BAB I

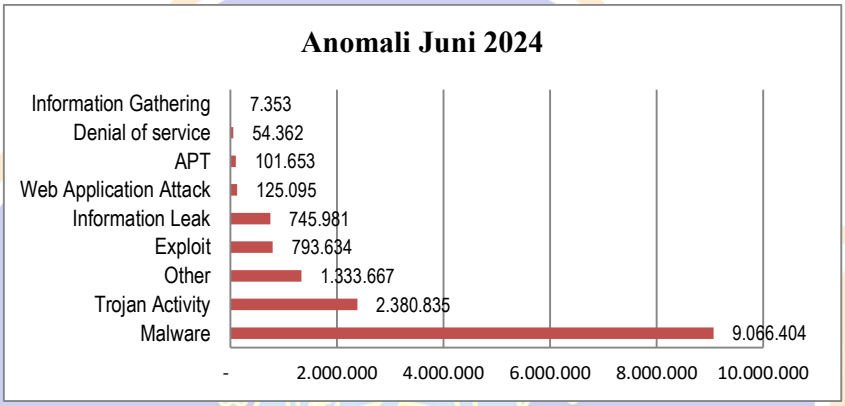
PENDAHULUAN

1.1 Latar Belakang Masalah

Perkembangan TI (Teknologi Informasi) di Indonesia telah menjadi pendorong utama adanya transformasi sosial dan ekonomi. Hal ini mendorong digitalisasi layanan publik, efisiensi industri, serta transparansi pada pemerintahan (Cholik, 2021). Namun, tantangan akan keamanan data, kesenjangan digital, dan kesiapan sumber daya manusia harus terpenuhi. Dengan demikian pemanfaat teknologi dapat dirasakan secara optimal. Untuk hasil yang baik, diperlukan kolaborasi antara pemerintah, industri, dan masyarakat dalam memperkuat regulasi keamanan informasi (Sudarmanto et al., 2024).

Serangan terhadap keamanan informasi di Indonesia sangatlah besar dan semakin kompleks. Hal ini terlihat dari peningkatan peretasan data pribadi dan serangan siber seperti spionase, *hacking*, dan kebocoran informasi (Makbull Rizki, 2022). Salah satu kasus serangan siber yang paling dahsyat terjadi pada bulan Juni 2024. Dimana serangan tersebut menargetkan Pusat Data Nasional (PDN), yang mempengaruhi lebih dari 160 lembaga pemerintah, termasuk layanan imigrasi dan operasi bandara. Dalam siaran pers Wamenkominfo Nezar Patria, peretasan PDN terjadi akibat adanya serangan siber oleh *Brain Cipher* dengan menggunakan aplikasi *ransomware* (Komdigi.go.id, 2024). *Ransomware* merupakan perangkat lunak yang bekerja dengan cepat seperti virus untuk dapat mengenkripsi data baik secara keseluruhan maupun sebagian.

Hasil laporan BSSN (Badan Siber dan Sandi Negara) pada bulan Juni 2024, telah terjadi peningkatan anomali trafik mulai bulan Mei sebanyak 12.273.078 anomali menjadi 14.608.983. Dengan jumlah anomali tertinggi terjadi pada tanggal 5 Juni 2024 yaitu sebesar 863.392 anomali trafik (BSSN RI, 2024). Secara umum pada awal Januari 2024 hingga pertengahan Juni 2024 terdapat 91.413.397 terjadi trafik anomali, 17,45% aktivitas dari *trojan* dan 59,61% merupakan aktivitas dari *malware* (BSSN RI, 2024).



