

LAMPIRAN

Lampiran 1. Tabel State of the Art

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
1	Aulia Oktaviana, Kusworo Adi, Budi Warsito (Oktaviana et al., 2024)	<i>Adopting COBIT 2019 for the Evaluation of Information Technology Risk Management in a Startup Company</i>	Mengevaluasi manajemen risiko proses bisnis perusahaan <i>start-up</i> XYZ yang sangat bergantung pada I&T, serta memberikan rekomendasi untuk perbaikan ke depan, khususnya dalam konteks	Kuesioner berbasis domain COBIT 2019 (APO12, EDM03)	Perusahaan telah melakukan identifikasi risiko terhadap risiko potensial dan tingkat dampaknya. Berdasarkan hasil pengukuran, kapabilitas proses EDM03 dan APO12 berada pada Level 1	Menyajikan hasil evaluasi terhadap proses EDM03 dan APO12, serta memberikan rekomendasi untuk perbaikan berkelanjutan .	Penilaian masih menunjukkan bahwa perusahaan berada di tahap awal (level 1), sehingga pelaksanaan manajemen risiko masih rendah.	Menjadi acuan awal struktur instrumen yang bisa disesuaikan dengan konteks instansi publik

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
			perubahan pasca pandemi.		dengan kesenjangan menuju target sebesar 2 level. Hasil tersebut menunjukkan bahwa penerapan proses manajemen risiko masih memerlukan penguatan dan standardisasi.			
2	Mar'atus Solikhah, Lena	<i>Implementation of the COBIT 2019 Framework on</i>	Melakukan penilaian terhadap tata	Metode kualitatif-deskriptif, menggunakan	APO12 berada pada level 3, sedangkan	Menggunakan domain APO12	Penilaian hanya terbatas pada dua subdomain (APO12 dan	Memberikan gambaran implementasi

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
	Magdalena , Muhamma d Hatta (Solikhah et al., 2024)	<i>Information Technology Governance and Risk Management (Study Case: CV. Syntax Corporation Indonesia)</i>	kelola dan manajemen I&T yang diterapkan oleh CV. Syntax Corporation Indonesia, sebagai bahan evaluasi dan peningkatan efektivitas penerapan I&T.	an <i>framework</i> COBIT 2019, dengan fokus pada subdomain APO12 dan BAI09 yang diperoleh dari hasil mapping	BAI09 berada pada Level 2, Hasil penilaian digunakan untuk membentuk <i>Critical Success Factor</i> (CSF) dan menghasilkan rekomendasi.	(<i>Managed Risk</i>) dan BAI09 (<i>Manage Assets</i>) dari COBIT 2019 secara eksplisit untuk evaluasi kapabilitas tata kelola dan manajemen risiko I&T.	BAI09), sehingga belum menyeluruh terhadap semua proses I&T dan Masih bersifat deskriptif tanpa ada uji implementasi atau validasi lanjutan. Penelitian ini menyebutkan rencana visualisasi menggunakan <i>dashboard</i> , namun tidak dijelaskan	domain APO12 dalam manajemen risiko I&T, yang dapat dijadikan perbandingan pendekatan di sektor publik.

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
							secara detail atau disertai implementasi dalam isi artikel.	
3	Adhi Fernandes Gamaliel, Gerry Firmansyah, Agung Mulyo Widodo, Budi Tjahjono (Gamaliel et al., 2024)	<i>Risk Management Analysis On The School Activity Plan and Budget Application Information System (ARKAS) Using COBIT 2019</i>	Menganalisis dan mengelola risiko dalam implementasi Sistem Informasi Rencana Kegiatan dan Anggaran Sekolah (ARKAS) untuk meningkatkan efisiensi dan	Menggunakan <i>framework</i> COBIT 2019 untuk melakukan analisis manajemen risiko I&T di lingkungan sekolah dan melakukan analisis	Identifikasi tantangan seperti resistensi terhadap perubahan, keterbatasan sumber daya, dan risiko keamanan informasi dan Rekomendasi diberikan untuk	Fokus pada lingkungan pendidikan, sehingga memberi wawasan spesifik tentang implementasi I&T di sekolah.	Tidak dijelaskan detail level kapabilitas proses dalam <i>framework</i> COBIT 2019.	Bahan komparatif untuk melihat penerapan COBIT pada aplikasi sektor publik

