# LAMPIRAN

Lampiran 1. Data Responden

Daftar Responden Wawancara:

| Kode Responden | Nama Responden | Jabatan |
|---|---|---|
| R1 | I Nyoman Murditha, S.Kom.,M.Eng | Kepala Dinas Komunikasi, Informatika dan Persandian Kab. Bangli |
| R2 | I Ketut Yadnya,SH | Kabid Persandian dan Pengamanan Informasi |

Daftar Responden Kuesioner

| Kode Responden | Nama Responden | Jabatan |
|---|---|---|
| R1 | I Wayan Ana Kurniawan,SS | Pranata Komputer |
| R2 | I Putu Yoga Andreyana,S.kom | Pranata Komputer |
| R3 | I Wayan Armada, S.Sos | Sandiman Ahli Muda |
| R4 | I Ketut Suardana,SE | Sandiman Ahli Muda |
| R5 | I Kadek Sutapa | Operator sandi dan Telekomunikasi |
| R6 | I Made Juliawan , SE | Operator sandi dan Telekomunikasi |
| R7 | Ni Nyoman Sriantini,SE | Pengelola Data |
| R8 | I Wayan Artayasa | Teknisi |
| R9 | I Kadek Aldi Oka Ardita | Teknisi |

Lampiran 2. Lembar Wawancara

## LEMBAR WAWANCARA

**BIODATA NARASUMBER**

| | | |
|---|---|---|
| Identitas Instansi Pemerintahan | : | Diskominfosan Kabupaten Bangli |
| Alamat | : | Jalan Brigjen Ngurah Rai No. 30 Telepon: (0366) 93804 |
| Nama Narasumber | : | |
| NIP | : | |
| Jabatan | : | |
| Tanggal Wawancara | : | |
| Tujuan | : | Penggalian Informasi mengenai tata kelola dan kategori sistem TI pada Dinas Komunikasi Informatika dan Persandian Kabupaten Bangli |

## DAFTAR PERTANYAAN (R1 & R2)

**Kategori Sistem Elektronik**

Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan

| NO | Karakteristik Instansi/Perusahaan | Jawaban |
|---|---|---|
| 1 | Nilai investasi sistem elektronik yang terpasang<br>[A] Lebih dari Rp.30 Miliar<br>[B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar<br>[C] Kurang dari Rp.3 Miliar | |
| 2 | Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik<br>[A] Lebih dari Rp.10 Miliar<br>[B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar<br>[C] Kurang dari Rp.1 Miliar | |
| 3 | Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu<br>[A] Peraturan atau Standar nasional dan internasional<br>[B] Peraturan atau Standar nasional<br>[C] Tidak ada Peraturan khusus | |
| 4 | Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik<br>[A] Teknik kriptografi khusus yang disertifikasi oleh Negara<br>[B] Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri<br>[C] Tidak ada penggunaan teknik kriptografi | |
| 5 | Jumlah pengguna Sistem Elektronik<br>[A] Lebih dari 5.000 pengguna<br>[B] 1.000 sampai dengan 5.000 pengguna<br>[C] Kurang dari 1.000 pengguna | |
| 6 | Data pribadi yang dikelola Sistem Elektronik<br>[A] Data pribadi yang memiliki hubungan dengan Data Pribadi | |

| NO | Karakteristik Instansi/Perusahaan | Jawaban |
|---|---|---|
| | lainnya<br>[B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha<br>[C] Tidak ada data pribadi | |
| 7 | Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi<br>[A] Sangat Rahasia<br>[B] Rahasia dan/ atau Terbatas<br>[C] Biasa | |
| 8 | Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi<br>[A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik<br>[B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung<br>[C] Proses yang hanya berdampak pada bisnis perusahaan | |
| 9 | Dampak dari kegagalan Sistem Elektronik<br>[A] Membahayakan pertahanan keamanan negara<br>[B] Tidak tersedianya layanan publik berskala nasional atau berdampak pada layanan di sektor lain<br>[C] Tidak tersedianya layanan publik dalam 1 propinsi atau internal 1 instansi/perusahaan | |
| 10 | Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme)<br>[A] Menimbulkan korban jiwa<br>[B] Terbatas pada kerugian finansial<br>[C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial) | |
| 10 | Untuk dilakukan penilaian pada penelitian ini, maka pada level berapa tingkat kapabilitas yang diharapakan?<br>[Level 2 Managed] (bersifat teknis dan terpisah, belum terdukentasi)<br>[Level 3 Estabilished] (Terdefinisi, dokumentasi, belum terstruktur)<br>[Level 4 Predictable] (diterapkan secara efektif dan selaras)<br>[Level 5 Optimizing] (penerapan yang komprehensif, berkelanjutan) | |

Sumber : (Jenny, 2024; Toolkit Indeks KAMI, 2023)

Tanda tangan & Nama Responden:……..

Lampiran 3. Lembar Kuesioner

KUESIONER
EVALUASI KEAMANAN INFORMASI PEMERINTAH
KABUPATEN BANGLI MENGGUNAKAN KOMBINASI
FRAMEWORK
INDEKS KAMI 5.0 DAN COBIT 2019
(Studi Kasus Dinas Komunikasi Informasi dan Persandian Kabupaten
Bangli)

## A. BIODATA NARASUMBER

| | | |
|---|---|---|
| Identitas Instansi Pemerintahan | : | Diskominfosan Kabupaten Bangli |
| Alamat | : | Jalan Brigjen Ngurah Rai No. 30<br>Telepon: (0366) 93804 |
| Nama Narasumber | : | |
| NIP | : | |
| Jabatan | : | |
| Tanggal Pengisian Kuesioner | : | |

Kuesioner ini disampaikan untuk mengetahui tingkat kemampuan / Capability Level proses keamanan infromasi dibuat berdasarkan INDEKS KAMI 5.0 dan COBIT 2019

Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada kolom TEMUAN yang tersedia. Penilaian didasarkan atas kondisi berikut:

- Yes : Bernilai 1 (menyatakan adanya aktivitas)
- No : Bernilai 0 (menyatakan tidak adanya aktivitas)

Kuesioner diberikan secara bertahap, sesuai dengan tingkat kemampuan yang dinilai. Informasi yang diterima dari kuesioner ini bersifat rahasia dan hanya digunakan untuk kepentingan penelitian. Tidak ada jawaban yang salah dalam menjawab kuesioner ini. Atas bantuannya saya ucapkan terima kasih


Dewi, G. K. (2021). Analisis Keamanan Sistem Informasi Universitas X. *ABIS: Accounting and Business Information Systems Journal*, *9*(1). https://doi.org/10.22146/abis.v9i1.64235

ISACA COBIT Design Guide. (2019). COBIT® 2019 Design Guide - Designing an Information and Technology Governance Solution. In *www.icasa.org/COBITuse*.

ISACA COBIT Governance and Management Objectives. (2019). COBIT® 2019 Framework - Governance and Management Objectives. In *COBIT® 2019 Framework*.

Jenny, M. S. (2024). Analisis Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.2 Pada Sistem Informasi Akademik (SIMAK) Universitas Siliwangi. *JURNAL SISTEM INFORMASI DAN TENOLOGI*, 73–80. https://doi.org/10.24176/sitech.v7i1.12390

Pratiwi, H. A., & Wulandari, L. (2021). Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 pada Dinas Komunikasi dan Informatika Kota Bogor. *Journal of Industrial Engineering & Management Research*, *2*(5), 146–163.

Toolkit Indeks KAMI. (2023). *Toolkit Indeks KAMI Versi 5.0.16 Agustus 2023*.

**B. Penilaian tingkat kemampuan /Capability level 2 (COBIT 2019)**

Pada level ini proses telah direncanakan, dilaksanakan, dimonitor, dan disesuaikan secara memadai, sehingga hasil kerja proses dikelola dan diverifikasi..

**EDM03 Ensure Risk Optimisation**

**TUJUAN :** Untuk meminimalkan potensi dampak negatif. Tujuan dari optimasi risiko bukan hanya untuk menghindari risiko, tetapi juga untuk memanfaatkan peluang yang ada, memastikan keberlanjutan, dan meningkatkan kinerja organisasi secara keseluruhan.

| No | Aktivitas Tata Kelola | TEMUAN | |
|---|---|---|---|
| | | Y | T |
| **EDM03.01 Mengevaluasi manajemen risiko** | | | |
| 1 | Apakah Diskominfosan Kabupaten Bangli memahami konteks terkait risiko keamanan informasi? | | |
| 2 | Apakah Diskominfosan Kabupaten Bangli menentukan tingkat level risiko terkait keamanan informasi yang bersedia diambil organisasi dalam upayanya mencapai tujuan organisasi? | | |
| 3 | Apakah Diskominfosan Kabupaten Bangli menentukan tingkat toleransi risiko terhadap kemampuan mengelola risiko, seperti penyimpangan yang dapat diterima sementara dari risiko? | | |
| 4 | Apakah Diskominfosan Kabupaten Bangli menentukan tingkat keselarasan strategi risiko keamanan informasi dengan strategi risiko organisasi dan memastikan selera risiko berada di bawah kapasitas risiko organisasi? | | |
| **EDM03.02 Mengarahkan manajemen risiko** | | | |
| 5 | Apakah kebijakan dan strategi risiko keamanan informasi pada Diskominfosan Kabupaten Bangli sudah diterapkan dan dijalankan dalam pekerjaan sehari-hari? | | |
| 6 | Apakah Diskominfosan Kabupaten Bangli memiliki rencana yang jelas tentang bagaimana cara mengkomunikasikan risiko (ancaman) kepada semua karyawan dan tingkatan manajemen? | | |
| 7 | Jika terjadi risiko atau ancaman mendadak, apakah Diskominfosan Kabupaten Bangli tahu langkah-langkah pasti untuk merespons dan melaporkannya kepada manajemen yang tepat? | | |
| 8 | Apakah seluruh karyawan pada Diskominfosan Kabupaten Bangli didorong dan tahu caranya melaporkan risiko atau kekhawatiran kepada pihak yang bertanggung jawab, kapan saja dibutuhkan? | | |
| **EDM03.03 Memantau manajemen risiko** | | | |
| 8 | Apakah setiap masalah manajemen risiko selalau di laporkan kepada managemen atau pimpinan pada Diskominfosan Kabupaten Bangli? | | |

