentingan, seperti bidang tata kelola dan SDM SPBE lalu bidang infrastruktur & layanan SPBE, serta teknisi/programmer saja | Pencatatan masih manual                                                                                                                                                                      |
| OPPORTUNITY                                                                                                                                                                                                                                                         | STRATEGIC S-O                                                                                                                                                                                                            | STRATEGIC W-O                                                                                                                                                                                |
| Perbup Buleleng Nomor 79 Tahun 2018 Tentang Standar Operasional Dan Prosedur Manajemen Data Center Pada Pemerintah Kabupaten Buleleng, pada BAB 2, Bagian Kesatu tentang ruang server dan perangkat pendukung, Pasal 5 ayat (6) tentang Akses Fisik ke Ruang Server | Menggunakan kebijakan tidak tertulis untuk membatasi akses ke ruang server sesuai dengan Perbup Buleleng Nomor 79 Tahun 2018 untuk meningkatkan keamanan dan manajemen ruang server                                      | Memanfaatkan Perbup Buleleng Nomor 79 Tahun 2018 untuk mengimplementasikan sistem pencatatan otomatis sehingga meminimalkan kesalahan dan inefisiensi yang disebabkan oleh pencatatan manual |
| THREAT                                                                                                                                                                                                                                                              | STRATEGIC S-T                                                                                                                                                                                                            | STRATEGIC W-T                                                                                                                                                                                |
| Kehilangan data atau kerusakan data                                                                                                                                                                                                                                 | Menerapkan kebijakan akses terbatas ke ruang server untuk mengurangi risiko kehilangan atau kerusakan data                                                                                                               | Mengganti sistem pencatatan manual dengan sistem pencatatan otomatis untuk meningkatkan keamanan dan mengurangi kemungkinan kehilangan atau kerusakan data                                   |

### R13. Ruangan server tidak dipantau melalui CCTV

| INTERNAL<br>EKSTERNAL                                                                                                                                                                                                                                                          | STRENGTH                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | WEAKNESS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                | <ol style="list-style-type: none"> <li>1. Sudah ada CCTV</li> <li>2. Keamanan fisik ruangan server dipantau secara <i>real-time</i></li> <li>3. Mengurangi risiko akses tidak sah atau kebocoran data</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                 | <ol style="list-style-type: none"> <li>1. Ada beberapa kamera CCTV yang mati/tidak berfungsi dengan baik</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                               |
| OPPORTUNITY                                                                                                                                                                                                                                                                    | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    | STRATEGIC W-O                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <ol style="list-style-type: none"> <li>1. Perbup Buleleng Nomor 79 Tahun 2018 Tentang Standar Operasional Dan Prosedur Manajemen Data Center Pada Pemerintah Kabupaten Buleleng, pada BAB 2 tentang Standar Operasional dan Prosedur, Pasal 4 bagian (1), dan (2) e</li> </ol> | <ol style="list-style-type: none"> <li>9. Memanfaatkan CCTV yang ada dan pemantauan real-time untuk memenuhi standar operasional dan prosedur yang diatur dalam Perbup Buleleng Nomor 79 Tahun 2018. Hal ini dapat dilakukan dengan meningkatkan kualitas CCTV, menambah jumlah CCTV, dan memastikan semua CCTV berfungsi dengan baik.</li> <li>10. Menggunakan CCTV dan pemantauan real-time untuk mencegah terjadinya serangan fisik atau pencurian perangkat keras. Hal ini dapat dilakukan dengan memantau aktivitas di sekitar ruangan server secara terus menerus dan segera mengambil tindakan jika ada aktivitas mencurigakan</li> </ol> | <ol style="list-style-type: none"> <li>1. Memanfaatkan Perbup Buleleng Nomor 79 Tahun 2018 untuk memperbaiki CCTV yang mati/tidak berfungsi dengan baik. Hal ini dapat dilakukan dengan mengajukan permohonan anggaran untuk perbaikan atau penggantian CCTV.</li> <li>2. Memanfaatkan peluang untuk meningkatkan keamanan fisik ruangan server dengan memperbaiki CCTV yang mati/tidak berfungsi dengan baik. Hal ini dapat dilakukan dengan bekerja sama dengan vendor CCTV untuk mendapatkan layanan perbaikan atau</li> </ol> |

|                                                                                                                                                                                                                                        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | penggantian CCTV yang berkualitas.                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| THREAT                                                                                                                                                                                                                                 | STRATEGIC S-T                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | STRATEGIC W-T                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| <ol style="list-style-type: none"> <li>1. Adanya kemungkinan terjadinya risiko serangan fisik atau pencurian perangkat keras</li> <li>2. Adanya kemungkinan terjadinya risiko serangan fisik atau pencurian perangkat keras</li> </ol> | <ol style="list-style-type: none"> <li>1. Memanfaatkan CCTV dan pemantauan real-time untuk mencegah terjadinya serangan fisik atau pencurian perangkat keras. Hal ini dapat dilakukan dengan memantau aktivitas di sekitar ruangan server secara terus menerus dan segera mengambil tindakan jika ada aktivitas mencurigakan</li> <li>2. Meningkatkan kualitas CCTV dan menambah jumlah CCTV untuk memperkuat keamanan fisik ruangan server. Hal ini dapat dilakukan dengan mengajukan permohonan anggaran untuk perbaikan atau penggantian CCTV, serta untuk pembelian CCTV baru</li> </ol> | <ol style="list-style-type: none"> <li>1. Membuat rencana untuk mengatasi risiko serangan fisik atau pencurian perangkat keras. Hal ini dapat dilakukan dengan membuat SOP untuk menghadapi situasi darurat, seperti kebakaran, gempa bumi, atau perampokan</li> <li>2. Meningkatkan kesadaran karyawan tentang pentingnya keamanan fisik ruangan server. Hal ini dapat dilakukan dengan mengadakan pelatihan tentang keamanan fisik dan memberikan informasi tentang risiko yang mungkin terjadi</li> </ol> |

**R14. Tidak tersedia pemadam api (Contoh: NOVEC) dalam ruangan server**

| <div>INTERNAL</div> <div> </div> <div>EKSTERNAL</div>                           | STRENGTH                                                                                                                                                                                                                                                                                                                                                                                         | WEAKNESS                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                 | <div>1. Sudah ada Alat Pemadam Api Ringan (APAR), sudah memberikan perlindungan dasar terhadap risiko kebakaran, memungkinkan tindakan cepat dalam situasi darurat.</div> <div>2. Gedung sudah dilengkapi dengan alarm kebakaran untuk mengevakuasi personil saat kebakaran terjadi</div> <div>3. Sudah mendapat sosialisasi tentang penggunaan APAR oleh Dinas Pemadam Kebakaran Buleleng</div> | <div>1. Tidak efektif untuk kondisi kebakaran yang lebih besar</div> <div>2. APAR konvensional yang menggunakan air atau busa memiliki kemungkinan merusak peralatan elektronik sensitif di dalam ruangan server</div> <div>3. Sosialisasi hanya dilakukan kepada staff yang ditunjuk untuk mewakili Diskominfo, tidak seluruh staff mendapatkan sosialisasi penggunaan APAR</div> |
| OPPORTUNITY                                                                     | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                                                                    | STRATEGIC W-O                                                                                                                                                                                                                                                                                                                                                                      |
| <div>1. Sosialisasi penggunaan APAR oleh Dinas Pemadam Kebakaran Buleleng</div> | <div>9. Meningkatkan pelatihan penggunaan APAR kepada seluruh staff menggunakan fasilitas dan dukungan dari Dinas Pemadam Kebakaran Buleleng</div> <div>10. Memanfaatkan alarm kebakaran yang sudah ada untuk latihan simulasi kebakaran secara berkala</div>                                                                                                                                    | <div>1. Mengganti atau menambah APAR konvensional dengan APAR yang menggunakan bahan pemadam yang aman untuk peralatan elektronik sensitif, serta mengadakan pelatihan penggunaan untuk seluruh staff</div> <div>2. Mengembangkan program pelatihan rutin dan menyeluruh untuk semua staff agar lebih siap dalam situasi darurat kebakaran</div>                                   |