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
			efektivitas dalam perencanaan dan pengelolaan anggaran sekolah.	dokumen ARKAS	peningkatan kualitas manajemen anggaran sekolah dan dapat dijadikan acuan oleh sekolah lain			
4	I Made Oka Semara Putra, Linawati, I Nyoman Setiawan (Putra et al., 2023)	<i>Audit Risk Management</i> pada Sistem Evaluasi dan 273 Pengawasan Realisasi Anggaran di Kabupaten Gianyar Menggunakan	Mengawasi realisasi anggaran di setiap Organisasi Perangkat Daerah (RAO) di Kabupaten Gianyar dan Menganalisis dan menilai	Menggunakan dua <i>framework</i> utama yaitu NIST 800-30 dan COBIT 2019	Dari NIST 800-30 ditemukan 12 celah (<i>gaps</i>) dari 12 ancaman, dengan 8 risiko dikategorikan sedang (<i>medium</i>) dan	Menyediakan gambaran risiko keamanan dan efektivitas pengelolaan sistem secara detail serta Menggabungkan dua <i>framework</i>	Tidak dijelaskan secara mendalam bagaimana rekomendasi perbaikan akan diimplementasikan dan dievaluasi	Menjadi contoh untuk perluasan metode pengukuran risiko.

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
		Kerangka Kerja COBIT 2019 dan NIST 800-30	risiko serta tingkat kematangan tata kelola I&T menggunakan <i>framework</i> COBIT 2019 dan NIST 800-30.		4 risiko rendah (<i>low</i>), Dari COBIT 2019 ditemukan bahwa Nilai tertinggi pada domain APO 13 (manajemen keamanan informasi) dengan skor 4,58 (kategori <i>Fully</i> - 91%), Nilai terendah pada beberapa domain seperti APO	yang populer dan komprehensif (NIST 800-30 dan COBIT 2019) untuk analisis risiko dan tata kelola I&T	keberhasilanny a.	

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
					13 (proses 2 & 3), DSS 02, DSS 03, dan DSS 04 dengan nilai 3,00 (kategori Largely - 60%). <i>Gap</i> terbesar pada proses ketiga domain APO 14 sebesar 1,92, menunjukkan masalah pada efektivitas penggunaan data masalah yang tidak berjalan			

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
					sesuai fungsi sistem.			
5	Saul Carlos Immanuel Simatupang, Melissa Indah Fianty (Simatupang & Fianty, 2023)	<i>Assessment of Capability level s and Improvement Recommendations Using COBIT 2019 for the IT Consulting Industry</i>	Mengukur dan menilai tingkat kapabilitas tata kelola I&T perusahaan khususnya dalam hal operasional dan keamanan dan Mengidentifikasi dan memperbaiki permasalahan terkait Standar Operasional Prosedur (SOP) dokumentasi risiko I&T.	Kuesioner berbasis domain COBIT 2019; validasi ahli	Proses APO12 (Manajemen Risiko) mencapai level kapabilitas 2, dengan target level 3, terdapat gap 1 level, Proses DSS01 (Manajemen Operasi) telah mencapai level 3, memenuhi target, roses	Memberikan gambaran yang jelas tentang gap dan area yang perlu diperbaiki.	Studi belum menjelaskan secara detail langkah-langkah teknis untuk mengatasi downtime dan kehilangan data, Rekomendasi masih bersifat umum, belum spesifik pada tindakan implementasi SOP atau	Memberikan contoh nyata penerapan domain APO12 untuk mengukur kapabilitas manajemen risiko, sehingga bisa dibandingkan dengan pendekatan di Diskominfo Klungkung.

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
					DSS02 (Manajemen Layanan) mencapai Level 2, dengan target Level 3, terdapat <i>gap</i> 1 level dan SOP untuk dokumentasi risiko I&T belum lengkap atau belum optimal.		mitigasi <i>downtime</i> .	
6	Gilberth Wattimury, Ahmad Faza	COBIT 2019 <i>Implementation for Enhancing IT</i>	Meningkatkan tata kelola I&T pada institusi pendidikan	Studi dokumentasi dan wawancara	Terjadi ketidaksesuaian antara kebijakan dan	Relevan dalam menilai <i>gap</i> antara dokumen dan	Tidak eksplisit digunakan domain risiko seperti	Berguna untuk menyusun rekomendasi perbaikan kontrol

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
	(Wattimury & Faza, 2023)	<i>governance in Educational Institutions</i>	melalui <i>framework</i> COBIT 2019		implementasi kontrol I&T	praktik; bisa disesuaikan ke sektor publik	APO12/EDM03	I&T berbasis praktik nyata
7	I Nyoman Rai Widartha Kesuma, Irman Hermadi, Yani Nurhadrya ni (Kesuma et al., 2023)	Evaluasi Tata Kelola Teknologi Informasi di Dinas Pertanian Gianyar Menggunakan COBIT 2019	Meningkatkan pelayanan publik dan kapasitas serta akuntabilitas kinerja birokrasi di Dinas Pertanian Gianyar melalui penerapan I&T menggunakan COBIT 2019	Menggunakan <i>framework</i> COBIT 2019 sebagai standar evaluasi tata kelola I&T yang lengkap dan komprehensif dan menggunakan 3 domain	Ketiga proses prioritas (MEA03, BAI04, EDM03) baru mencapai tingkat kapabilitas level 1.	Fokus pada proses prioritas yang sangat relevan untuk peningkatan kepatuhan, ketersediaan layanan, dan pengelolaan risiko.	Tidak dijelaskan secara rinci kendala-kendala yang dihadapi organisasi dalam mengimplementasikan tata kelola I&T.	Menjadi referensi pendekatan FGD dan pengambilan data pada sektor pemerintah daerah