**APO12 Manage Risk**

**TUJUAN:** Untuk mengelola resiko mulai dari merencanakan, menerapkan, dan memantau kerangka kerja manajemen risiko yang efektif, serta menjadikannya bagian integral dari manajemen risiko organisasi secara luas

| No | Aktivitas Tata Kelola | TEMUAN | |
|---|---|---|---|
| | | Y | T |
| **APO12.01 Mengumpulkan data.** | | | |
| 1 | Apakah Diskominfosan Kabupaten Bangli menetapkan dan mengelola metode untuk pengumpulan, klasifikasi, dan analisis data terkait risiko keamanan informasi? | | |

| | | | |
|---|---|---|---|
| 2 | Apakah Diskominfosan Kabupaten Bangli melakukan pencatatan data terkait risiko keamanan informasi yang relevan dan signifikan pada lingkungan operasi internal dan eksternal organisasi? | | |
| **APO12.03 Menjaga profil risiko.** | | | |
| 3 | Apakah Diskominfosan Kabupaten Bangli memiliki daftar proses kerja utama, dan tahu persis apa saja teknologi, data, dan karyawan yang mendukung setiap proses pada pusat data? | | |
| 4 | Apakah semua pihak sudah sepakat mengenai layanan keamanan dan teknologi mana yang paling penting agar layanan pusat data tetap berjalan, serta memahami potensi kelemahan (titik rentan) berada? | | |
| 5 | Apakah skenario ancaman dan risiko keamanan informasi saat ini dikelompokkan berdasarkan jenis ancaman, pelayanan yang terdampak, dan area kerja yang bertanggung jawab? | | |
| **APO12.05 Menetapkan portofolio tindakan manajemen risiko.** | | | |
| 6 | Apakah Diskominfosan Kabupaten Bangli selalu menjaga inventaris aktivitas pengendalian yang ada untuk mengurangi risiko dan yang memungkinkan risiko diambil sesuai dengan selera dan toleransi risiko? | | |

**APO13 Manage Security**

**TUJUAN:** Menjaga informasi dan aset teknologi informasi pada tingkat risiko keamanan yang dapat diterima oleh organisasi.

| No | Aktivitas Tata Kelola | TEMUAN | |
|---|---|---|---|
| | | Y | T |
| **APO13.01 Menetapkan dan memelihara sistem manajemen keamanan informasi (ISMS)** | | | |
| 1 | Apakah Diskominfosan Kabupaten Bangli memiliki batasan yang jelas (ruang lingkup) mengenai sistem dan lokasi mana saja yang wajib dilindungi oleh aturan keamanan pemerintahan? | | |
| 2 | Apakah sistem manajemen keamanan informasi pada Diskominfosan Kabupaten Bangli sudah sesuai dengan kebijakan organisasi dan lingkungan kerja tempat pusat data beroperasi? | | |
| 3 | Apakah cara Diskominfosan Kabupaten Bangli mengelola keamanan informasi sejalan dengan pendekatan manajemen keamanan yang berlaku di seluruh Diskominfosan? | | |
| 4 | Untuk menerapkan, menjalankan, atau mengubah sistem keamanan informasi yang ada, apakah Diskominfosan Kabupaten Bangli selalu mendapatkan persetujuan resmi dari manajemen puncak?. | | |
| 5 | Apakah Diskominfosan Kabupaten Bangli memiliki dokumen resmi yang menjelaskan secara rinci tentang ruang lingkup (batasan) dan bagaimana aturan keamanan itu diterapkan? | | |
| 6 | Apakah tanggung jawab setiap orang dalam menjaga keamanan data sudah ditetapkan dan dikomunikasikan dengan jelas? | | |
| 7 | Apakah pengelolaan manajemen keamanan informasi (ISMS) sudah diketahui dan dipahami oleh semua pihak pada Diskominfosan Kabupaten Bangli? | | |

**BAI10 Manage Configuration**

**TUJUAN:** Memastikan organisasi memiliki informasi yang akurat, lengkap, dan terkini tentang semua aset dan komponen teknologi yang digunakan untuk memberikan layanan. Informasi ini kemudian digunakan untuk mengelola layanan tersebut secara efektif..

| No | Aktivitas Tata Kelola | TEMUAN | |
|---|---|---|---|
| | | Y | T |
| **BAI10.02 Menetapkan dan memelihara repositori konfigurasi dan garis dasar.** | | | |
| 1 | Apakah Diskominfosan Kabupaten Bangli memiliki daftar lengkap dari semua aset dan komponen teknologi (seperti server, aplikasi, software) yang kita gunakan? | | |
| **BAI10.03 Memelihara dan mengendalikan item konfigurasi.** | | | |
| 2 | Apakah setiap perubahan pada aset teknologi dan sistem pusat data selalu dicatat dan diperbarui secara rutin? | | |
| 3 | Jika terjadi perubahan teknologi informasi, apakah sebelumnya dilakukan proses membandingkan usulan tersebut dengan konfigurasi awal yang sudah disepakati (*baseline*) untuk memastikan semuanya aman? | | |
| 4 | Apakah setelah dilakukan perubahan teknologi seluruh data/dokumen dan konfigurasi aset tersebut segera dapat diperbarui dan akurat? | | |
| **BAI10.04 Membuat laporan status dan konfigurasi.** | | | |
| 5 | Apakah Diskominfosan Kabupaten Bangli secara rutin membuat laporan tentang perbedaan atau penyimpangan antara kondisi sistem saat ini dan konfigurasi awal yang seharusnya (*baseline*)? | | |

**DSS04 Manage Continuity**

**TUJUAN:** Menetapkan dan memelihara sebuah rencana yang memungkinkan organisai dapat merespons insiden dan gangguan secara cepat, demi melanjutkan operasional proses kinerja kritis dan mempertahankan ketersediaan informasi pada tingkat yang dapat diterima oleh organisasi

| No | Aktivitas Tata Kelola | TEMUAN | |
|---|---|---|---|
| | | Y | T |
| **DSS04.01 Menetapkan kebijakan, tujuan, dan cakupan kesinambungan bisnis.** | | | |
| 1 | Apakah Diskominfosan Kabupaten Bangli telah mengidentifikasi proses kerja (internal maupun yang dikerjakan pihak luar) yang paling penting agar keamanan informasi tetap berjalan, termasuk yang diwajibkan oleh hukum? | | |
| 2 | Apakah pihak-pihak utama yang bertanggung jawab atas keberlangsungan keamanan informasi telah ditetapkan, serta peran mereka dalam menyetujui kebijakan sudah jelas? | | |
| 3 | Apakah Diskominfosan Kabupaten Bangli memiliki tujuan dan batas minimum yang disepakati dan didokumentasikan untuk menjamin ketahanan dan kelangsungan operasi pusat data jika terjadi gangguan? | | |
| 4 | Apakah Diskominfosan Kabupaten Bangli telah menentukan proses kerja pendukung dan layanan keamanan data mana saja yang paling krusial untuk menjaga kelangsungan kerja pusat data? | | |
| **DSS04.02 Mempertahankan ketahanan bisnis.** | | | |

| | | | |
|---|---|---|---|
| 5 | Apakah Diskominfosan Kabupaten Bangli sudah memikirkan dan mencatat berbagai skenario terburuk (seperti bencana, kegagalan sistem) yang bisa menyebabkan gangguan besar pada pusat data yang dikelola? | | |
| 6 | Apakah Diskominfosan Kabupaten Bangli secara resmi mengukur seberapa besar kerugian (dampak) yang ditimbulkan oleh gangguan terhadap proses kerja yang paling penting? | | |
| 7 | Sudahkah Diskominfosan Kabupaten Bangli menetapkan batas waktu maksimal yang boleh kita alami saat sistem terganggu, dan target waktu kapan proses kerja dan keamanan data harus pulih? | | |
| 8 | Apakah Diskominfosan Kabupaten Bangli sudah memiliki kondisi seperti apa yang mengharuskan rencana pemulihan segera diaktifkan, dan siapa yang berhak mengambil keputusan tersebut? | | |
| **DSS04.03 Mengembangkan dan menerapkan respons kesinambungan bisnis.** | | | |
| 9 | Jika terjadi gangguan pada pusat data, apakah Diskominfosan Kabupaten Bangli sudah memiliki prosedur yang jelas tentang apa yang harus dilakukan, bagaimana cara berkomunikasi, dan siapa yang bertanggung jawab atas setiap langkah? | | |
| 10 | Apakah Diskominfosan Kabupaten Bangli memastikan bahwa vendor atau mitra kerja utama juga punya rencana pemulihan yang baik, dan apakah Diskominfosan Kabupaten Bangli memverifikasinya? | | |
| 11 | Apakah prosedur pemulihan Diskominfosan Kabupaten Bangli mencakup langkah-langkah detail untuk memastikan data pada pusat data tetap utuh (tidak rusak) dan proses layanan dapat berjalan normal kembali? | | |
| 12 | Apakah Diskominfosan Kabupaten Bangli memiliki dokumen rencana pemulihan yang terkini dan siap pakai yang menjelaskan cara menjalankan operasi pusat data penting selama dan setelah gangguan? | | |
| 13 | Apakah Diskominfosan Kabupaten Bangli sudah mencatat dan mengamankan semua sumber daya (orang, tempat kerja, teknologi) yang diperlukan untuk menjalankan Rencana Pemulihan? | | |
| 14 | Apakah Diskominfosan Kabupaten Bangli memiliki kebijakan backup yang jelas, aman, dan disimpan di lokasi terpisah (di luar kantor) untuk semua data dan dokumen penting? | | |
| 15 | Apakah Diskominfosan Kabupaten Bangli sudah mengidentifikasi dan memastikan bahwa tim yang bertugas melaksanakan rencana pemulihan memiliki keterampilan yang dibutuhkan? | | |
| **DSS04.04 Menjalankan, menguji, dan meninjau rencana kesinambungan bisnis dan rencana respons bencana.** | | | |
| 16 | Apakah Diskominfosan Kabupaten Bangli memiliki tujuan yang jelas saat melakukan latihan/simulasi pemulihan untuk memastikan semua bagian rencana bekerja dengan baik? | | |
| 17 | Apakah Diskominfosan Kabupaten Bangli secara rutin melakukan latihan pemulihan yang realistis, melibatkan semua pihak terkait, dan memastikan proses bisnis tidak terganggu parah selama pengujian? | | |
| 18 | Apakah Diskominfosan Kabupaten Bangli memiliki peran dan tanggung jawab setiap orang dalam melaksanakan latihan dan pengujian rencana pemulihan ditetapkan secara jelas? | | |
| **DSS04.06 Melakukan pelatihan rencana kesinambungan.** | | | |