| THREAT                                                                                                                                                                                                                                                                                                                                   | STRATEGIC S-T                                                                                                                                                                                                                                                                     | STRATEGIC W-T                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. Kerusakan peralatan dan data</li> <li>2. Risiko terhadap keselamatan personil yang mungkin harus mengoperasikan APAR dalam kondisi berbahaya</li> <li>3. Kebakaran dapat menyebabkan downtime yang signifikan, mengakibatkan kerugian finansial dan gangguan operasional yang besar</li> </ol> | <ol style="list-style-type: none"> <li>1. Menggunakan APAR dan alarm kebakaran untuk meminimalisir kerusakan peralatan dan data saat kebakaran terjadi</li> <li>2. Mengadakan latihan evakuasi rutin menggunakan alarm kebakaran untuk memastikan keselamatan personil</li> </ol> | <ol style="list-style-type: none"> <li>1. Menambah infrastruktur perlindungan kebakaran yang lebih efektif, seperti sistem pemadam kebakaran otomatis yang tidak merusak peralatan elektronik</li> <li>2. Menyusun dan mensosialisasikan prosedur darurat yang jelas dan mudah diikuti oleh seluruh staff untuk mengurangi downtime dan risiko finansial serta operasional saat kebakaran terjadi</li> </ol> |

**R15. Tidak ada tim monitoring khusus server**

| INTERNAL<br>EKSTERNAL                                                                                                                                                                                                                                            | STRENGTH                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | WEAKNESS                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                  | <ol style="list-style-type: none"> <li>1. Sudah ada tim monitoring khusus server memungkinkan pemantauan server secara real-time dan respons cepat terhadap masalah atau Gangguan</li> <li>2. Kolaborasi yang baik antara tim moniotirng server dan tim keamanan siber untuk penanganan insiden</li> </ol>                                                                                                                                                                            | <ol style="list-style-type: none"> <li>1. Ketergantungan pada tim monitoring server dan tim keamanan siber, jika tim monitoring khusus tersebut terlalu terbebani atau kekurangan anggota, efisiensi pemantauan bisa menurun.</li> </ol>                                                                                                                                                                                                                                   |
| OPPORTUNITY                                                                                                                                                                                                                                                      | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | STRATEGIC W-O                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <ol style="list-style-type: none"> <li>1. Pemkab Buleleng memiliki Perbup Nomor 58 Tahun 2019 tentang Tata Kelola Sistem Pemerintahan Berbasis Elektronik di lingkungan Pemkab Buleleng khususnya pada bagian V Sumber Daya Manusia, pasal 17 dan 18.</li> </ol> | <ol style="list-style-type: none"> <li>9. Memanfaatkan tim monitoring khusus yang sudah ada untuk memastikan kepatuhan terhadap Perbup Nomor 58 Tahun 2019 tentang Tata Kelola Sistem Pemerintahan Berbasis Elektronik, khususnya pada bagian V Sumber Daya Manusia, pasal 17 dan 18</li> <li>10. Menggunakan kolaborasi yang baik antara tim monitoring server dan tim keamanan siber untuk mendukung pelatihan dan pengembangan SDM sesuai dengan peraturan yang berlaku</li> </ol> | <ol style="list-style-type: none"> <li>1. Mengurangi ketergantungan pada tim monitoring server dengan melatih dan mengembangkan SDM lain sesuai dengan Perbup Nomor 58 Tahun 2019, pasal 17 dan 18, sehingga ada lebih banyak personel yang mampu melakukan pemantauan server</li> <li>2. Meningkatkan kapasitas dan jumlah anggota tim monitoring server melalui rekrutmen dan pelatihan, sesuai dengan kebutuhan yang diatur dalam Perbup Nomor 58 Tahun 2019</li> </ol> |
| THREAT                                                                                                                                                                                                                                                           | STRATEGIC S-T                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | STRATEGIC W-T                                                                                                                                                                                                                                                                                                                                                                                                                                                              |

|                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                                      |                                                                                                                                                                                                                                                                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. Risiko keamanan siber meningkat jika tidak ada pemantauan yang tepat terhadap aktivitas server dan lalu lintas jaringan, contoh Cyber Crime (Hacker, cracker, virus, malware)</li> <li>2. Kehilangan Data, tanpa pemantauan yang tepat, potensi kehilangan data meningkat karena masalah tidak terdeteksi yang dapat menyebabkan kerusakan data.</li> </ol> | <ol style="list-style-type: none"> <li>1. Menggunakan kemampuan tim monitoring khusus untuk mengidentifikasi dan merespons ancaman keamanan siber dengan cepat, mengurangi risiko kehilangan data dan kerusakan</li> <li>2. Mengembangkan prosedur tanggap darurat yang didukung oleh kolaborasi antara tim monitoring server dan tim keamanan siber untuk menghadapi ancaman cyber crime</li> </ol> | <ol style="list-style-type: none"> <li>1. Mengurangi risiko dengan menyusun rencana kontingensi yang mencakup alternatif pemantauan jika tim monitoring utama terlalu terbebani atau kekurangan anggota</li> <li>2. Mengembangkan dan menerapkan kebijakan backup data yang kuat untuk memastikan bahwa data tetap aman meskipun terjadi masalah pada server atau sistem keamanan</li> </ol> |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### R16. Server mengalami down

| INTERNAL<br>EKSTERNAL                                                                                                    | STRENGTH                                                                                                                                                                                                                                                                                                                                            | WEAKNESS                                                                                                                                                                                                                                                                                                                     |
|--------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                          | <ol style="list-style-type: none"> <li>Memiliki tim IT yang cukup baik untuk mengatasi permasalahan pada server</li> <li>Memiliki infrastruktur TI yang tergolong baik dan layak digunakan, hal ini terdapat dalam RENSTRA Diskominfo 2023-2026</li> <li>Menggunakan teknologi <i>cloud computing</i> untuk efisiensi beban kerja server</li> </ol> | <ol style="list-style-type: none"> <li>Kendala saat konfigurasi</li> <li>Kinerja server melambat</li> <li>Kendala pada <i>hardware</i></li> </ol>                                                                                                                                                                            |
| OPPORTUNITY                                                                                                              | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                       | STRATEGIC W-O                                                                                                                                                                                                                                                                                                                |
| <ol style="list-style-type: none"> <li><i>Internet Service Provider (ISP)</i> yang lebih andal</li> </ol>                | <ol style="list-style-type: none"> <li>Menggunakan tim IT yang kompeten untuk memanfaatkan teknologi cloud computing, meningkatkan efisiensi kerja server</li> <li>Memanfaatkan infrastruktur TI yang baik untuk mengintegrasikan layanan dari ISP yang andal, memastikan konektivitas yang konsisten dan cepat</li> </ol>                          | <ol style="list-style-type: none"> <li>Meningkatkan pelatihan tim untuk mengatasi kendala konfigurasi dan mengoptimalkan kinerja server menggunakan layanan ISP yang lebih andal</li> <li>Mengganti atau memperbarui hardware dengan bantuan ISP yang lebih baik untuk meningkatkan keandalan dan performa sistem</li> </ol> |
| THREAT                                                                                                                   | STRATEGIC S-T                                                                                                                                                                                                                                                                                                                                       | STRATEGIC W-T                                                                                                                                                                                                                                                                                                                |
| <ol style="list-style-type: none"> <li><i>Cyber Crime (Hacking, cracking, virus, malware, phishing, cyber</i></li> </ol> | <ol style="list-style-type: none"> <li>Meningkatkan keamanan sistem dengan menggunakan keahlian tim IT untuk mencegah serangan siber seperti hacking dan malware.</li> </ol>                                                                                                                                                                        | <ol style="list-style-type: none"> <li>Mengembangkan protokol respons yang lebih cepat dan efektif untuk menangani kendala hardware dan kinerja server guna mengurangi</li> </ol>                                                                                                                                            |

|                                                                                                                                                     |                                                                                                                 |                                                                                                                                                                  |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>espionage, cyber terrorism)</i><br>2. Kerugian finansial akibat <i>downtime</i><br>3. Penurunan reputasi akibat penanganan masalah yang tertunda | 2. Memanfaatkan infrastruktur TI yang layak untuk mengurangi <i>downtime</i> dan menghindari kerugian finansial | kerugian finansial dan penurunan reputasi<br>2. Meningkatkan pelatihan keamanan siber dan implementasi alat keamanan untuk mengatasi ancaman seperti cyber crime |
|-----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------|