Gambar 1.1 Klasifikasi Anomali Juni 2024
(Sumber: Laporan Bulanan Publik BSSN RI Juni, 2024)

Melalui BSSN dan CSIRT (*Computer Security Incident Response Team*) selaku institusi terdepan dalam melawan ancaman siber di Indonesia, pemerintah dengan segala upaya berupaya meningkatkan keamanan siber nasional. Keamanan siber yang tangguh menuntut integrasi harmonis antara kepastian regulasi (legalitas), ketahanan infrastruktur (teknis), dan tata kelola internal (organisasi). Hal ini harus didukung oleh penguatan kompetensi SDM (kapasitas) serta sinergi strategis (kerja sama) antar pemangku kepentingan demi menciptakan ekosistem digital yang aman. Selain itu pula menurut Khando dkk. (2021), faktor-faktor tambahan seperti integrasi dukungan manajemen, pelatihan, budaya keamanan,

serta penyesuaian terhadap karakteristik demografis dan pengalaman kerja pegawai perlu lebih dioptimalkan.

Untuk melindungi data dan informasi secara nasional, pemerintah Indonesia telah menerapkan berbagai regulasi dan kebijakan. Regulasi tersebut bertujuan untuk meningkatkan keamanan siber dan data dari berbagai sektor, terutama pada pemerintahan dan layanan publik. Pada UURI Tahun 2008 nomor 11, dan telah dilakukan perbaikan pada tahun 2016 UURI Nomor 19, di dalam pasal 15 pada ayat 1 menyebutkan:

> "*Setiap Penyelenggara Sistem Elektronik harus menyelenggarakan Sistem Elektronik secara andal dan aman serta bertanggungjawab terhadap beroperasinya Sistem Elektronik sebagaimana mestinya*".

Tercantum juga dalam Peraturan Pemerintah No. 82 Tahun 2012 pada pasal berikutnya 14 dan ayat 1, bahwa:

> "*Penyelenggara Sistem Elektronik wajib memiliki kebijakan tata kelola, prosedur kerja pengoperasian, dan mekanisme audit yang dilakukan secara berkala terhadap Sistem Elektronik*".

BSSN dalam menjaga stabilitas keamanan siber nasional tahun 2020 juga mengeluarkan regulasi untuk mengatur pengamanan pada penyelenggara sistem elektronik. Selain itu juga untuk menjaga hak-hak atas kepemilikan data, kewajiban bagi pengelola data, serta upaya hukum bagi yang menyalahgunakan data pribadi masyarakat. Dalam menjaga akan keamanan data pribadi, pemerintah kembali mengeluarkan regulasi tahun 2022, perihal Perlindungan Data Pribadi (UU RI Nomor 27, 2022).

Untuk mendorong pertumbuhan ekonomi digital dan pengaturan informasi elektronik secara menyeluruh, Pemerintah Daerah Kabupaten Bangli, telah mengambil langkah signifikan dalam mengimplementasikan Sistem Pemerintahan

Berbasis Elektronik (SPBE). Penyelenggaraan SPBE pada Pemerintah Kabupaten Bangli telah tertuang dalam Peraturan Daerah Kabupaten Bangli Nomor 1 Tahun 2012, Road Map Reformasi Birokrasi Tahun 2022-2024, dan juga Peraturan Bupati Bangli tentang Penerapan SPBE pada Pemerintah Kabupaten Bangli menuju Bangli yang SMART (Perbup Bangli Nomor 16, 2023)

Keberhasilan SPBE tidak hanya berpijak pada kecanggihan perangkat keras, melainkan pada terciptanya ekosistem digital yang harmonis. Hal ini menuntut ketersediaan infrastruktur yang reliabel sekaligus pemberdayaan sumber daya manusia sebagai penggerak utama inovasi dalam tata kelola pemerintahan. Dalam penelitian Juliantari dkk. (2020), Pemerintah Daerah Kabupaten Bangli telah memiliki perangkat teknologi informasi yang layak, sehingga mampu untuk menyelenggarakan SPBE dan menambah keunggulan kompetitif sebagai nilai tambah bagi organisasi. Berbagai aplikasi SPBE yang telah mendukung kinerja Pemerintah Kabupaten Bangli di antaranya, Sistem Informasi Kepegawaian (SIMPEG), e-kinerja Sadiapadu, sistem rencana, sistem anggaran, sistem kontrol, sistem pengelolaan asset dan aplikasi elektronik lainnya. Melalui skema interaksi *Government-to-Government* (G2G) dan *Government-to-Citizen* (G2C), rangkaian *platform* ini berperan sebagai jembatan digital yang memfasilitasi kolaborasi birokrasi sekaligus mendekatkan kehadiran negara dalam memenuhi kebutuhan setiap individu.