| | | | |
|---|---|---|---|
| 19 | Apakah semua karyawan yang terlibat dilatih dan diberikan informasi yang cukup tentang apa yang harus dilakukan sesuai Rencana Pemulihan (*Business Continuity Plan*) dan (*Disaster Recovery Plan*)? | | |
| **DSS04.07 Mengelola pengaturan cadangan.** | | | |
| 20 | Apakah Diskominfosan Kabupaten Bangli mempunyai jadwal backup data yang teratur dan memastikan backup tersebut aman, terenkripsi, dan sesuai dengan jenis data yang dibutuhkan? | | |
| 21 | Apakah Diskominfosan Kabupaten Bangli memiliki aturan yang jelas mengenai di mana data backup disimpan (di kantor dan di luar kantor) dan bagaimana cara mengaksesnya dengan mudah saat dibutuhkan? | | |
| 22 | Apakah Diskominfosan Kabupaten Bangli secara rutin menguji data backup yang tersimpan untuk memastikan bahwa data tersebut dapat digunakan (bukan data rusak) jika terjadi pemulihan? | | |
| 23 | Apakah Diskominfosan Kabupaten Bangli memastikan bahwa vendor atau pihak ketiga yang mengelola sistem kita juga melakukan backup data kita sesuai standar keamanan yang kita minta? | | |

**DSS05 Manage Security Services**

**TUJUAN:** Untuk melindungi informasi organisasi, pada semua media, terhadap akses, penggunaan, pengungkapan, modifikasi, kerusakan, dan perusakan yang tidak sah, melalui pengelolaan layanan keamanan secara operasional

| No | Aktivitas Tata Kelola | TEMUAN | |
|---|---|---|---|
| | | Y | T |
| **DSS05.01 Melindungi dari perangkat lunak berbahaya.** | | | |
| 1 | Apakah Diskominfosan Kabupaten Bangli menginstal dan mengaktivasi pada *software* pemindai virus atau perangkat lunak perlindungan pada semua fasilitas pemrosesan data? | | |
| 2 | Apakah Diskominfosan Kabupaten Bangli melakukan pengaturan pada sistem jaringan atau email agar hanya menerima data dan email yang dikenal dan terfilter dari ancaman seperti *spyware* atau *phishing*? | | |
| **DSS05.02 Mengelola keamanan jaringan dan konektivitas.** | | | |
| 3 | Apakah Diskominfosan Kabupaten Bangli mengizinkan hanya perangkat yang berwenang untuk memiliki akses ke informasi organisasi dan jaringan? | | |
| 4 | Apakah Diskominfosan Kabupaten Bangli menerapkan sistem keamanan jaringan seperti *firewall* dan *software* deteksi intrusi untuk membatasi akses ke jaringan organisasi? | | |
| 5 | Apakah Diskominfosan Kabupaten Bangli menerapkan kebijakan untuk mengendalikan lalu lintas masuk dan keluar agar informasi dan jaringan terlindungi, seperti membatasi akses ke beberapa situs web atau memblokir email yang mengandung *virus*. | | |
| 6 | Apakah Diskominfosan Kabupaten Bangli menerapkan protokol keamanan yang disetujui untuk konektivitas jaringan, untuk memastikan bahwa informasi yang dikirim melalui jaringan aman dan tidak dapat dicuri atau dimodifikasi oleh pihak yang tidak berwenang. | | |
| **DSS05.03 Mengelola keamanan titik akhir.** | | | |
| 7 | Apakah Diskominfosan Kabupaten Bangli mengkonfigurasikan peralatan jaringan dengan cara yang aman seperti mengatur perangkat jaringan seperti | | |

| | | | |
|---|---|---|---|
| | *switch, router, firewall,* dan *data center* agar bekerja dengan cara yang memastikan keamanan jaringan | | |
| 8 | Apakah Diskominfosan Kabupaten Bangli menerapkan mekanisme penguncian perangkat, seperti hanya orang yang memiliki hak akses yang dapat mengakses perangkat, ini bisa melalui password, PIN, atau metode pengenalan sidik jari. | | |
| 9 | Apakah Diskominfosan Kabupaten Bangli mengelola dan memantau akses ke sistem informasi dan data dari jarak jauh, misalnya melalui perangkat seluler atau teleworking (bekerja dari rumah), seperti pembatasan akses, pengaturan VPN, pemantauan aktivitas, dan lain-lain. | | |
| 10 | Apakah Diskominfosan Kabupaten Bangli mengelola konfigurasi jaringan dengan cara yang aman, seperti melalui pembatasan akses, pengaturan *firewall*, pengaturan alamat IP, pemantauan aktivitas, enkripsi koneksi jaringan, dan lain sebagainya | | |
| 11 | Apakah Diskominfosan Kabupaten Bangli menerapkan proses kontrol dan pembatasan akses ke jaringan komputer melalui perangkat seperti komputer atau perangkat mobile yang terhubung ke jaringan? | | |
| 12 | Apakah Diskominfosan Kabupaten Bangli melindungi sistem dari perubahan, kerusakan, atau manipulasi yang tidak sah untuk menjaga integritas sistem? | | |
| 13 | Apakah Diskominfosan Kabupaten Bangli melindungi perangkat ponsel/tablet yang digunakan untuk kerja juga dilindungi dengan fitur pemblokiran situs web atau tautan berbahaya? | | |
| 14 | Ketika sebuah komputer atau perangkat pengolah data tidak lagi digunakan, apakah Diskominfosan memastikan data sensitif dihapus secara total dan aman? | | |
| 15 | Apakah Diskominfosan Kabupaten Bangli melakukan pemfilteran situs web, memblokir tautan email yang berbahaya, dan menonaktifkan tautan klik-tayang (yaitu tautan yang otomatis mengarahkan pengguna ke situs web tanpa persetujuan pengguna) pada perangkat mobile. | | |
| **DSS05.04 Mengelola identitas pengguna dan akses logis.** | | | |
| 16 | Apakah hak akses (ke sistem dan data) setiap pengguna layanan pusat data dibatasi hanya pada yang benar-benar dibutuhkan untuk pekerjaannya? | | |
| **DSS05.05 Mengelola akses fisik ke aset keamanan informasi.** | | | |
| 17 | Apakah semua pengunjung (termasuk teknisi/vendor) yang masuk ke area server atau ruang TI selalu dicatat dan dipantau? | | |
| 18 | Apakah semua staf dan vendor diwajibkan untuk selalu memakai tanda pengenal saat berada di dalam area kantor/fasilitas? | | |
| 19 | Apakah pengunjung (termasuk vendor) yang masuk ke area sensitif selalu didampingi oleh staf Diskominfosan Kabupaten Bangli? | | |
| 20 | Apakah area sensitif pada pusat data dilindungi oleh pembatasan fisik (kunci, pagar, CCTV, dll.) untuk mengontrol akses? | | |
| **DSS05.06 Mengelola dokumen sensitif dan perangkat keluaran.** | | | |
| 21 | Apakah ada aturan yang jelas tentang bagaimana cara mengelola (menerima, menyimpan, memindahkan, dan membuang) dokumen dan print out yang bersifat rahasia? | | |
| 22 | Apakah data sensitif yang tersimpan di komputer atau sistem dilindungi dengan menggunakan enkripsi (pengkodean) yang kuat? | | |
| **DSS05.07 Mengelola kerentanan dan memantau infrastruktur untuk kejadian yang terkait dengan keamanan.** | | | |

| | | | |
|---|---|---|---|
| 23 | Apakah Diskominfosan Kabupaten Bangli menggunakan portofolio teknologi, layanan, dan aset yang didukung (pemindai kerentanan, fuzzer dan *sniffer*, penganalisis protokol) untuk mengidentifikasi kerentanan keamanan informasi? | | |
| 24 | Apakah Diskominfosan Kabupaten Bangli menetapkan dan mengkomunikasikan skenario risiko, sehingga mudah dikenali, dan kemungkinan dampaknya dipahami? | | |
| 25 | Apakah Diskominfosan Kabupaten Bangli meninjau log peristiwa secara berkala untuk mengetahui potensi insiden? | | |
| 26 | Apakah Diskominfosan Kabupaten Bangli memastikan laporan (tiket) insiden keamanan segera dibuat ketika hasil pemantauan menemukan adanya potensi insiden? | | |

Sumber : (ISACA COBIT Governance and Management Objectives, 2019; Toolkit Indeks KAMI, 2023)

Tanda tangan & Nama Responden:……..