**R17. Kondisi server yang tidak memadai/tidak layak (Contoh: Server usang)**

| INTERNAL<br>EKSTERNAL                                                                                                            | STRENGTH                                                                                                                                                                                                                                                                                                                                            | WEAKNESS                                                                                                                                                                                                                                                                                                                                  |
|----------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                  | <ol style="list-style-type: none"> <li>Memiliki tim IT yang cukup baik untuk mengatasi permasalahan pada server</li> <li>Memiliki infrastruktur TI yang tergolong baik dan layak digunakan, hal ini terdapat dalam RENSTRA Diskominfo 2023-2026</li> <li>Menggunakan teknologi <i>cloud computing</i> untuk efisiensi beban kerja server</li> </ol> | <ol style="list-style-type: none"> <li>Masih ada server yang telah usang namun tetap digunakan meski performa kurang optimal</li> <li>Kendala pada <i>hardware</i></li> <li>Kinerja server melambat</li> </ol>                                                                                                                            |
| OPPORTUNITY                                                                                                                      | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                       | STRATEGIC W-O                                                                                                                                                                                                                                                                                                                             |
| <ol style="list-style-type: none"> <li>Penggunaan <i>Network Attach Storage</i> (NAS)</li> </ol>                                 | <ol style="list-style-type: none"> <li>Memanfaatkan tim IT yang baik untuk mengintegrasikan penggunaan <i>Network Attach Storage</i> (NAS) agar meningkatkan efisiensi dan keamanan data</li> <li>Menggunakan infrastruktur TI yang layak dan teknologi <i>cloud computing</i> untuk mengoptimalkan kinerja NAS dan beban kerja server</li> </ol>   | <ol style="list-style-type: none"> <li>Mengatasi masalah server yang usang dengan menggantinya atau memperbaruinya dengan solusi NAS untuk meningkatkan performa dan efisiensi</li> <li>Mengurangi kendala pada <i>hardware</i> dan memperbaiki performa server dengan memanfaatkan teknologi NAS yang lebih andal dan efisien</li> </ol> |
| THREAT                                                                                                                           | STRATEGIC S-T                                                                                                                                                                                                                                                                                                                                       | STRATEGIC W-T                                                                                                                                                                                                                                                                                                                             |
| <ol style="list-style-type: none"> <li><i>Cyber Crime</i> (<i>Hacking, cracking, virus, malware, phishing, cyber</i>)</li> </ol> | <ol style="list-style-type: none"> <li>Memanfaatkan tim IT yang kompeten untuk meningkatkan keamanan sistem guna melawan ancaman <i>cyber crime</i></li> </ol>                                                                                                                                                                                      | <ol style="list-style-type: none"> <li>Menggantikan server usang dan memperbaiki kendala hardware untuk mengurangi risiko <i>downtime</i> dan kerugian finansial</li> </ol>                                                                                                                                                               |

|                                                                                    |                                                                                                                                                                            |                                                                                                                                                             |
|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>espionage, cyber terrorism)</i><br>2. Kerugian finansial akibat <i>downtime</i> | 2. Memanfaatkan infrastruktur TI yang baik dan teknologi <i>cloud computing</i> untuk membangun sistem keamanan yang lebih kuat dan tangguh terhadap serangan <i>cyber</i> | 2. Mengatasi kinerja server yang melambat dengan memperbarui perangkat keras dan perangkat lunak serta meningkatkan keamanan terhadap serangan <i>cyber</i> |
|------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|



### R18. Perangkat mengalami overhear dan overload

| INTERNAL<br>EKSTERNAL                                                                                                                                                                                                                                                                                                                                | STRENGTH                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | WEAKNESS                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                                                                                      | <ol style="list-style-type: none"> <li>Memiliki sistem pendingin dalam ruangan server</li> <li>Memiliki prosedur respons cepat untuk menangani situasi <i>overheat</i> dan <i>overload</i></li> <li>Menggunakan teknologi <i>cloud computing</i> untuk efisiensi beban kerja</li> </ol>                                                                                                                                                                                                                                                                   | <ol style="list-style-type: none"> <li>Kinerja server dan layanan melambat</li> <li>Kerusakan pada <i>hardware</i> dan <i>software</i> bila tidak dimonitoring</li> </ol>                                                                                                                                                                         |
| OPPORTUNITY                                                                                                                                                                                                                                                                                                                                          | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | STRATEGIC W-O                                                                                                                                                                                                                                                                                                                                     |
| <ol style="list-style-type: none"> <li>Perbup Buleleng Nomor 79 Tahun 2018 Tentang Standar Operasional Dan Prosedur Manajemen Data Center Pada Pemerintah Kabupaten Buleleng, pada BAB 2, Bagian Kesatu tentang ruang server dan perangkat pendukung, Pasal 5 ayat (1) tentang Ruang server wajib memenuhi standar pendukung bagian a,b,c</li> </ol> | <ol style="list-style-type: none"> <li>Memanfaatkan sistem pendingin dalam ruangan server untuk memastikan ruang server memenuhi standar yang ditetapkan dalam Perbup Buleleng Nomor 79 Tahun 2018</li> <li>Menggunakan prosedur respons cepat untuk <i>overheat</i> dan <i>overload</i> sebagai bagian dari implementasi standar operasional yang tercantum dalam Perbup Buleleng</li> <li>Memanfaatkan teknologi <i>cloud computing</i> untuk mendukung efisiensi dan memenuhi standar perangkat pendukung yang diatur dalam Perbup Buleleng</li> </ol> | <ol style="list-style-type: none"> <li>Mengatasi kinerja server yang melambat dengan memastikan ruang server dan perangkat pendukung sesuai standar yang tercantum dalam Perbup Buleleng</li> <li>Meminimalisir kerusakan hardware dan software dengan meningkatkan monitoring sesuai dengan standar operasional dalam Perbup Buleleng</li> </ol> |

| THREAT                                                                                                                                                                                                                                                                                                                                                         | STRATEGIC S-T                                                                                                                                                                                                                                                                                                                                                                                                        | STRATEGIC W-T                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. Suhu lingkungan yang tinggi dapat meningkatkan risiko <i>overheating</i> perangkat</li> <li>2. Multitasking dapat meningkatkan beban pada perangkat dan menyebabkan <i>overload</i></li> <li>3. <i>Cyber Crime</i> (<i>Hacking, cracking, virus, malware, phishing, cyber espionage, cyber terrorism</i>)</li> </ol> | <ol style="list-style-type: none"> <li>1. Menggunakan sistem pendingin untuk mengurangi risiko <i>overheating</i> akibat suhu lingkungan yang tinggi</li> <li>2. Menggunakan prosedur respons cepat untuk menangani situasi <i>overload</i> akibat multitasking yang berlebihan</li> <li>3. Menggunakan teknologi <i>cloud computing</i> untuk mengurangi risiko yang berkaitan dengan <i>cyber crime</i></li> </ol> | <ol style="list-style-type: none"> <li>1. Meningkatkan efisiensi server dan layanan untuk mengurangi dampak negatif suhu lingkungan yang tinggi</li> <li>2. Meningkatkan monitoring hardware dan <i>software</i> untuk mencegah <i>overload</i> akibat multitasking berlebihan</li> <li>3. Mengurangi risiko <i>cyber crime</i> dengan meningkatkan keamanan dan efisiensi sistem untuk mengatasi kinerja server yang melambat</li> <li>4. Meminimalkan risiko kerusakan hardware dan <i>software</i> dengan langkah-langkah proaktif terhadap ancaman <i>cyber crime</i></li> </ol> |