Secara umum seluruh aplikasi yang ada di Kabupaten Bangli saling terintegrasi ke dalam sistem *Goverment Resource Management System* (GRMS) dan berada dalam pengawasan Diskominfosan Kabupaten Bangli. Pengelolaan sumber daya pemerintahan yang terintegrasi, digunakan untuk mengelola berbagai

aspek pemerintahan, mulai dari penyusunan anggaran, perencanaan proyek, pengadaan barang/jasa, hingga monitoring kinerja pada pemerintah. Sehingga menjadi tanggung jawab yang sangat besar Diskominfosan Kabupaten Bangli dalam menjaga operasional, integritas, ketersediaan, dan kerahasiaan data pemerintahan.

Sesuai dengan keterangan dari Plt. Kepala Bidang Persandian dan Keamanan Informasi Diskominfosan Kabupaten Bangli, serangan siber berupa *malware, phishing*, dan *Distributed Denial of Service* (DDoS) sering mengganggu operasional pusat data yang ada. Apalagi dengan minimnya dana anggaran, infrastruktur, serta tenaga kerja yang terlatih, pastinya risiko meningkatknya kebocoran akan tinggi begitu juga operasional akan mengalami keterlambatan.

Berbagai upaya telah dilakukan oleh Diskominfosan Kabupaten Bangli seperti halnya peningkatan kapasitas SDM, penguatan infrastruktur keamanan dan pembentukan tim respons insiden. Selain langkah-langkah tersebut, upaya analisis dan evaluasi atas keamanan pusat data Diskominfosan Kabupaten Bangli perlu menjadi perhatian. Mengacu pada Peraturan Presiden bahwasannya seluruh audit SPBE yang meliputi audit keamanan infrastruktur dan audit keamanan aplikasi, baik bersifat umum ataupun khusus paling sedikit dilaksanakan 1 (satu) kali dalam kurun waktu 2 (dua) tahun (Perpres Nomor 95, 2018). Namun hingga saat ini Diskominfosan Kabupaten Bangli belum pernah untuk melakukan audit dan evaluasi keamanan informasi yang memenuhi standar yang ditetapkan.

Dalam melakukan evaluasi SMKI (Sistem Manajemen Keamanan Informasi), terhadap beberapa standar yang dapat digunakan di antaranya, *Information Technology Infrastructure Library (ITIL*), COBIT, dan *Val IT*. Selain kerangka

kerja tersebut, terdapat pula alat ukur yang dikembangkan BSSN. Indeks KAMI (Keamanan Informasi) merupakan kerangka kerja yang bertugas menilai kesiapan dan tingkat keamanan informasi suatu organisasi, terutama di sektor pemerintahan dan lembaga yang mengelola data strategis (Surya et al., 2024).

Indeks KAMI merupakan standar keamanan informasi yang berbasis pada SNI ISO/IEC 27001, mengacu pada kerangka kerja yang lebih luas dalam pengelolaan risiko. Indeks KAMI membantu organisasi dalam memahami kebijakan dan penerapan keamanan informasi yang telah dilakukan dan memberikan rekomendasi peningkatan berdasarkan hasil evaluasi (Khusna, 2023). Indeks KAMI memiliki pendekatan yang komprehensif, dan fleksibel dalam evaluasi keamanan informasi. Terdapat lima aspek utama meliputi, pengelolaan risiko, tata kelola, kerangka kerja kebijakan dan prosedur, manajemen aset, serta penerapan teknologi keamanan informasi (Dewi, 2021).