Lampiran 4. Surat Keterangan Penelitian


PEMERINTAH KABUPATEN BANGLI

DINAS PENANAMAN MODAL DAN
PELAYANAN TERPADU SATU PINTU

Jalan Brigjen Ngurah Rai No. 2A, Telp. (0366) 5510099, BANGLI-80613
Website : https://www.dpmptsp.banglikab.go.id/
Email : perijinan@gmail.com


## SURAT KETERANGAN PENELITIAN

NOMOR : 000.9.2/115/XII/DPMPTSP

Dasar : 1. Undang-Undang Nomor 18 Tahun 2002 tentang Sistem Nasional Penelitian, Pengembangan dan Penerapan Ilmu Pengetahuan dan Teknologi;
2. Peraturan Menteri Dalam Negeri Republik Indonesia Nomor 3 Tahun 2018 tentang Penerbitan Surat Keterangan Penelitian.

Menimbang : 1. bahwa sesuai Surat permohonan dari UNIVERSITAS PENDIDIKAN GANESHA PROGRAM PASCASARJANA tertanggal 03 November 2025 Nomor 5721/UN48.14.1/PT.02.05/2025 Perihal Mohon Izin Pengambilan Data
2. bahwa untuk tertib administrasi dan pengendalian serta pengembangan perlu diterbitkan surat keterangan penelitian.
3. bahwa berdasarkan pertimbangan sebagaimana huruf a dan b serta hasil verifikasi dan validasi Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kabupaten Bangli berkas persyaratan administrasi telah memenuhi syarat.

Kepala Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kabupaten Bangli memberikan rekomendasi penelitian kepada :

| | |
|---|---|
| 1. Nama | : I Nyoman Suarka |
| 2. No. KTP | 5106021505770008 |
| 3. Alamat | : Tempek Kelod Kangin, Lingk/Br. Bebalang, Desa Bebalang, Kec. Bangli. Kab. Bangli |
| 4. Pekerjaan | : PNS |
| 5. Nama Lembaga | : UNIVERSITAS PENDIDIKAN GANESHA PROGRAM PASCASARJANA |

Untuk melaksanakan penelitian, dengan rincian sebagai berikut :

| | |
|---|---|
| 1. Judul Penelitian | : Evaluasi Keamanan Informasi Pemerintah Kabupaten Bangli Menggunakan Kombinasi Framework Indeks KAMI 5,0 dan COBIT 2019 (Studi Kasus Dinas Komunikasi Informasi dan Persandian Kabupaten Bangli) |
| 2. Lokasi/Tempat | : Dinas Komunikasi Informatika dan Persandian Kabupaten Bangli |
| 3. Jumlah Peserta | : 1 Orang |
| 4. Lama Penelitian | : 03 November 2025 - 31 Januari 2026 |

Dengan Ketentuan yang harus ditaati sebagai berikut :
1. Sebelum melakukan penelitian terlebih dahulu agar melaporkan kepada pejabat setempat yang akan dijadikan obyek penelitian.
2. Mematuhi ketentuan dan peraturan yang berlaku di daerah/wilayah penelitian.
3. Tidak dibenarkan melakukan penelitian yang materinya bertentangan dengan topik/judul penelitian dimaksud.
4. Setelah pelaksanaan kegiatan dimaksud selesai, agar melapor kembali dan menyerahkan hasil penelitian kepada Badan Kesatuan Bangsa dan Politik Kabupaten Bangli, Organisasi Perangkat Daerah yang menjadi objek penelitian, Dinas Penanaman Modal dan Pelayanan Terpadu Satu Pintu Kabupaten Bangli, dan Bagian Umum Sekretariat Daerah Kabupaten Bangli.
5. Surat Rekomendasi yang dikeluarkan dapat dibatalkan sewaktu-waktu apabila tidak sesuai ketentuan dan peraturan perundang-undangan yang berlaku.

Demikian Surat Rekomendasi ini dikeluarkan untuk dipergunakan dimana perlu.

Dikeluarkan di : Bangli
Pada tanggal : 04 Desember 2025
**Ditandatangani Secara Elektronik Oleh :**
Kepala Dinas Penanaman Modal dan
Pelayanan Terpadu Satu Pintu
Kabupaten Bangli,

**Jetet Hiberon, A.P., M.Si.**
**Pembina Tk I (IV/b)**
**NIP. 197309151993111001**

Tembusan :
1. Bupati Bangli cq. Sekretaris Daerah Kabupaten Bangli
2. DANDIM 1626 Bangli di Bangli
3. Kapolres Bangli di Bangli
4. Kepala DPMPTSP Provinsi Bali di Denpasar
5. Kepala Bagian Umum Setda Kab.Bangli
6. OPD yang menjadi objek penelitian (Dinas Komunikasi, Informatika dan Persandian Kabupaten Bangli)
7. Yang bersangkutan
8. Arsip.

Lampiran 5. Surat Mohon Izin Pengambilan Data

KEMENTERIAN PENDIDIKAN TINGGI, SAINS DAN TEKNOLOGI
UNIVERSITAS PENDIDIKAN GANESHA
**PROGRAM PASCASARJANA**
**Jl. Udayana No 11 Singaraja Bali, Telp. 081999446444**
**Laman: http://pasca.undiksha.c.id.**

Nomor : 5721/UN48.14.1/PT.02.05/2025 03 Nopember 2025
Lamp : 1 (satu) gabung
Perihal : Mohon Izin Pengambilan Data

Yth. **Kepala Diskominfosan Kabupaten Bangli**
di **Tempat**

Dengan hormat, dalam rangka pengumpulan data untuk Penelitian Tesis mahasiswa Program Pascasarjana Universitas Pendidikan Ganesha, bersama ini kami mohon kesedian Bapak/Ibu untuk dapat menerima dan mengijinkan mahasiswa kami dengan identitas:

| | |
|---|---|
| Nama | : I Nyoman Suarka |
| NIM | : 2229101052 |
| Program Studi | : Ilmu Komputer (S2) |
| Judul Tesis | : Evaluasi Keamanan Informasi Pemerintah Kabupaten Bangli Menggunakan Kombinasi Framework Indeks KAMI 5.0 dan COBIT 2019 (Studi Kasus Dinas Komunikasi Informasi dan Persandian Kabupaten Bangli). |

untuk mendapatkan data/informasi yang dibutuhkan oleh mahasiswa dalam melakukan penelitian.

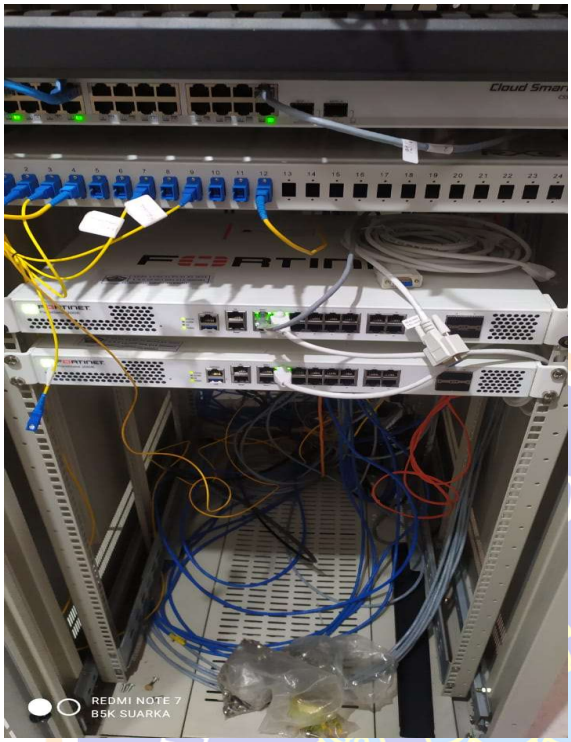
Demikain disampaikan, atas perkenaan dan kerja sama yang baik kami ucapkan terima kasih.