**R19. Sistem operasi pada server tidak menyediakan interface untuk mengakses dan mengelola server (Contoh: CLI maupun GUI)**

| INTERNAL<br>EKSTERNAL                                                                              | STRENGTH                                                                                                                                                                                      | WEAKNESS                                                                                                                                                                                    |
|----------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                    | Terdapat interface untuk mengelola server                                                                                                                                                     | Kemungkinan kurangnya aksesibilitas dan visibilitas                                                                                                                                         |
| OPPORTUNITY                                                                                        | STRATEGIC S-O                                                                                                                                                                                 | STRATEGIC W-O                                                                                                                                                                               |
| Peningkatan aksesibilitas dan visibilitas untuk keamanan sistem server yang lebih baik             | Memanfaatkan <i>interface</i> yang tersedia untuk meningkatkan aksesibilitas dan visibilitas dalam mengelola server, guna memperkuat keamanan sistem server dan mencegah ancaman <i>cyber</i> | Mengatasi kurangnya aksesibilitas dan visibilitas dengan memanfaatkan peningkatan peluang teknologi untuk keamanan sistem server yang lebih baik                                            |
| THREAT                                                                                             | STRATEGIC S-T                                                                                                                                                                                 | STRATEGIC W-T                                                                                                                                                                               |
| <i>Cyber Crime (Hacking, cracking, virus, malware, phishing, cyber espionage, cyber terrorism)</i> | Menggunakan interface yang ada untuk mengimplementasikan langkah-langkah keamanan guna melindungi server dari ancaman <i>cyber</i> seperti <i>hacking</i> , <i>virus</i> , dan <i>malware</i> | Mengurangi risiko <i>cyber crime</i> dengan memperbaiki kekurangan aksesibilitas dan visibilitas melalui penerapan langkah-langkah keamanan yang lebih ketat dan pemantauan yang lebih baik |

**R20. Tidak melakukan backup data secara berkala atau otomatis**

| INTERNAL    | STRENGTH                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | WEAKNESS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <div></div> | <ol style="list-style-type: none"> <li>1. Di dukung dengan hardware yang baik (Contoh: Hardisk, Hardisk Server, Memory Server, Router, dan Switch) hal ini terdapat dalam RENSTRA Diskominfosanti 2023-2026</li> <li>2. SOP Penyediaan Layanan Government <i>Cloud Computing</i> yang menunjukkan bahwa Diskominfosanti memiliki dan menggunakan <i>cloud computing</i> yang digunakan untuk <i>backup data</i></li> <li>3. Pemkab Buleleng sudah memiliki peta rencana SPBE yang berisikan kriteria manajemen data SPBE</li> <li>4. Memiliki tim IT yang cukup baik untuk Melakukan backup data secara rutin</li> <li>5. Surat Edaran Nomor 400.13.53/1853/T.Kelola.Kominfosanti/VII/2023 mengenai Pedoman Penyelenggaraan Audit Teknologi Informasi Dan Komunikasi (TIK) Lingkup Pemerintah Kabupaten Buleleng berisikan amanat objek Audit TIK diantaranya Infrastruktur SPBE (Pusat data dan jaringan intra Pemkab), Aplikasi SPBE, dan Keamanan Infrastruktur</li> </ol> | <ol style="list-style-type: none"> <li>1. Belum ada pedoman manajemen data SPBE</li> <li>2. Terjadi kesalahan konfigurasi <i>backup</i></li> <li>3. Tidak ada SOP <i>backup data</i></li> <li>4. Belum ada jadwal yang dibuat khusus untuk Melakukan backup data secara rutin</li> <li>5. Kekurangan <i>Network Attach Storage</i> (NAS) untuk Melakukan backup data secara rutin secara berkala dan otomatis</li> <li>6. Kegagalan sistem perangkat keras seperti kerusakan infrastruktur misalkan dengan terjadinya hardisk error</li> </ol> |
| EKSTERNAL   | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | STRATEGIC W-O                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| OPPORTUNITY |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |

|                                                                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                                    |                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>1. Pemkab Buleleng memiliki Perbup Nomor 49 Tahun 2022 tentang Satu Data Daerah, pada pasal 13 bagian keempat tentang penyebaran data, ayat (5) bahwa pengelolaan data dilakukan oleh bidang komunikasi dan informatika, urusan pemerintahan bidang persandian, dan urusan pemerintahan bidang statistik</p> | <p>1. Mengoptimalkan <i>hardware</i> yang baik dan <i>cloud computing</i> untuk mendukung implementasi Perbup Nomor 49 Tahun 2022 tentang Satu Data Daerah</p> <p>2. Memanfaatkan tim IT yang kompeten untuk melakukan <i>backup data</i> secara rutin sesuai dengan SOP yang ada dan mendukung pengelolaan data berdasarkan peta rencana SPBE</p> | <p>1. Mengembangkan pedoman manajemen data SPBE dan SOP backup data berdasarkan Perbup Nomor 49 Tahun 2022</p> <p>2. Menyusun jadwal rutin untuk <i>backup data</i> dan mengatasi kekurangan NAS melalui alokasi anggaran atau hibah dari pemerintah pusat</p> |
| <b>THREAT</b>                                                                                                                                                                                                                                                                                                   | <b>STRATEGIC S-T</b>                                                                                                                                                                                                                                                                                                                               | <b>STRATEGIC W-T</b>                                                                                                                                                                                                                                           |
| <p>1. Bencana Alam (Contoh: Banjir, Kebakaran, dll)</p>                                                                                                                                                                                                                                                         | <p>1. Memastikan <i>hardware</i> yang baik dan <i>cloud computing</i> dilindungi dari ancaman bencana alam dan <i>cyber crime</i> melalui kebijakan keamanan data yang ketat</p>                                                                                                                                                                   | <p>1. Mengatasi kesalahan konfigurasi backup dan kekurangan SOP dengan segera membuat pedoman dan SOP yang diperlukan untuk mengurangi</p>                                                                                                                     |

|                                                                                                                                                                                                                      |                                                                                                                                                                                  |                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>2. Kehilangan data atau kerusakan data</p> <p>3. <i>Cyber Crime (Hacking, cracking, virus, malware, phishing, cyber espionage, cyber terrorism)</i></p> <p>4. Pencurian data akibat kerusakan <i>hardware</i></p> | <p>2. Mengadakan audit rutin sesuai dengan Surat Edaran Nomor 400.13.53/1853/T.Kelola.KominfoSanti/VII/2023 untuk mengidentifikasi potensi kerusakan data dan pencurian data</p> | <p>risiko kehilangan data atau kerusakan data</p> <p>2. Mengatasi kegagalan sistem perangkat keras dengan meningkatkan pemeliharaan dan perbaikan infrastruktur secara berkala serta menambahkan sistem backup yang lebih andal.</p> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