Selain Indeks KAMI, COBIT merupakan kerangka kerja dan manajemen TI yang dipergunakan secara global dan dikembangkan oleh ISACA. Kerangka kerja ini dirancang untuk melaksanakan tugas organisasi dalammenyelaraskan strategi TI dan tujuan bisnis, sekaligus memastikan manajemen risiko, keamanan, dan kepatuhan yang efektif (Wijanarko, 2023). Salah satu kemampuannya yaitu untuk menilai dan meningkatkan kemampuan manajemen keamanan informasi organisasi. Dengan menyediakan pendekatan terstruktur untuk mengelola proses TI, memastikan bahwa risiko keamanan diidentifikasi, dikurangi, dan dipantau secara terus-menerus (Haay & Sitokdana, 2022). COBIT dapat diintegrasikan dengan standar keamanan dan manajemen risiko yang lain seperti *NIST Cybersecurity Framework*, *ISO/IEC 27001*, dan sebagainya. Sehingga

memungkinkan organisasi untuk mengadopsi praktik terbaik sambil tetap mematuhi persyaratan peraturan (Titan et al., 2024).

Dalam kesempatan ini, penulis meneliti tentang tata kelola keamanan informasi pada Pemerintah Daerah Kabupaten Bangli. Dengan fokus penelitian pada pengelolaan keamanan informasi pusat data E-Kinerja SADIAPADU pada Diskominfosan Pemerintah Kabupaten Bangli. Penelitian ini menghadirkan pendekatan baru dengan mengintegrasikan kerangka kerja Indeks KAMI 5.0 dan COBIT 2019. Indeks KAMI 5.0 akan mengukur kematangan kebijakan dan implementasi keamanan informasi sedangkan COBIT 2019 mengukur tata kelola, pengendalian risiko, dan efektivitas proses keamanan informasi. Informasi dan data diperoleh melalui proses observasi, wawancara dan penyebaran kuesioner terhadap pejabat dan staf Diskominfosan Kabupaten Bangli. Observasi dilakukan dengan melihat secara fisik pusat data dan kebijakan yang berjalan, serta dilakukan studi dokumen seperti berbagai SK (surat keputusan), berbagai SOP (standar operasional prosedur) yang ada, serta hasil laporan audit, dan kebijakan keamanan informasi yang ada.

Penggunaan kerangka kerja Indeks KAMI 5.0 dan COBIT 2019 secara simultan masih terbatas, beberapa penelitian telah mulai memetakan elemen-elemen Indeks KAMI ke standar internasional. Dalam hasil penelitian Supriyanto dkk.(2025) dengan berjudul "*Alignment of KAMI Index with Global Security Standards in Information Security Risk Maturity Evaluation*" menguji kesesuaian Indeks KAMI dengan standar global, menunjukkan adanya upaya harmonisasi namun belum bersifat komprehensif untuk konteks tata kelola proses TI. Penelitian lain yang menggabungkan 2 (dua) kerangka kerja yaitu Wibawa dkk. (2024),

dengan judul "*Information Security Evaluation at Hospital Using Index KAMI 5.0 and Recommendations Based on ISO/IEC 27001:2022*". Sejumlah studi juga telah menggabungkan pendekatan tata kelola COBIT dengan *framework* lainnya seperti ISO 27001:2013, seperti penelitian Aflakhah & Soewito (2023), yang berjudul "*Assessing Information Security using COBIT 2019 and ISO 27001:2013 for Developing a Mitigation Plan*". Penggabungan Indeks KAMI dengan COBIT saat ini baru dilakukan oleh Habibullah dkk. (2024) dan Bahri dkk. (2025) dengan studi kasus pada institusi pendidikan atau pondok pesantren. Kajian pemetaan Indeks KAMI dengan COBIT pada penelitan tersebut masih relatif terbatas dari segi keluasan sampel dan penerapan pada level pemerintahan daerah (OPD).

Dengan demikian, terdapat kekosongan penelitian pada hal model evaluasi yang mengintegrasikan Indeks KAMI 5.0 dan COBIT 2019 secara simultan, untuk menilai keamanan SPBE di pemerintahan daerah secara empiris dan kontekstual. Penelitian ini dapat mengisi *research gap* tersebut dengan menerapkan pendekatan terintegrasi Indeks KAMI 5.0 dengan COBIT 2019 untuk: (1) menghasilkan pengukuran kematangan keamanan informasi yang komprehensif dan kontekstual untuk Diskominfosan Kabupaten Bangli; (2) memperlihatkan bagaimana kondisi tata kelola keamanan informasi yang ada melalui Indeks KAMI dan COBIT, dan (3) menyusun rekomendasi peningkatan tata kelola keamanan SPBE yang selaras antara kebijakan nasional dan praktik tata kelola sesuai standar COBIT 2019.