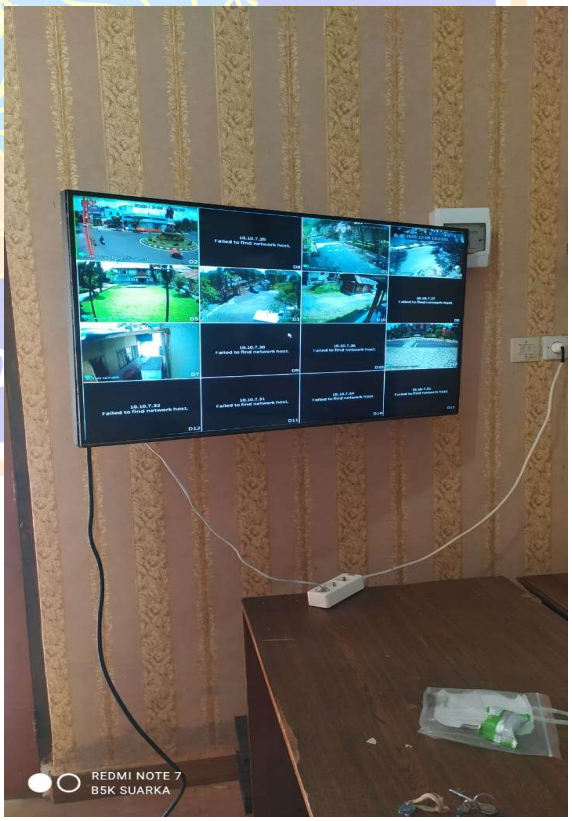
a.n Direktur,
Wakil Direktur I,

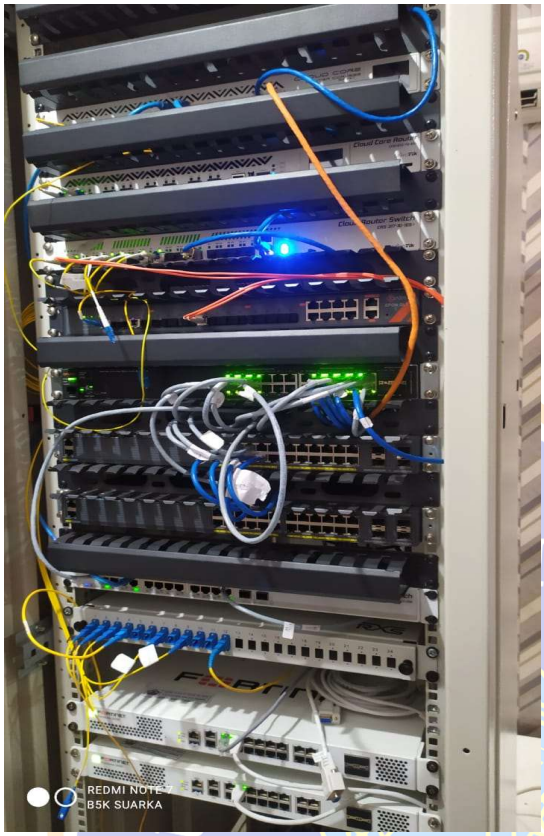
Ida Bagus Putu Arnyana
NIP 195812311986011005

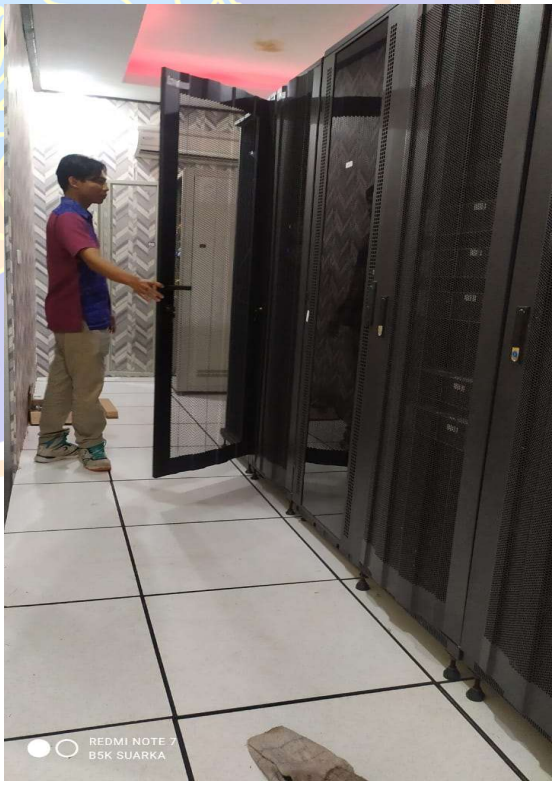
Tembusan :
1. Kepala Subbagian Program Pascasarjana
2. Mahasiswa yang bersangkutan

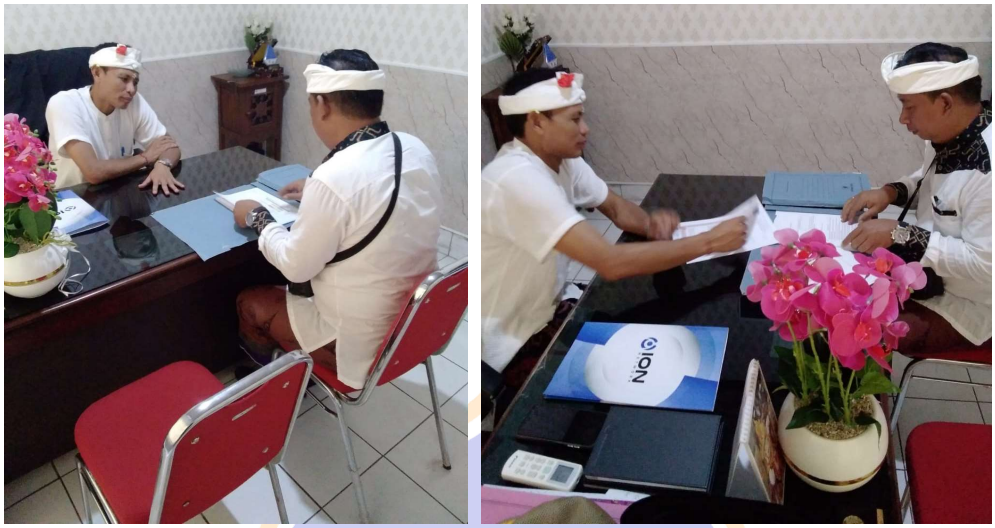
Lampiran 6. Dokumentasi Proses Pengambilan Data



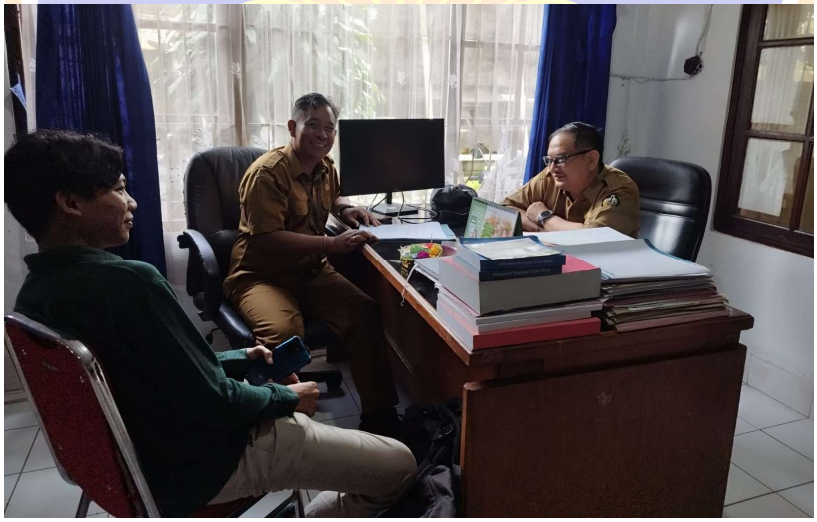




REDMI NOTE 7
B5K SUARKA

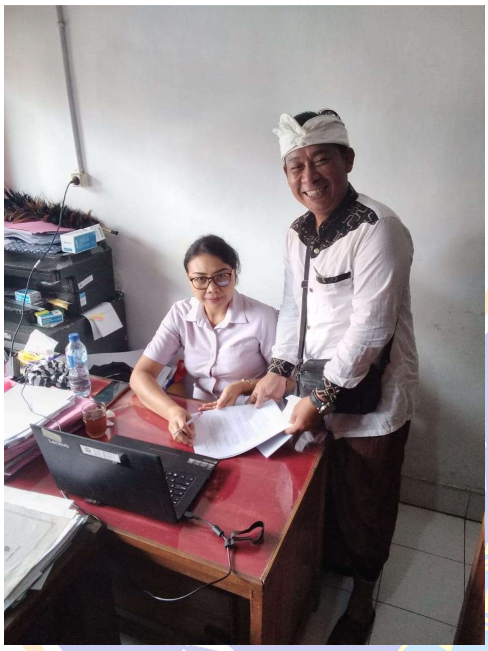
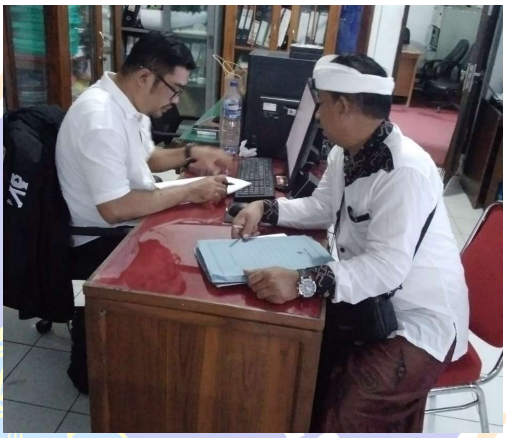

REDMI NOTE 7
B5K SUARKA



Wawancara dengan Kepala Dinas Komunikasi Informasi dan Persandian Kabupaten Bangli



Wawancara dengan Kepala Bidang Persandian dan Pengawasan Informasi Diskominfosan Kabupaten Bangli