### R21. Maintenance tidak terjadwal

| INTERNAL<br>EKSTERNAL                                                                                                                                                                                 | STRENGTH                                                                                                                                                                                                                                                                                                                                   | WEAKNESS                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                       | <ol style="list-style-type: none"> <li>1. <i>Maintenance</i> terjadwal</li> <li>2. Pemkab Buleleng sudah memiliki peta rencana SPBE yang berisikan kriteria manajemen data SPBE</li> </ol>                                                                                                                                                 | <ol style="list-style-type: none"> <li>1. Belum ada pedoman manajemen data SPBE</li> <li>2. Kemungkinan terjadinya <i>downtime</i> saat sistem tidak di maintenance dengan baik</li> </ol>                                                                                                                                                                                    |
| OPPORTUNITY                                                                                                                                                                                           | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                              | STRATEGIC W-O                                                                                                                                                                                                                                                                                                                                                                 |
| <ol style="list-style-type: none"> <li>1. Pemkab Buleleng memiliki Perbup Nomor 49 Tahun 2022 tentang Satu Data Daerah, pada pasal 13 bagian keempat tentang penyebarluasan data, ayat (5)</li> </ol> | <ol style="list-style-type: none"> <li>1. Memanfaatkan jadwal maintenance yang teratur untuk memastikan pemenuhan standar manajemen data yang tercantum dalam peta rencana SPBE</li> <li>2. Mengoptimalkan pemanfaatan Perbup Nomor 49 Tahun 2022 untuk memastikan penyebarluasan data dilakukan sesuai dengan standar yang ada</li> </ol> | <ol style="list-style-type: none"> <li>1. Menyusun dan mengimplementasikan pedoman manajemen data SPBE dengan mengacu pada Perbup Nomor 49 Tahun 2022 untuk meningkatkan kualitas manajemen data</li> <li>2. Memanfaatkan kesempatan dari Perbup untuk mendapatkan dukungan dalam meminimalisir downtime melalui pemeliharaan dan pengelolaan data yang lebih baik</li> </ol> |
| THREAT                                                                                                                                                                                                | STRATEGIC S-T                                                                                                                                                                                                                                                                                                                              | STRATEGIC W-T                                                                                                                                                                                                                                                                                                                                                                 |
| <ol style="list-style-type: none"> <li>1. Kehilangan data atau kerusakan data</li> </ol>                                                                                                              | <ol style="list-style-type: none"> <li>1. Menggunakan jadwal maintenance teratur untuk meminimalkan risiko kehilangan atau</li> </ol>                                                                                                                                                                                                      | <ol style="list-style-type: none"> <li>1. Mengembangkan pedoman manajemen data SPBE yang kuat untuk mengurangi risiko</li> </ol>                                                                                                                                                                                                                                              |

|                                                                                                                         |                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                    |
|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>2. <i>Cyber Crime</i><br/>(<i>Hacking, cracking, virus, malware, phishing, cyber espionage, cyber terrorism</i>)</p> | <p>kerusakan data dan memastikan proteksi terhadap ancaman <i>cyber crime</i></p> <p>2. Mengimplementasikan kriteria manajemen data dari peta rencana SPBE sebagai langkah pencegahan terhadap serangan <i>cyber</i></p> | <p>kehilangan atau kerusakan data serta ancaman <i>cyber crime</i></p> <p>2. Meningkatkan frekuensi dan kualitas <i>maintenance</i> untuk memastikan sistem selalu dalam kondisi optimal dan mengurangi <i>downtime</i> yang dapat dimanfaatkan oleh pelaku <i>cyber crime</i></p> |
|-------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



## R22. Server mengalami serangan (Contoh: Virus)

| INTERNAL                                                                                                                                                                                   | STRENGTH                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | WEAKNESS                                                                                                                                                                                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                            | <ol style="list-style-type: none"> <li>1. Ada langkah penanganan dengan mengecek log dari server dimana sistem diserang</li> <li>2. Kolaborasi yang baik antara tim moniotirng server dan tim keamanan siber untuk penanganan insiden</li> <li>3. Meningkatkan keamanan SPBE melalui perbaikan dari hasil IT Security Assessment dari BSSN tahun 2022 dengan Nomor Laporan Dokumen 030/D21/LAP/03/2022</li> <li>4. Serah Terima perangkat Honeypot (honeypot adalah sistem tidak terlindungi yang menarik peretas dan mengumpulkan data tentang taktik dan teknik mereka) kepada Dinas Kominfosanti pada 24 September 2019 berdasarkan PKS BSSN Nomor 075/18/PKS/PEM/2019</li> </ol> | <ol style="list-style-type: none"> <li>1. Belum ada pedoman manajemen keamanan informasi SPBE</li> <li>2. Terjadi <i>web defacement</i></li> <li>3. Belum semua perangkat diinstall antivirus</li> </ol> |
| EKSTERNAL                                                                                                                                                                                  | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        | STRATEGIC W-O                                                                                                                                                                                            |
| <b>OPPORTUNITY</b><br><ol style="list-style-type: none"> <li>1. Serah Terima perangkat Honeypot (honeypot adalah sistem tidak terlindungi yang menarik peretas dan mengumpulkan</li> </ol> | <ol style="list-style-type: none"> <li>1. Meningkatkan kolaborasi antara tim monitoring server dan tim keamanan siber untuk memaksimalkan penggunaan perangkat Honeypot dalam mengidentifikasi dan mencegah serangan</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <ol style="list-style-type: none"> <li>1. Mengembangkan pedoman manajemen keamanan informasi SPBE dengan dukungan dari perangkat Honeypot dan program sertifikasi TI</li> </ol>                          |

|                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p>data tentang taktik dan teknik mereka) kepada Dinas Kominfosanti pada 24 September 2019 berdasarkan PKS BSSN Nomor 075/18/PKS/PEM/2019</p> <p>2. Program sertifikasi TI support kepada tim TI dan atau calon pegawai/staff</p> | <p>2. Menggunakan hasil IT Security <i>Assessment</i> dari BSSN untuk meningkatkan keamanan SPBE, serta memanfaatkan program sertifikasi TI untuk meningkatkan kemampuan tim TI</p>                                                                                                                                            | <p>2. Memastikan semua perangkat diinstall antivirus sebagai langkah pencegahan awal terhadap ancaman yang telah diidentifikasi oleh Honeypot</p>                                                                                                                             |
| <b>THREAT</b>                                                                                                                                                                                                                     | <b>STRATEGIC S-T</b>                                                                                                                                                                                                                                                                                                           | <b>STRATEGIC W-T</b>                                                                                                                                                                                                                                                          |
| <p>1. <i>Cyber Crime (Worm, Trojan, Ransomware, Spyware, Adware, Cryptominer, File-Infected Viruses, etc)</i></p>                                                                                                                 | <p>1. Menggunakan log server dan kolaborasi tim untuk mendeteksi dan merespons dengan cepat terhadap serangan <i>cyber</i> seperti Worm, Trojan, Ransomware, dan lainnya</p> <p>2. Menerapkan perbaikan hasil IT Security <i>Assessment</i> dari BSSN untuk memperkuat sistem terhadap berbagai jenis ancaman <i>cyber</i></p> | <p>1. Menyusun dan menerapkan pedoman manajemen keamanan informasi SPBE untuk mengurangi risiko <i>web defacement</i> dan serangan lainnya</p> <p>2. Memastikan semua perangkat dilengkapi antivirus untuk mencegah serangan <i>malware</i> dan <i>cybercrime</i> lainnya</p> |

**R23. Data corrupt**

| INTERNAL<br>EKSTERNAL                                                                                                                            | STRENGTH                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | WEAKNESS                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                  | <ol style="list-style-type: none"> <li>1. Surat Edaran nomor 400.13.53/1853/T.Kelola.Kominfosanti/VII/2023 mengenai Pedoman Penyelenggaraan Audit Teknologi Informasi Dan Komunikasi (TIK) Lingkup Pemerintah Kabupaten Buleleng berisikan amanat objek Audit TIK diantaranya Infrastruktur SPBE (Pusat data dan jaringan intra Pemkab), Aplikasi SPBE, dan Keamanan Infrastruktur.</li> <li>2. SOP Penyediaan Layanan <i>Government Cloud Computing</i> yang menunjukkan bahwa Diskominfosanti memiliki dan menggunakan <i>cloud computing</i></li> <li>3. Pemkab Buleleng sudah memiliki peta rencana SPBE yang berisikan kriteria manajemen data SPBE</li> <li>4. Memiliki tim IT yang cukup baik untuk melakukan <i>backup data</i></li> </ol> | <ol style="list-style-type: none"> <li>1. Belum ada pedoman manajemen data SPBE</li> <li>2. Kegagalan sistem perangkat keras seperti kerusakan infrastruktur seperti dengan terjadinya <i>hardisk error</i></li> <li>3. Tidak ada SOP pemulihan data rusak atau data hilang</li> </ol> |
| OPPORTUNITY                                                                                                                                      | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | STRATEGIC W-O                                                                                                                                                                                                                                                                          |
| <ol style="list-style-type: none"> <li>1. Pemkab Buleleng memiliki Perbup Nomor 49 Tahun 2022 tentang Satu Data Daerah, pada pasal 13</li> </ol> | <ol style="list-style-type: none"> <li>1. Manfaatkan keberadaan Perbup Nomor 49 Tahun 2022 tentang Satu Data Daerah untuk memperkuat infrastruktur SPBE, aplikasi, dan keamanan infrastruktur yang telah diamankan</li> </ol>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <ol style="list-style-type: none"> <li>1. Kembangkan pedoman manajemen data SPBE dengan memanfaatkan dasar hukum dari Perbup Nomor 49 Tahun 2022 tentang Satu Data Daerah</li> </ol>                                                                                                   |