Lebih lanjut penelitian ini memiliki urgensi yang sangat tinggi dalam era digital saat ini. Pemerintah daerah dihadapkan pada tantangan besar dalam melindungi data sensitif dan memastikan kelangsungan operasional layanan publik. Serangan siber yang semakin canggih dan meningkatnya ancaman terhadap

infrastruktur TI pemerintah menuntut adanya evaluasi menyeluruh terhadap sistem keamanan informasi yang ada. Berdasarkan laporan *National Audit Office* (NAO) di Inggris, departemen pemerintahan menghadapi ancaman siber yang parah dan berkembang dengan cepat, dengan banyak sistem TI kritis yang rentan terhadap serangan (Nao.org.uk, 2025). Menurut Sulubara (2024), dalam jurnal bidang Ilmu Pertahanan Hukum dan Komunikasi, kasus *cybercrime* berupa pencurian akan data, peretasan *website* pemerintah, dan kebocoran data dari lembaga pemerintah mengalami peningkatan signifikan. Kasus-kasus menunjukkan kerentanan infrastruktur digital Indonesia. Oleh karena itu, penelitian ini menjadi krusial untuk mengidentifikasi celah keamanan, menilai efektivitas kontrol, dan dapat merekomendasikan suatu hasil yang dapat dilaksanakan dalam meningkatkan ketahanan siber di tingkat daerah.

Dalam penelitian kali ini penulis memiliki beberapa alasan, pertama berdasarkan penelitian yang dilakukan oleh Dicky Insan Khamil dkk. Peneliti mengevaluasi pengelolaan keamanan, serta kesiapan dalam pelaksanaan keamanan informasi. Dengan kondisi, sistem keamanan informasi tersebut sesuai dengan Permenkominfo nomor 4 pada tahun 2016 serta Standar ISO/IEC 27001. Dari hasil akhir evaluasi menunjukkan, skor akhir 190 yang berarti status kesiapan yang dimiliki "Tidak Layak". Hal ini menunjukan bahwa Diskominfo Kabupaten Gianyar belum memenuhi Standar ISO/IEC 27001 dan perlu peningkatan efektifitas kinerja keamanan informasi terutama dalam aspek manajemen risiko dan area kerangka kerja pegawai.

Kedua, melalui formalisasi regulasi dalam Peraturan Bupati Bangli Nomor 16 Tahun 2024, Pemerintah Kabupaten Bangli menegaskan komitmennya untuk

memperkuat tata kelola keamanan informasi. Langkah ini menjadi landasan hukum yang krusial dalam menjamin keamanan data publik di dalam ekosistem SPBE. Sehingga penulis berupaya memberikan rekomendasi dan solusi konkret terhadap serangan dan ancaman keamanan informasi yang semakin meningkat. Penulis pula berupaya memberikan gambaran tentang manajemen keamanan SPBE yang sesuai dengan standar yang ada terutama standar COBIT 2019.

Ketiga, penilaian dengan kerangka kerja yang diakui secara nasional dan internasional seperti Indeks KAMI 5.0 dan COBIT 2019, akan dapat memberikan hasil kerangka kerja yang komprehensif dan mutakhir. Sehingga dapat meningkatkan keamanan informasi di Diskominfosan Kabupaten Bangli. Dalam upaya memperkuat resiliensi digital, pengukuran dilakukan melalui Indeks KAMI 5.0 yang meninjau aspek fundamental mulai dari tata kelola hingga perlindungan aset. Analisis ini diperdalam dengan mengadopsi standar COBIT 2019, pada domain manajemen risiko dan operasional keamanan, guna memastikan bahwa setiap instrumen teknologi yang digunakan benar-benar mampu melindungi kepentingan seluruh pemangku kepentingan.