Proses pengisian kuesioner penelitian

Proses pengisian kuesioner penelitian

Proses pengisian kuesioner penelitian

Proses penolahan data dengan Indeks KAMI 5.0

| | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| 1 | **Bagian II: Tata Kelola Keamanan Informasi** | | | | | | | |
| 2 | Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi. | | | | | | | |
| 3 | **[Penilaian]** Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh | | | | **Status** | Skor | **NOMOR DOKUMEN** | **NAMA DOKUMEN** |
| 4 | **#** | | | **Fungsi/Organisasi Keamanan Informasi** | | | | |
| 5 | 2.1 | II | 1 | Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait? | Diterapkan Secara Menyeluruh | 3 | | Draf perbup smki, SOTK, SKP Kabid Sandi |
| 6 | 2.2 | II | 1 | Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya? | Diterapkan Secara Menyeluruh | 3 | | SOTK, Pohon Kinerja, SK SMKI |
| 7 | 2.3 | II | 1 | Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi? | Diterapkan Secara Menyeluruh | 3 | | Anjab ABK, SOTK, SK Tim SMKI |
| 8 | 2.4 | II | 1 | Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi? | Diterapkan Secara Menyeluruh | 3 | | DPA, Anjab, ABK |
| 9 | 2.5 | II | 1 | Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan? | Dalam Penerapan / Diterapkan Sebagian | 2 | | SK Team SMKI, Draf Perbup SMKI |
| 10 | 2.6 | II | 1 | Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi? | Dalam Penerapan / Diterapkan Sebagian | 2 | | |
| 11 | 2.7 | II | 1 | Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku? | Dalam Penerapan / Diterapkan Sebagian | 2 | | Sertifikat sandiman, pelatihan sandi man |
| 12 | 2.8 | II | 1 | Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait? | Diterapkan Secara Menyeluruh | 3 | | notulen rapat bvio, bukti sosialisasi |
| 13 | 2.9 | II | 2 | Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi? | Diterapkan Secara Menyeluruh | 6 | | Surat usulan diklat |
| 14 | 2.10 | II | 2 | Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada? | Dalam Penerapan / Diterapkan Sebagian | 4 | | SOP Penanganan syber |
| 15 | 2.11 | II | 2 | Apakah instansi/perusahaan anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku? | Dalam Perencanaan | 2 | | Draf Perbup SMKI |
| 16 | 2.12 | II | 2 | Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada? | Dalam Penerapan / Diterapkan Sebagian | 4 | | NDA Jaringan, SOTK |
| 17 | 2.13 | II | 2 | Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak? | Dalam Penerapan / Diterapkan Sebagian | 4 | | Screen Shoot chat dengan callcenter BSRE, laporan penanganan dan kegagalan sistem |

Pengantar | Identitas Responden | I Kategori SE | II Tata Kelola | III Risiko | IV Kerangka Kerja | V Pengelolaan Aset | VI Teknologi

**Hasil Observasi**

**Lampiran 1. lembar observasi**

**Checklist Observasi Keamanan Informasi Pusat Data Layanan e-Kinerja Diskominfosan Kabupaten Bangli**

**A. Pengamanan Fisik**

| No. | Pertanyaan Observasi | Ya | Tidak |
|---|---|---|---|
| 1 | Ruangan server terkunci dan hanya bisa diakses oleh petugas berwenang | ✓ | |
| 2 | CCTV aktif dan mencakup area pintu masuk pusat data | ✓ | |
| 3 | Terdapat pencatatan akses fisik ke ruang server (log manual/otomatis) | ✓ | |
| 4 | Ruangan pusat data dilengkapi dengan AC dan UPS | ✓ | |
| 5 | Tidak ada perangkat asing (flashdisk/harddisk pribadi) yang dicolokkan ke server | ✓ | |
| 6 | Ruang pusat data bersih dan tertata | ✓ | |
| 7 | Tersedia sistem pemadam kebakaran (*fire extinguisher*) | ✓ | |
| 8 | Pintu ruang server menggunakan akses biometrik/kartu | | ✓ |
| 9 | Dinding ruang server tidak berlubang atau rawan akses luar | ✓ | |
| 10 | Tidak ada aktivitas makan/minum di ruang server | ✓ | |

**B. Keamanan Akses Sistem dan Jaringan**

| No. | Pertanyaan Observasi | Ya | Tidak |
|---|---|---|---|
| 1 | Seluruh user memiliki username dan password unik | ✓ | |
| 2 | Sistem meminta penggantian password secara berkala | ✓ | |
| 3 | Sistem menggunakan autentikasi dua faktor (2FA) | | ✓ |
| 4 | Hak akses pengguna disesuaikan dengan tugas dan tanggung jawabnya (*role-based access control*) | ✓ | |
| 5 | Tidak ditemukan user ganda atau tidak aktif tapi masih punya akses | ✓ | |
| 6 | Admin memantau log akses pengguna secara berkala | ✓ | |
| 7 | Sistem logout otomatis jika tidak aktif dalam waktu tertentu | ✓ | |
| 8 | Pengguna tidak berbagi akun dengan orang lain | ✓ | |
| 9 | Tidak ditemukan penggunaan password default pabrik | ✓ | |
| 10 | Terdapat sistem VPN atau segmentasi jaringan untuk akses luar | | ✓ |

**C. Prosedur dan Dokumentasi Keamanan**

| No. | Pertanyaan Observasi | Ya | Tidak |
|---|---|---|---|
| 1 | Tersedia mekanisme pelaporan insiden keamanan siber | ✓ | |
| 2 | Terdapat sistem monitoring real-time (dashboard/server status) | ✓ | |
| 3 | Notifikasi/*alert* diterima saat ada aktivitas mencurigakan | | ✓ |
| 4 | Tindakan terhadap insiden terdokumentasi | ✓ | |
| 5 | Staf memahami prosedur tanggap insiden | ✓ | |
| 6 | Ada log percobaan login gagal | ✓ | |
| 7 | Terdapat monitoring penggunaan CPU, RAM, dan jaringan | ✓ | |
| 8 | Backup dilakukan secara rutin (harian/mingguan) Bulanan | ✓ | |
| 9 | Restore data pernah diuji coba dan berhasil | ✓ | |
| 10 | Laporan insiden dievaluasi untuk perbaikan | ✓ | |

**D. Pengelolaan Insiden dan Monitoring**

| No. | Pertanyaan Observasi | Ya | Tidak |
|---|---|---|---|
| 1 | Audit sistem dilakukan minimal sekali dalam setahun | ✓ | |
| 2 | Hasil audit ditindaklanjuti dengan perbaikan | | |
| 3 | Penilaian performa sistem dilakukan secara berkala | ✓ | |
| 4 | Penilaian tingkat kepatuhan terhadap SOP tersedia | ✓ | |
| 5 | Sistem diuji terhadap celah keamanan secara berkala (*penetration testing*) | ✓ | |
| 6 | Sistem dilindungi firewall aktif | ✓ | |
| 7 | IDS/IPS (*Intrusion Detection/Prevention System*) terpasang | ✓ | |
| 8 | Data terenkripsi baik saat transit maupun disimpan | ✓ | |
| 9 | Server tidak menampung file/data yang tidak terkait tugasnya | ✓ | |
| 10 | Kegiatan teknis dicatat dalam log book harian | ✓ | |

**E. Dokumen Evaluasi Keamanan Informasi**

| No. | Pertanyaan Observasi | Ya | Tidak |
|---|---|---|---|
| 1 | SK pembentukan Tim Keamanan Informasi | ✓ | |
| 2 | SOP keamanan informasi pusat data | ✓ | |
| 3 | Dokumen perencanaan strategis TI (Renstra, Renja, Master Plan TI) | ✓ | |
| 4 | Laporan penilaian risiko keamanan informasi tahunan | ✓ | |
| 5 | Laporan monitoring harian server & jaringan | | ✓ |
| 6 | SK penunjukan pejabat penanggung jawab keamanan TI | ✓ | |
| 7 | Dokumen Audit Internal/Eksternal Keamanan Informasi | ✓ | |
| 8 | Daftar inventaris aset TI (*hardware, software*, data, user) | ✓ | |
| 9 | Log backup server | ✓ | |
| 10 | SOP Penanganan Insiden | ✓ | |

Sumber : (Dewi, 2021; ISACA COBIT Design Guide, 2019; Pratiwi & Wulandari, 2021)

Tanda tangan & Nama Responden: I Kadek Aldy Oka Ardita

Tanda tangan & Nama Observer: I Nyoman Suyatna

**Hasil wawancara**

**Lampiran 1. Lembar Wawancara**

**LEMBAR WAWANCARA**

**BIODATA NARASUMBER**

| | | |
|---|---|---|
| Identitas Instansi Pemerintahan | : | Diskominfosan Kabupaten Bangli |
| Alamat | : | Jalan Brigjen Ngurah Rai No. 30 Telepon: (0366) 93804 |
| Nama Narasumber | : | I NYOMAN MURDITHA, S.Kom, M.Eng. |
| NIP | : | 19790827200501003 |
| Jabatan | : | KADIS KOMINFOSAN. KAB. BANGLI. |
| Tanggal Wawancara | : | 5 - NOVEMBER - 2025 |
| Tujuan | : | Penggalian informasi mengenai kategori sistem elektronik/pusat data yang digunakan pada Dinas Komunikasi Informatika dan Persandian Kabupaten Bangli |