|                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| bagian keempat tentang penyebaran data, ayat (5)                                                                                                                                                            | <p>dalam Surat Edaran No. 400.13.53/1853/T.Kelola.KominfoSanti/VII/2023</p> <ol style="list-style-type: none"> <li>Gunakan kemampuan <i>cloud computing</i> yang dimiliki oleh DiskominfoSanti untuk memfasilitasi penyebaran data sesuai dengan Perbup Nomor 49 Tahun 2022</li> <li>Manfaatkan tim IT yang kompeten untuk mengimplementasikan manajemen data SPBE yang sesuai dengan peta rencana SPBE Pemkab Buleleng</li> </ol>                                                                                                                | <ol style="list-style-type: none"> <li>Buat SOP pemulihan data rusak atau data hilang dengan memperhatikan ketentuan dalam Perbup Nomor 49 Tahun 2022 tentang penyebaran data</li> <li>Investasikan dalam teknologi yang lebih handal untuk mengurangi risiko kegagalan sistem perangkat keras</li> </ol>                                                                                                                                                                                                                       |
| <b>THREAT</b>                                                                                                                                                                                               | <b>STRATEGIC S-T</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | <b>STRATEGIC W-T</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <ol style="list-style-type: none"> <li>Bencana Alam (Contoh: Banjir, Kebakaran, dll)</li> <li><i>Cyber Crime (Hacking, cracking, virus, malware, phishing, cyber espionage, cyber terrorism)</i></li> </ol> | <ol style="list-style-type: none"> <li>Tingkatkan keamanan infrastruktur SPBE dengan memanfaatkan amanat dalam Surat Edaran No. 400.13.53/1853/T.Kelola.KominfoSanti/VII/2023 untuk melindungi dari ancaman <i>cyber crime</i></li> <li>Implementasikan solusi backup data secara berkala dan otomatis melalui tim IT untuk mengurangi dampak bencana alam terhadap data</li> <li>Gunakan layanan <i>cloud computing</i> yang ada untuk membuat cadangan data di lokasi yang aman dan berbeda guna mengurangi risiko dari bencana alam</li> </ol> | <ol style="list-style-type: none"> <li>Kembangkan SOP pemulihan data dan manajemen risiko yang mencakup prosedur menghadapi bencana alam dan ancaman <i>cyber crime</i></li> <li>Lakukan pelatihan rutin bagi tim IT untuk menangani kegagalan perangkat keras dan meningkatkan kesiapsiagaan terhadap ancaman <i>cyber crime</i></li> <li>Buat mekanisme monitoring dan audit berkala terhadap infrastruktur TIK untuk mendeteksi dan mengatasi masalah sebelum terjadi kegagalan sistem atau serangan <i>cyber</i></li> </ol> |

**R24. Tidak melakukan *back up data* dan *system server* secara berkala**

| INTERNAL<br>EKSTERNAL                                                                                                                                                                                                                                                             | STRENGTH                                                                                                                                                                                                                                                                                                                                                                                        | WEAKNESS                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                                   | <ol style="list-style-type: none"> <li>1. Di dukung dengan hardware yang baik (Contoh: Hardisk, Hardisk Server, Memory Server, Router, dan Switch) hal ini terdapat dalam RENSTRA Diskominfo 2023-2026</li> <li>2. SOP Penyediaan Layanan <i>Government Cloud Computing</i></li> <li>3. Pemkab Buleleng sudah memiliki peta rencana SPBE yang berisikan kriteria manajemen data SPBE</li> </ol> | <ol style="list-style-type: none"> <li>1. Belum ada pedoman manajemen data SPBE</li> <li>2. Terjadi kesalahan konfigurasi <i>backup</i></li> <li>3. Tidak ada SOP <i>backup data</i></li> </ol>                                                                                                                                                |
| OPPORTUNITY                                                                                                                                                                                                                                                                       | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                                                                   | STRATEGIC W-O                                                                                                                                                                                                                                                                                                                                  |
| <ol style="list-style-type: none"> <li>1. Pemkab Buleleng memiliki Perbup Nomor 49 Tahun 2022 tentang Satu Data Daerah, pada pasal 13 bagian keempat tentang penyebaran data, ayat (5) bahwa pengelolaan data dilakukan oleh bidang komunikasi dan informatika, urusan</li> </ol> | <ol style="list-style-type: none"> <li>1. Mengoptimalkan penggunaan <i>hardware</i> yang ada untuk mendukung implementasi Perbup No. 49 Tahun 2022</li> <li>2. Menerapkan SOP <i>Government Cloud</i> untuk meningkatkan kualitas pengelolaan data</li> <li>3. Memanfaatkan peta rencana SPBE untuk mendukung penerapan Perbup No. 49 Tahun 2022</li> </ol>                                     | <ol style="list-style-type: none"> <li>1. Mengembangkan pedoman manajemen data SPBE berdasarkan Perbup No. 49 Tahun 2022</li> <li>2. Melakukan pelatihan dan peningkatan kapasitas dalam konfigurasi <i>backup</i></li> <li>3. Menyusun dan mengimplementasikan SOP <i>backup data</i> yang selaras dengan Perbup No. 49 Tahun 2022</li> </ol> |

|                                                                                                                                                                                                                                                                   |                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| pemerintahan bidang persandian, dan urusan pemerintahan bidang statistik                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                          |                                                                                                                                                                                                                                                                                                                                                         |
| <b>THREAT</b>                                                                                                                                                                                                                                                     | <b>STRATEGIC S-T</b>                                                                                                                                                                                                                                                                                     | <b>STRATEGIC W-T</b>                                                                                                                                                                                                                                                                                                                                    |
| <ol style="list-style-type: none"> <li>1. Bencana Alam (Contoh: Banjir, Kebakaran, dll)</li> <li>2. Kehilangan data atau kerusakan data</li> <li>3. <i>Cyber Crime (Hacking, cracking, virus, malware, phishing, cyber espionage, cyber terrorism)</i></li> </ol> | <ol style="list-style-type: none"> <li>1. Membangun infrastruktur fisik yang tahan terhadap bencana alam</li> <li>2. Menggunakan <i>Government Cloud</i> untuk menjaga keamanan dan keberlanjutan data</li> <li>3. Mengimplementasikan kebijakan keamanan siber berdasarkan peta rencana SPBE</li> </ol> | <ol style="list-style-type: none"> <li>1. Menyusun pedoman manajemen data SPBE yang termasuk mitigasi risiko bencana alam</li> <li>2. Mengembangkan SOP dan pelatihan khusus untuk konfigurasi <i>backup</i> guna mengurangi risiko kehilangan data</li> <li>3. Menyusun SOP <i>backup data</i> yang juga mengandung protokol keamanan siber</li> </ol> |