Berdasarkan uraian latar belakang di atas, penulis melakukan penelitian dengan tema "Evaluasi Keamanan Informasi Menggunakan Kombinasi *Framework* Indeks KAMI 5.0 dan COBIT 2019 dengan Studi Kasus pada Diskominfosan Pemerintah Kabupaten Bangli"

1.2 Identifikasi Masalah

Berdasarkan uraian latar belakang tersebut, penulis mengidentifikasi beberapa masalah yang ada sebagai berikut.

1) Upaya penanganan keamanan informasi pada pusat data Diskominfosan Kabupaten Bangli selama ini dilakukan secara spontan, tidak terencana dan tidak terdokumentasi. Hal ini disebabkan kurangnya informasi mengenai kondisi keamanan informasi pusat data, serta belum ada acuan formal dalam mengidentifikasi risiko dan langkah perbaikan yang sistematis.
2) Belum pernah dilakukan analisis kesiapan dan kematangan keamanan informasi pada Diskominfosan Kabupaten Bangli terutama pada pusat data E-Kinerja SADIAPADU sejak dilaunching pada bulan Juni 2021.
3) Pengelolaan keamanan informasi pada instansi-instansi di bawah Pemerintah Daerah Kabupaten Bangli saat ini masih minim.
4) Pusat data Diskominfosan Kabupaten Bangli sering mengalami serangan siber, menyebabkan layanan publik Pemerintah Kabupaten Bangli tidak dapat beroperasi secara maksimal.

1.3 Batasan Masalah

Agar masalah tidak melebar, penulis membatasi penelitian ini sebagai berikut.

1) Fokus penelitian hanya pada tata kelola keamanan informasi pusat data E-Kinerja SADIAPADU Pemerintah Kabupaten Bangli pada Diskominfosan Kabupaten Bangli, bukan aspek lain dari fitur-fitur sistem informasi.
2) Evaluasi Indeks KAMI berfokus pada pengukuran tingkat kesiapan, kelengkapan, dan kepatuhan penerapan keamanan informasi berdasarkan standar ISO 27001. Sehingga akan memberikan gambaran proses keamanan

informasi pada E-Kinerja SADIAPADU Diskominfosan Kabupaten Bangli secara umum.

3) Evaluasi kapabilitas proses keamanan informasi diimplementasikan menggunakan instrumen COBIT 2019. Fokus pengukuran diarahkan pada titik-titik kritis tata kelola yang meliputi optimasi risiko (*EDM03*), manajemen risiko (*APO12*), penyelarasan keamanan (*APO13*), hingga aspek teknis seperti manajemen konfigurasi (*BAI10*), kontinuitas bisnis (*DSS04*), serta operasional layanan keamanan (*DSS05*).

4) Evaluasi keamanan informasi tidak melibatkan pengujian secara teknis seperti *Application Security Testing, Penetration Testing*, *atau Network Security Testing,* hanya berlandaskan persepsi dan penilaian subjektif responden terhadap kondisi keamanan informasi yang ada.

5) Observasi yang dilakukan hanya menilai proses kesiapan tata kelola dan kematangan keamanan informasi, tidak mencangkup kerentanan teknis sistem secara langsung. Berdasarkan hasil pengukuran tingkat kematangan Indeks KAMI 5.0 dan COBIT 2019, rekomendasi yang dihasilkan tetap memiliki dasar yang objektif. Perlu kajian lebih lanjut untuk evaluasi kemanan sistem secara teknis untuk melindungi infrastruktur dari akses ilegal, peretasan, dan serangan siber, serta memastikan kerahasiaan data tetap terjaga, akurasi informasi terjamin, dan sistem selalu dapat diakses oleh pengguna yang berwenang

1.4 Rumusan Masalah

Berdasarkan identifikasi dan pembatasan masalah di atas, permasalahan yang menjadi fokus penelitian ini adalah seperti berikut.