**DAFTAR PERTANYAAN (R1)**

**Bagian I: Kategori Sistem Elektronik**

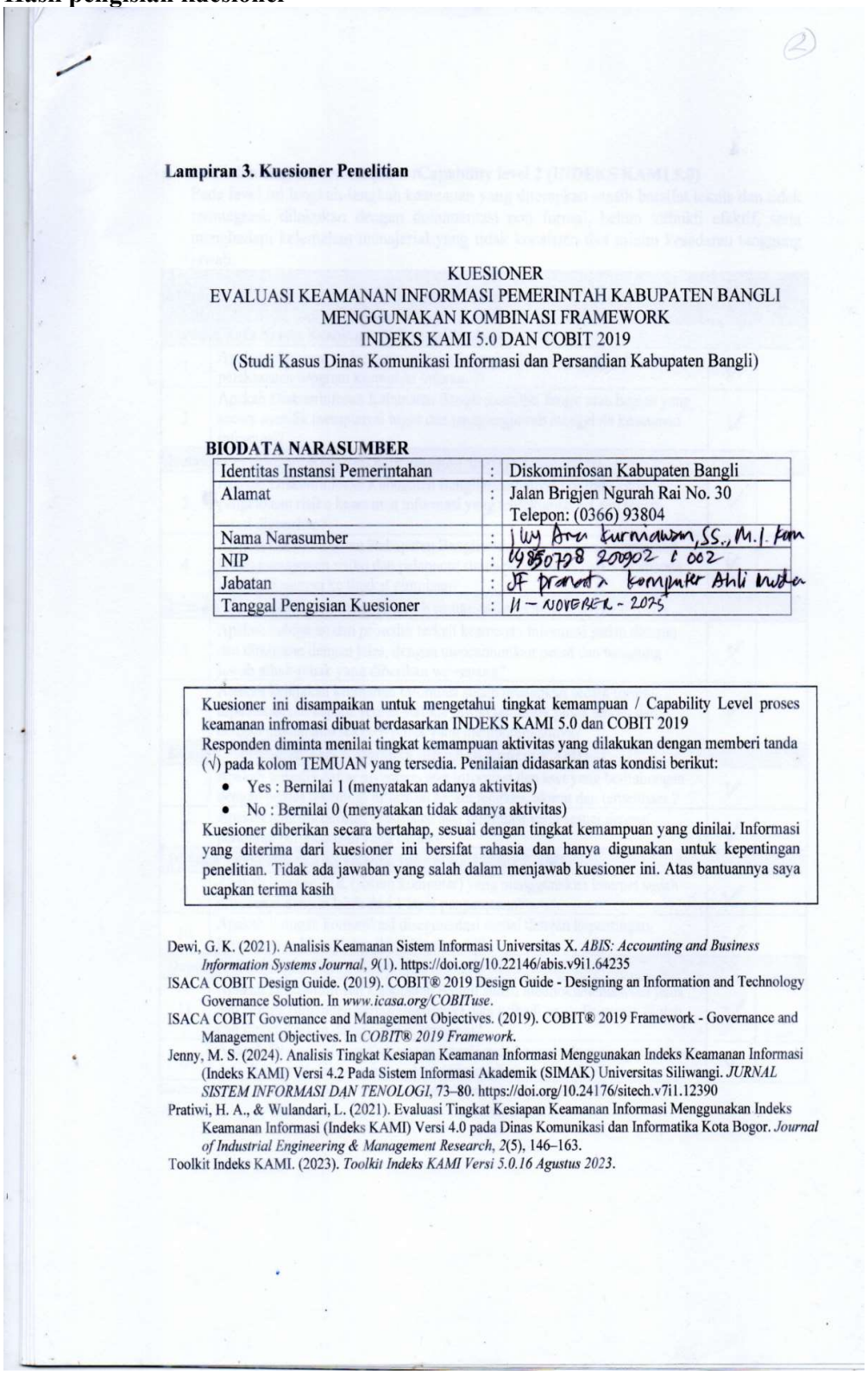
| NO | Karakteristik Instansi/Perusahaan | Jawaban |
|---|---|---|
| 1 | Nilai investasi pusat data yang terpasang<br>[A] Lebih dari Rp.30 Miliar<br>[B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar<br>[C] Kurang dari Rp.3 Miliar | C |
| 2 | Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan pusat data<br>[A] Lebih dari Rp.10 Miliar<br>[B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar<br>[C] Kurang dari Rp.1 Miliar | C |
| 3 | Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu<br>[A] Peraturan atau Standar nasional dan internasional<br>[B] Peraturan atau Standar nasional<br>[C] Tidak ada Peraturan khusus | B |
| 4 | Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik<br>[A] Teknik kriptografi khusus yang disertifikasi oleh Negara<br>[B] Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri<br>[C] Tidak ada penggunaan teknik kriptografi | B |
| 5 | Jumlah pengguna yang terhubung dengan pusat data<br>[A] Lebih dari 5.000 pengguna<br>[B] 1.000 sampai dengan 5.000 pengguna<br>[C] Kurang dari 1.000 pengguna | B |

| NO | Karakteristik Instansi/Perusahaan | Jawaban |
|---|---|---|
| 6 | Data pribadi yang dikelola oleh pusat data<br>[A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya<br>[B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha<br>[C] Tidak ada data pribadi | B |
| 7 | Tingkat klasifikasi/kekritisan Data yang ada dalam pusat data, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi<br>[A] Sangat Rahasia<br>[B] Rahasia dan/ atau Terbatas<br>[C] Biasa | B |
| 8 | Tingkat kekritisan proses yang ada dalam pusat data, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi<br>[A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik<br>[B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung<br>[C] Proses yang hanya berdampak pada kegiatan instansi | B |
| 9 | Dampak dari kegagalan pusat data yang dikelola<br>[A] Membahayakan pertahanan keamanan negara<br>[B] Tidak tersedianya layanan publik berskala nasional atau berdampak pada layanan di sektor lain<br>[C] Tidak tersedianya layanan publik dalam 1 propinsi atau internal 1 instansi | B |
| 10 | Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi pusat data (sabotase, terorisme)<br>[A] Menimbulkan korban jiwa<br>[B] Terbatas pada kerugian finansial<br>[C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial) | B |
| 11 | Untuk dilakukan penilaian pada penelitian ini, maka pada level berapa tingkat kapabilitas yang diharapakan?<br>[Level 0 Incomplete] (tidak ada bukti tata kelola keamanan informasi)<br>[Level 1 Performed] (Ada bukti pemahaman keamanan informasi)<br>[Level 2 Managed] (bersifat teknis dan terpisah, belum terdokumentasi)<br>[Level 3 Estabilished] (Terdefinisi, terdokumentasi, belum terstruktur)<br>[Level 4 Predictable] (diterapkan secara efektif dan selaras)<br>[Level 5 Optimizing] (penerapan yang komprehensif, dan berkelanjutan) | 4 |

Sumber : (Jenny, 2024; Toolkit Indeks KAMI, 2023)

Tanda tangan & Nama Responden:.....

**Hasil pengisian kuesioner**



**Lampiran 3. Kuesioner Penelitian**

KUESIONER
EVALUASI KEAMANAN INFORMASI PEMERINTAH KABUPATEN BANGLI
MENGGUNAKAN KOMBINASI FRAMEWORK
INDEKS KAMI 5.0 DAN COBIT 2019
(Studi Kasus Dinas Komunikasi Informasi dan Persandian Kabupaten Bangli)

**BIODATA NARASUMBER**

| | | |
|---|---|---|
| Identitas Instansi Pemerintahan | : | Diskominfosan Kabupaten Bangli |
| Alamat | : | Jalan Brigjen Ngurah Rai No. 30<br>Telepon: (0366) 93804 |
| Nama Narasumber | : | I Wy Arya Purnawan, SS., M.I. Kom |
| NIP | : | 19850728 20902 1 002 |
| Jabatan | : | JF Pranata Komputer Ahli Muda |
| Tanggal Pengisian Kuesioner | : | 11 - NOVEMBER - 2025 |

Kuesioner ini disampaikan untuk mengetahui tingkat kemampuan / Capability Level proses keamanan infromasi dibuat berdasarkan INDEKS KAMI 5.0 dan COBIT 2019
Responden diminta menilai tingkat kemampuan aktivitas yang dilakukan dengan memberi tanda (√) pada kolom TEMUAN yang tersedia. Penilaian didasarkan atas kondisi berikut:

- Yes : Bernilai 1 (menyatakan adanya aktivitas)
- No : Bernilai 0 (menyatakan tidak adanya aktivitas)

Kuesioner diberikan secara bertahap, sesuai dengan tingkat kemampuan yang dinilai. Informasi yang diterima dari kuesioner ini bersifat rahasia dan hanya digunakan untuk kepentingan penelitian. Tidak ada jawaban yang salah dalam menjawab kuesioner ini. Atas bantuannya saya ucapkan terima kasih


Dewi, G. K. (2021). Analisis Keamanan Sistem Informasi Universitas X. *ABIS: Accounting and Business Information Systems Journal*, *9*(1). https://doi.org/10.22146/abis.v9i1.64235

ISACA COBIT Design Guide. (2019). COBIT® 2019 Design Guide - Designing an Information and Technology Governance Solution. In *www.icasa.org/COBITuse*.

ISACA COBIT Governance and Management Objectives. (2019). COBIT® 2019 Framework - Governance and Management Objectives. In *COBIT® 2019 Framework*.

Jenny, M. S. (2024). Analisis Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.2 Pada Sistem Informasi Akademik (SIMAK) Universitas Siliwangi. *JURNAL SISTEM INFORMASI DAN TENOLOGI*, 73–80. https://doi.org/10.24176/sitech.v7i1.12390

Pratiwi, H. A., & Wulandari, L. (2021). Evaluasi Tingkat Kesiapan Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Indeks KAMI) Versi 4.0 pada Dinas Komunikasi dan Informatika Kota Bogor. *Journal of Industrial Engineering & Management Research*, *2*(5), 146–163.

Toolkit Indeks KAMI. (2023). *Toolkit Indeks KAMI Versi 5.0.16 Agustus 2023*.

**B. Penilaian tingkat kemampuan /Capability level 2 (COBIT 2019)**

Pada level ini proses telah direncanakan, dilaksanakan, dimonitor, dan disesuaikan secara memadai, sehingga hasil kerja proses dikelola dan diverifikasi..