**R25. Tidak dilakukan kelola hak akses pengguna**

| INTERNAL<br>EKSTERNAL                                                                                                                                                                                                                                                  | STRENGTH                                                                                                                                                                                                                           | WEAKNESS                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                                        | 1. Memiliki kebijakan yang bisa masuk ke dalam ruang server hanya yang berkepentingan, seperti bidang tata kelola dan SDM SPBE kaku bidang infrastruktur & layanan SPBE, serta teknisi/programmer saja                             | 1. Pencatatan masih manual                                                                                                                                                                                                                  |
| OPPORTUNITY                                                                                                                                                                                                                                                            | STRATEGIC S-O                                                                                                                                                                                                                      | STRATEGIC W-O                                                                                                                                                                                                                               |
| 1. Perbup Buleleng Nomor 79 Tahun 2018 Tentang Standar Operasional Dan Prosedur Manajemen Data Center Pada Pemerintah Kabupaten Buleleng, pada BAB 2, Bagian Kesatu tentang ruang server dan perangkat pendukung, Pasal 5 ayat (6) tentang Akses Fisik ke Ruang Server | Memanfaatkan kebijakan yang ada untuk memastikan hanya yang berkepentingan yang memiliki akses ke ruang server sesuai dengan Perbup Buleleng Nomor 79 Tahun 2018, yang akan meningkatkan keamanan dan manajemen <i>data center</i> | Mengimplementasikan sistem pencatatan digital untuk menggantikan pencatatan manual, dengan mengacu pada standar operasional dan prosedur yang tercantum dalam Perbup Buleleng Nomor 79 Tahun 2018, untuk meningkatkan efisiensi dan akurasi |
| THREAT                                                                                                                                                                                                                                                                 | STRATEGIC S-T                                                                                                                                                                                                                      | STRATEGIC W-T                                                                                                                                                                                                                               |

|                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                   |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ol style="list-style-type: none"> <li>1. Kehilangan data atau kerusakan data</li> <li>2. <i>Cyber Crime</i> (<i>Hacking, cracking, virus, malware, phishing, cyber espionage, cyber terrorism</i>)</li> </ol> | <p>Memfaatkan kebijakan akses terbatas ke ruang server untuk mengurangi risiko kehilangan atau kerusakan data serta mencegah ancaman <i>cyber crime</i> dengan memastikan hanya individu yang terlatih dan berkepentingan yang dapat mengakses ruang server</p> | <p>Mengembangkan dan mengimplementasikan prosedur pencadangan data yang teratur serta sistem keamanan yang kuat untuk melindungi data dari kehilangan, kerusakan, dan ancaman <i>cyber crime</i>, sambil beralih dari pencatatan manual ke pencatatan digital</p> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|



## R26. Pemakaian software non orisinal

| INTERNAL<br>EKSTERNAL                                                                                                                                                                                                                                       | STRENGTH                                                                                                                                                                                                                                                                                                                                                             | WEAKNESS                                                                                                                                                                                                                                                                                                         |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                                                                             | <ol style="list-style-type: none"> <li>Seluruh <i>software</i> yang diinstal memiliki lisensi orisinal</li> <li>Telah melakukan sosialisasi dan pelatihan penggunaan <i>software</i> orisinal</li> </ol>                                                                                                                                                             | <ol style="list-style-type: none"> <li><i>Software</i> non orisinal akan berisiko pada kinerja layanan</li> <li><i>Software</i> non orisinal akan berisiko mengalami serangan siber</li> </ol>                                                                                                                   |
| OPPORTUNITY                                                                                                                                                                                                                                                 | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                                        | STRATEGIC W-O                                                                                                                                                                                                                                                                                                    |
| <ol style="list-style-type: none"> <li>Perbup Buleleng Nomor 79 Tahun 2018 Tentang Standar Operasional Dan Prosedur Manajemen Data Center Pada Pemerintah Kabupaten Buleleng, pada BAB 2, Bagian Kedua tentang perangkat lunak, Pasal 6 ayat (2)</li> </ol> | <ol style="list-style-type: none"> <li>Memanfaatkan lisensi orisinal untuk memenuhi standar operasional yang diatur dalam Perbup Buleleng Nomor 79 Tahun 2018</li> <li>Menggunakan pelatihan dan sosialisasi yang sudah dilakukan untuk memastikan semua staf memahami pentingnya penggunaan <i>software</i> orisinal sesuai dengan regulasi yang berlaku</li> </ol> | <ol style="list-style-type: none"> <li>Menggantikan <i>software</i> non orisinal dengan <i>software</i> orisinal untuk mengurangi risiko terhadap kinerja layanan</li> <li>Melakukan pelatihan tambahan tentang keamanan siber untuk mengurangi risiko serangan terhadap <i>software</i> non orisinal</li> </ol> |
| THREAT                                                                                                                                                                                                                                                      | STRATEGIC S-T                                                                                                                                                                                                                                                                                                                                                        | STRATEGIC W-T                                                                                                                                                                                                                                                                                                    |
| <ol style="list-style-type: none"> <li><i>Cyber Crime (Hacking, cracking, virus, malware, phishing, cyber</i></li> </ol>                                                                                                                                    | <ol style="list-style-type: none"> <li>Memanfaatkan lisensi orisinal untuk meningkatkan keamanan terhadap ancaman siber seperti <i>hacking, malware, dan phishing</i></li> </ol>                                                                                                                                                                                     | <ol style="list-style-type: none"> <li>Segera mengganti semua <i>software</i> non orisinal dengan <i>software</i> orisinal untuk mencegah potensi serangan siber dan kehilangan data</li> </ol>                                                                                                                  |

|                                                                              |                                                                                                                          |                                                                                                                                       |
|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| <i>espionage, cyber terrorism)</i><br>2. Kehilangan data atau kerusakan data | 2. Menggunakan pelatihan dan sosialisasi untuk meningkatkan kesadaran staf tentang ancaman siber dan cara menghindarinya | 2. Menerapkan prosedur <i>backup</i> dan pemulihan data yang kuat untuk mengurangi dampak dari potensi kehilangan atau kerusakan data |
|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|



**R27. Dokumentasi atau tata cara penggunaan program / aplikasi tidak lengkap**

| INTERNAL<br>EKSTERNAL                          | STRENGTH                                                                                                                                                                                  | WEAKNESS                                                                                                                                                                                                                                                         |
|------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                | Sedang dalam proses pengajuan untuk membuat panduan pengguna setiap layanan                                                                                                               | Layanan kehilangan pengguna                                                                                                                                                                                                                                      |
| OPPORTUNITY                                    | STRATEGIC S-O                                                                                                                                                                             | STRATEGIC W-O                                                                                                                                                                                                                                                    |
| <i>Usability Testing</i>                       | Memfaatkan proses pembuatan panduan pengguna untuk meningkatkan usability testing sehingga layanan lebih mudah digunakan dan meningkatkan pengalaman pengguna                             | Menggunakan hasil usability testing untuk mengidentifikasi dan memperbaiki faktor-faktor yang menyebabkan kehilangan pengguna. Panduan pengguna yang jelas juga bisa membantu menarik kembali pengguna yang hilang                                               |
| THREAT                                         | STRATEGIC S-T                                                                                                                                                                             | STRATEGIC W-T                                                                                                                                                                                                                                                    |
| Kerugian reputasi penurunan kepercayaan publik | Menggunakan panduan pengguna yang komprehensif untuk menjaga reputasi dan meningkatkan kepercayaan publik terhadap layanan, sehingga dapat mengurangi risiko penurunan kepercayaan publik | Mengidentifikasi penyebab utama kehilangan pengguna dan bekerja untuk memperbaikinya dengan meningkatkan kualitas layanan melalui panduan pengguna yang baik dan hasil dari usability testing, untuk mencegah kerugian reputasi dan penurunan kepercayaan publik |

**R28. Antar muka (user interface) program atau aplikasi susah dipahami**

| INTERNAL<br>EKSTERNAL                          | STRENGTH                                                                                                                                           | WEAKNESS                                                                                                                          |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|
|                                                | Terdapat <i>interface</i> untuk mengelola server                                                                                                   | Kemungkinan kurangnya aksesibilitas dan visibilitas                                                                               |
| OPPORTUNITY                                    | STRATEGIC S-O                                                                                                                                      | STRATEGIC W-O                                                                                                                     |
| <i>Usability Testing</i>                       | Memanfaatkan interface pengelolaan server yang ada untuk melakukan Usability Testing dan meningkatkan pengalaman pengguna                          | Meningkatkan aksesibilitas dan visibilitas melalui Usability Testing, sehingga pengguna dapat lebih mudah mengelola server        |
| THREAT                                         | STRATEGIC S-T                                                                                                                                      | STRATEGIC W-T                                                                                                                     |
| Kerugian reputasi penurunan kepercayaan publik | Menggunakan interface yang ada untuk memperbaiki dan mengoptimalkan sistem guna mengurangi risiko kerugian reputasi dan menjaga kepercayaan publik | Mengatasi kekurangan aksesibilitas dan visibilitas dengan cepat untuk mencegah penurunan kepercayaan publik dan kerugian reputasi |