1) Bagaimana hasil penilaian menyeluruh terhadap tata kelola keamanan informasi pada Pusat Data E-Kinerja SADIAPADU Kabupaten Bangli dengan mengomparasikan parameter Indeks KAMI 5.0 serta praktik terbaik dari COBIT 2019?
2) Berapakah *capability maturity level* (tingkat kemampuan dan kematangan) pengelolaan keamanan informasi yang ada saat ini, dengan pengukuran menggunakan Indeks KAMI 5.0 dan COBIT 2019?
3) Aspek atau domain tata kelola keamanan informasi mana saja yang memiliki level rendah dan belum memenuhi standar diharapkan?
4) Strategi peningkatan apa yang dapat direkomendasikan untuk peningkatan pengelolaan keamanan informasi pada pusat data E-Kinerja SADIAPADU Pemerintah Kabupaten Bangli sesuai dengan framework COBIT 2019?

1.5 Tujuan Penelitian

Sesuai rumusan masalah di atas, tujuan yang ingin dicapai dalam penelitian ini adalah sebagai berikut.

1) Untuk mengetahui hasil penilaian proses tata kelola keamanan informasi terhadapat pusat data E-Kinerja SADIAPADU Pemerintah Kabupaten Bangli menggunakan *framework* Indeks KAMI 5.0 dan COBIT 2019.

2) Untuk mengetahui tingkat *capability maturity level* tata kelola keamanan informasi pada pusat data E-Kinerja SADIAPADU Pemerintah Kabupaten Bangli berdasarkan pengukuran Indeks KAMI 5.0 dan COBIT 2019.

3) Untuk mengetahui aspek atau domain tata kelola keamanan informasi pusat data E-Kinerja SADIAPADU yang menunjukkan level rendah dan belum memenuhi standar level yang diharapkan.

4) Merumuskan strategi dan rekomendasi peningkatan pengelolaan keamanan informasi pusat data E-Kinerja SADIAPADU Pemerintah Kabupaten Bangli sesuai standar COBIT 2019.

1.6 Manfaat Penelitian

1.6.1 Manfaat Teoretis

Manfaat yang diperorel secara teoretis dari penelitian ini meliputi.

1) Mampu memberikan wawasan tentang evaluasi tata kelola keamanan informasi pada pusat data E-Kinerja SADIAPADU dengan memanfaatkan *framework* Indeks KAMI 5.0 dan COBIT 2019.

2) Sebagai referensi untuk studi lanjutan yang berhubungan dengan penilaian tata kelola evaluasi keamanan informasi didasarkan pendekatan Indeks KAMI 5.0 dan COBIT 2019 sub domain EDM03, APO12, APO13, BAI10, DSS05, DSS04.

3) Meningkatkan pengetahuan tentang penilaian tata kelola keamanan informasi pusat data E-Kinerja SADIAPADU di Dinas Komunikasi Informasi dan Persandian Kabupaten Bangli.

1.6.2 Manfaat Praktis

Manfaat secara praktis dalam studi ini sebagai berikut.

1) Dapat menjadi acuan dalam menciptakan keamanan informasi pusat data yang lebih baik didasarkan pada arsitektur *framework* COBIT 2019 domain BAI (*Build, Acquare and Implement) ,* EDM *(Evaluate Direct and Monitor)*, DSS (*Deliver Service and Support)*, dan APO (*Align Plan and Organize)*
2) Mengetahui proses sejauh mana *capability maturity level* yang dihasilkan, sehingga dapat dijadikan sebagai rekomendasi Dinas Komunikasi Informatika dan Persandian Kabupaten Bangli.
3) Berkembang menjadi sumber daya yang dapat digunakan untuk memberikan saran perbaikan pada keamanan informasi pusat data berdasarkan arsitektur COBIT 2019 dan Indeks KAMI 5.0
4) Memberikan contoh bagi SKPD (Satuan Kerja Perangkat Daerah) lain di bawah Pemerintah Kabupaten Bangli, untuk secara rutin melakukan evaluasi keamanan informasi agar mampu menciptakan pemerintahan yang lebih baik.