**EDM03 Ensure Risk Optimisation**

**TUJUAN :** Untuk meminimalkan potensi dampak negatif. Tujuan dari optimasi risiko bukan hanya untuk menghindari risiko, tetapi juga untuk memanfaatkan peluang yang ada, memastikan keberlanjutan, dan meningkatkan kinerja organisasi secara keseluruhan.

| No | Aktivitas Tata Kelola | TEMUAN | |
|---|---|---|---|
| | | Y | T |
| **EDM03.01 Mengevaluasi manajemen risiko** | | | |
| 1 | Apakah Diskominfosan Kabupaten Bangli memahami konteks terkait risiko keamanan informasi? | √ | |
| 2 | Apakah Diskominfosan Kabupaten Bangli menentukan tingkat level risiko terkait keamanan informasi yang bersedia diambil organisasi dalam upayanya mencapai tujuan organisasi? | √ | |
| 3 | Apakah Diskominfosan Kabupaten Bangli menentukan tingkat toleransi risiko terhadap kemampuan mengelola risiko, seperti penyimpangan yang dapat diterima sementara dari risiko? | √ | |
| 4 | Apakah Diskominfosan Kabupaten Bangli menentukan tingkat keselarasan strategi risiko keamanan informasi dengan strategi risiko organisasi dan memastikan selera risiko berada di bawah kapasitas risiko organisasi? | √ | |
| **EDM03.02 Mengarahkan manajemen risiko** | | | |
| 5 | Apakah kebijakan dan strategi risiko keamanan informasi pada Diskominfosan Kabupaten Bangli sudah diterapkan dan dijalankan dalam pekerjaan sehari-hari? | √ | |
| 6 | Apakah Diskominfosan Kabupaten Bangli memiliki rencana yang jelas tentang bagaimana cara mengkomunikasikan risiko (ancaman) kepada semua karyawan dan tingkatan manajemen? | √ | |
| 7 | Jika terjadi risiko atau ancaman mendadak, apakah Diskominfosan Kabupaten Bangli tahu langkah-langkah pasti untuk merespons dan melaporkannya kepada manajemen yang tepat? | √ | |
| 8 | Apakah seluruh karyawan pada Diskominfosan Kabupaten Bangli didorong dan tahu caranya melaporkan risiko atau kekhawatiran kepada pihak yang bertanggung jawab, kapan saja dibutuhkan? | √ | |
| **EDM03.03 Memantau manajemen risiko** | | | |
| 8 | Apakah setiap masalah manajemen risiko selalau di laporkan kepada managemen atau pimpinan pada Diskominfosan Kabupaten Bangli? | √ | |

**APO12 Manage Risk**

**TUJUAN:** Untuk mengelola resiko mulai dari merencanakan, menerapkan, dan memantau kerangka kerja manajemen risiko yang efektif, serta menjadikannya bagian integral dari manajemen risiko organisasi secara luas

| No | Aktivitas Tata Kelola | TEMUAN | |
|---|---|---|---|
| | | Y | T |
| **APO12.01 Mengumpulkan data.** | | | |
| 1 | Apakah Diskominfosan Kabupaten Bangli menetapkan dan mengelola metode untuk pengumpulan, klasifikasi, dan analisis data terkait risiko keamanan informasi? | √ | |

| | | | |
|---|---|---|---|
| 9 | Apakah Diskominfosan Kabupaten Bangli mengelola dan memantau akses ke sistem informasi dan data dari jarak jauh, misalnya melalui perangkat seluler atau teleworking (bekerja dari rumah), seperti pembatasan akses, pengaturan VPN, pemantauan aktivitas, dan lain-lain. | ✓ | |
| 10 | Apakah Diskominfosan Kabupaten Bangli mengelola konfigurasi jaringan dengan cara yang aman, seperti melalui pembatasan akses, pengaturan *firewall*, pengaturan alamat IP, pemantauan aktivitas, enkripsi koneksi jaringan, dan lain sebagainya | ✓ | |
| 11 | Apakah Diskominfosan Kabupaten Bangli menerapkan proses kontrol dan pembatasan akses ke jaringan komputer melalui perangkat seperti komputer atau perangkat mobile yang terhubung ke jaringan? | ✓ | |
| 12 | Apakah Diskominfosan Kabupaten Bangli melindungi sistem dari perubahan, kerusakan, atau manipulasi yang tidak sah untuk menjaga integritas sistem? | ✓ | |
| 13 | Apakah Diskominfosan Kabupaten Bangli melindungi perangkat ponsel/tablet yang digunakan untuk kerja juga dilindungi dengan fitur pemblokiran situs web atau tautan berbahaya? | ✓ | |
| 14 | Ketika sebuah komputer atau perangkat pengolah data tidak lagi digunakan, apakah Diskominfosan memastikan data sensitif dihapus secara total dan aman? | ✓ | |
| 15 | Apakah Diskominfosan Kabupaten Bangli melakukan pemfilteran situs web, memblokir tautan email yang berbahaya, dan menonaktifkan tautan klik-tayang (yaitu tautan yang otomatis mengarahkan pengguna ke situs web tanpa persetujuan pengguna) pada perangkat mobile. | ✓ | |
| **DSS05.04 Mengelola identitas pengguna dan akses logis.** | | | |
| 16 | Apakah hak akses (ke sistem dan data) setiap pengguna layanan pusat data dibatasi hanya pada yang benar-benar dibutuhkan untuk pekerjaannya? | ✓ | |
| **DSS05.05 Mengelola akses fisik ke aset keamanan informasi.** | | | |
| 17 | Apakah semua pengunjung (termasuk teknisi/vendor) yang masuk ke area server atau ruang TI selalu dicatat dan dipantau? | ✓ | |
| 18 | Apakah semua staf dan vendor diwajibkan untuk selalu memakai tanda pengenal saat berada di dalam area kantor/fasilitas? | ✓ | |
| 19 | Apakah pengunjung (termasuk vendor) yang masuk ke area sensitif selalu didampingi oleh staf Diskominfosan Kabupaten Bangli? | ✓ | |
| 20 | Apakah area sensitif pada pusat data dilindungi oleh pembatasan fisik (kunci, pagar, CCTV, dll.) untuk mengontrol akses? | ✓ | |
| **DSS05.06 Mengelola dokumen sensitif dan perangkat keluaran.** | | | |
| 21 | Apakah ada aturan yang jelas tentang bagaimana cara mengelola (menerima, menyimpan, memindahkan, dan membuang) dokumen dan print out yang bersifat rahasia? | ✓ | |
| 22 | Apakah data sensitif yang tersimpan di komputer atau sistem dilindungi dengan menggunakan enkripsi (pengkodean) yang kuat? | ✓ | |
| **DSS05.07 Mengelola kerentanan dan memantau infrastruktur untuk kejadian yang terkait dengan keamanan.** | | | |
| 23 | Apakah Diskominfosan Kabupaten Bangli menggunakan portofolio teknologi, layanan, dan aset yang didukung (pemindai kerentanan, fuzzer dan *sniffer*, penganalisis protokol) untuk mengidentifikasi kerentanan keamanan informasi? | ✓ | |
| 24 | Apakah Diskominfosan Kabupaten Bangli menetapkan dan mengkomunikasikan skenario risiko, sehingga mudah dikenali, dan kemungkinan dampaknya dipahami? | ✓ | |
| 25 | Apakah Diskominfosan Kabupaten Bangli meninjau log peristiwa secara berkala untuk mengetahui potensi insiden? | ✓ | |

| | | | |
|---|---|---|---|
| 26 | Apakah Diskominfosan Kabupaten Bangli memastikan laporan (tiket) insiden keamanan segera dibuat ketika hasil pemantauan menemukan adanya potensi insiden? | V | |

Sumber : (ISACA COBIT Governance and Management Objectives, 2019; Toolkit Indeks KAMI, 2023)

Tanda tangan & Nama Responden: I Ws Arya Durniawan, SS., M.I.Kom

## RIWAYAT HIDUP PENULIS

I Nyoman Suarka, lahir pada 15 Mei 1977 di Kabupaten Bangli. Penulis merupakan anak ketiga dari pasangan I Nengah Belek dan Ni Nengah Kumpul, yang beralamatkan di banjar adat Bebalang, lingkungan Bebalang, kelurahan Bebalang, kecamatan dan kabupaten Bangli, provinsi Bali. Penulis telah menempuh pendidikan formal di SD Negeri 1 Bebalang tahun 1987, selanjutnya di SMP Negeri 3 Bangli tahun 1993, selanjutnya di SMA Negeri 1 Bangli tahun 1996, setelah itu pendidikan D3 di AMIK Denpasar tahun 1999 dan pendidikan S1 di STIMIK Asia Malang tahun 2002. Dalam pekerjaan penulis sempat bekerja di Koran NusaBali sebagai EDP (Electronic Data Processing), selain itu juga pernah bekerja di SMK Dwijendra Denpasar menjadi guru dan tahun 2010 penulis lulus seleksi menjadi guru PNS di Kabupaten Bangli. Selama menjadi guru PNS di Bangli penulis sempat mengajar di SMP dan SMA Gurukula dan akhirnya tahun 2018 dimutasikan ke SMK Negeri 4 Bangli hingga saat ini. Didorong atas keinginan belajar dan menambah pengetahuan yang lebih luas, akhirnya pada tahun 2022 penulis melanjutkan lagi studi S2 pada Universitas Pendidikan GANESHA Singaraja dengan bidang studi Ilmu Komputer. Dengan semangat yang tertatih-tatih dan dukungan dari berbagai pihak, diakhir studi penulis selesai melakukan penelitian tesis pada Dinas Komunikasi Informasi dan Persandian Kabupaten Bangli dengan judul Evaluasi Keamanan Informasi Pemerintah Kabupaten Bangli Menggunakan Kombinasi Framework Indeks Kami 5.0 dan Cobit 2019. Di bawah bimbingan tesis Kadek Yota Ernanda Aryanto, S.Kom., M.T., Ph.D, dan Prof.Dr. I Made Candiasa, M.I.Kom serta pembimbing akademik Dr. Ir. I Made Gede Sunarya, S.Kom., M.Cs. akhirnya tahun 2026 penulis dapat menyelesaikan proses pendidikan S2. Untuk kepentingan penelitian lebih lanjut penulis dapat dihubungi melalui e-mail: manksuarka@gmail.com