**R29. Layanan berbasis elektronik yang belum stabil tetapi digunakan**

| INTERNAL<br>EKSTERNAL                                                                                                                     | STRENGTH                                                                                                                                                                                                                                                                                                                                                   | WEAKNESS                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                           | Terdapat layanan berbasis elektronik yang wajib untuk digunakan                                                                                                                                                                                                                                                                                            | Layanan tidak stabil                                                                                                                                                                                                                                                                                                                                                                                                     |
| OPPORTUNITY                                                                                                                               | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                              | STRATEGIC W-O                                                                                                                                                                                                                                                                                                                                                                                                            |
| Sosialisasi penggunaan layanan berbasis elektronik oleh beberapa instansi pusat disesuaikan dengan penyediaan layanan yang akan digunakan | <ol style="list-style-type: none"> <li>1. Mengoptimalkan layanan berbasis elektronik yang wajib digunakan melalui sosialisasi yang efektif oleh instansi pusat</li> <li>2. Memanfaatkan kewajiban penggunaan layanan elektronik untuk memperkuat koordinasi dengan instansi pusat dalam rangka meningkatkan pemahaman dan keterampilan pengguna</li> </ol> | <ol style="list-style-type: none"> <li>1. Meningkatkan stabilitas layanan elektronik melalui pengembangan infrastruktur dan dukungan teknis yang memadai, didorong oleh sosialisasi dan feedback dari instansi pusat</li> <li>2. Menggunakan sosialisasi oleh instansi pusat sebagai alat untuk mengidentifikasi dan mengatasi kelemahan layanan, sehingga dapat meningkatkan kualitas dan stabilitas layanan</li> </ol> |
| THREAT                                                                                                                                    | STRATEGIC S-T                                                                                                                                                                                                                                                                                                                                              | STRATEGIC W-T                                                                                                                                                                                                                                                                                                                                                                                                            |
| Kerugian reputasi penurunan kepercayaan publik                                                                                            | <ol style="list-style-type: none"> <li>1. Menggunakan kewajiban penggunaan layanan elektronik sebagai momentum untuk meningkatkan reputasi dan kepercayaan publik dengan menunjukkan komitmen terhadap kualitas layanan</li> </ol>                                                                                                                         | <ol style="list-style-type: none"> <li>1. Memperbaiki stabilitas layanan untuk menghindari kerugian reputasi dan penurunan kepercayaan publik dengan fokus pada peningkatan infrastruktur dan layanan pelanggan</li> </ol>                                                                                                                                                                                               |

|  |                                                                                                                                                       |                                                                                                                                                     |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
|  | 2. Mengimplementasikan strategi komunikasi yang transparan terkait penggunaan layanan berbasis elektronik untuk mencegah penurunan kepercayaan publik | 2. Mengembangkan rencana mitigasi risiko untuk mengatasi potensi gangguan layanan yang dapat berdampak negatif pada reputasi dan kepercayaan publik |
|--|-------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|



**R30. Tidak ada sosialisasi dan pelatihan teknis sebelum perangkat lunak digunakan secara massif di organisasi**

| INTERNAL<br>EKSTERNAL                                                                                                                                                                          | STRENGTH                                                                                                                                                                                                                                                                                                                                                                                                       | WEAKNESS                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                                                                                                                                | <ol style="list-style-type: none"> <li>1. Efisiensi biaya operasional</li> <li>2. Efisiensi kinerja layanan</li> </ol>                                                                                                                                                                                                                                                                                         | <ol style="list-style-type: none"> <li>1. Kesalahan pengguna</li> </ol>                                                                                                                                                                                                                        |
| OPPORTUNITY                                                                                                                                                                                    | STRATEGIC S-O                                                                                                                                                                                                                                                                                                                                                                                                  | STRATEGIC W-O                                                                                                                                                                                                                                                                                  |
| <ol style="list-style-type: none"> <li>1. Sosialisasi penggunaan layanan berbasis elektronik oleh beberapa instansi pusat disesuaikan dengan penyediaan layanan yang akan digunakan</li> </ol> | <ol style="list-style-type: none"> <li>1. Memanfaatkan efisiensi biaya operasional dan kinerja layanan untuk mendukung program sosialisasi penggunaan layanan berbasis elektronik oleh beberapa instansi pusat</li> <li>2. Menggunakan efisiensi layanan untuk meningkatkan kualitas dan kecepatan dalam penyediaan layanan, sehingga lebih menarik bagi instansi pusat yang melakukan sosialisasi.</li> </ol> | <ol style="list-style-type: none"> <li>1. Mengurangi kesalahan pengguna melalui pelatihan dan sosialisasi yang diselenggarakan oleh instansi pusat</li> <li>2. Menyediakan panduan penggunaan yang lebih mudah dipahami dan akses bantuan cepat untuk mengurangi kesalahan pengguna</li> </ol> |
| THREAT                                                                                                                                                                                         | STRATEGIC S-T                                                                                                                                                                                                                                                                                                                                                                                                  | STRATEGIC W-T                                                                                                                                                                                                                                                                                  |
| <ol style="list-style-type: none"> <li>1. <i>Cyber Crime (Hacking, cracking, virus, malware, phishing, cyber espionage, cyber terrorism)</i></li> </ol>                                        | <ol style="list-style-type: none"> <li>1. Meningkatkan efisiensi kinerja layanan untuk memperkuat sistem keamanan dan melindungi dari ancaman <i>cyber crime</i></li> <li>2. Menggunakan efisiensi biaya operasional untuk berinvestasi dalam teknologi keamanan terbaru untuk mencegah kerugian reputasi dan penurunan kepercayaan publik</li> </ol>                                                          | <ol style="list-style-type: none"> <li>1. Mengembangkan program pelatihan pengguna yang berfokus pada pengamanan data dan pengenalan terhadap ancaman <i>cyber crime</i></li> <li>2. Meningkatkan kesadaran dan kesiapan terhadap ancaman cyber dengan menyediakan informasi</li> </ol>        |

|                                                         |  |                                                      |
|---------------------------------------------------------|--|------------------------------------------------------|
| 2. Kerugian reputasi<br>penurunan<br>kepercayaan publik |  | keamanan yang relevan dan terkini<br>kepada pengguna |
|---------------------------------------------------------|--|------------------------------------------------------|



## Lampiran 20. Dokumentasi



File Dokumentasi lengkap dapat di lihat melalui <https://bit.ly/Dokumentasi-Kertas-Kerja-Manrisk>



## RIWAYAT HIDUP PENULIS



Vany Adelia Putri lahir di Singaraja pada tanggal 30 November 2002. Penulis lahir dari pasangan suami istri Bapak Suyatno dan Ibu Rela Evi Mariana. Penulis berkebangsaan Indonesia dan beragama Islam. Penulis menyelesaikan pendidikan dasar di MI Maya Seririt dan lulus pada tahun 2014. Kemudian penulis melanjutkan di MTs Negeri 2 Buleleng dan lulus pada tahun 2017.

Pada tahun 2020, penulis lulus dari SMA Negeri 1 Seririt jurusan Matematika dan Ilmu Pengetahuan Alam (MIA) dan melanjutkan ke Sarjana Program Studi Sistem Informasi di Universitas Pendidikan Ganesha. Pada semester akhir tahun 2024 penulis telah menyelesaikan Skripsi yang berjudul ***“PERANCANGAN MANAJEMEN RISIKO OPERASIONAL SPBE PADA DINAS KOMUNIKASI INFORMATIKA PERSANDIAN DAN STATISTIK KABUPATEN BULELENG”***.