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
				yaitu MEA03, BAI04 dan EDM03				
8	Ike Pertiwi Windasari, Adian Fatchur Rochim, Septi Nurna Alfiani, Azizah Kamalia (Windasari et al., 2022)	Audit Tata Kelola Teknologi Informasi Domain <i>Monitor, Evaluate, and Asses dan Deliver, Service, Support</i> Berdasarkan <i>Framework</i> COBIT 2019	Mengukur tingkat kematangan (<i>maturity</i>) pelaksanaan I&T di universitas.	Menggunakan <i>framework</i> COBIT 2019 dengan fokus pada dua domain yaitu MEA dan DSS	Tingkat kapabilitas I&T universitas pada domain MEA dan DSS berada di level 1 (<i>Performed</i>)	Fokus pada dua domain penting yang sangat berpengaruh pada pengawasan dan pelayanan I&T di institusi pendidikan.	Tidak bahas risiko; hanya audit proses layanan	Pelengkap metodologi audit dan pemetaan proses I&T

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
9	Achmad Muchsinul Huda MJ (MJ, 2021)	Evaluasi Manajemen dan Tatakelola Teknologi Informasi pada Dinas Kominfo Kota Malang dengan Menggunakan <i>Framework</i> COBIT 2019	Mengidentifikasi prioritas proses manajemen dan tata kelola I&T pada Dinas KOMINFO Kota Malang	Menggunakan <i>Design Factor</i> dalam COBIT 2019 dengan domain BAI11	Tingkat kapabilitas BAI11 saat ini berada pada Level 2, sementara target yang ingin dicapai adalah level 3	Objek penelitian sesuai konteks saya (Diskominfo) dan Pendekatan menggunakan <i>Design Factor</i> COBIT 2019 membantu menentukan fokus prioritas yang tepat sesuai kebutuhan organisasi.	Tidak eksplisit gunakan domain risiko seperti APO12 atau EDM03, Penelitian fokus hanya pada satu proses (BAI11), sementara proses tata kelola I&T lain yang juga penting kurang dievaluasi.	Mendekati topik penelitian dan sangat relevan untuk dijadikan pembanding
10	Tata Sutabri, Aria	Analisa Domain Operasional	Menilai tingkat kematangan pengelolaan	Kuesioner dan skoring kapabilitas	Level kapabilitas proses <i>e-Gov</i>	Menggunakan domain manajemen	Tidak dijelaskan cara validasi	Relevan sebagai model pengukuran awal

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
	Dinata, Majduddin, Nyimas Hamidah Purnama Agustriani (Sutabri et al., 2024)	Untuk Pengukuran Tingkat Kematangan Tata Kelola Layanan E-Government Menggunakan Framework COBIT 2019 Pada Dinas Kominfo Kota Palembang	risiko sistem informasi pada layanan e-Government di Dinas Komunikasi dan Informatika Kota Palembang.	dengan domain EDM03 dan APO12	(APO12 dan EDM03) masih di bawah target	risiko eksplisit dalam COBIT 2019	instrumen atau proses wawancara	pada instansi pemerintah untuk domain risiko (APO12 & EDM03)
11	Senna Kristiawan Gounwala n, Andeka Rocky Tanaamah	Penggunaan Framework COBIT 2019 dalam Evaluasi Tata Kelola Teknologi Informasi	Mengevaluasi penggunaan framework COBIT 2019 dalam tata kelola I&T di Kospin Jasa.	Studi literatur dan perbandingan	Penggunaan COBIT 2019 mampu memberikan framework yang terstruktur	Memberi dasar teori kuat untuk penggunaan COBIT 2019	Informasi spesifik mengenai hasil evaluasi kapabilitas, gap, atau rekomendasi	Bisa dijadikan bagian landasan teori mengenai kelebihan COBIT 2019

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
	(Gouwnala n & Tanaamah, 2023)				dan komprehensif dalam tata kelola I&T di Kospin Jasa.		perbaikan tidak dijelaskan secara rinci.	
12	Mohamad Adhisyanda Aditya, R Dicky Mulyana, Ali Mulyawan (Aditya et al., 2019)	Perbandingan COBIT 2019 dan ITIL V4 Sebagai Panduan Tata Kelola dan <i>Management IT</i>	Membandingkan COBIT 2019 dengan <i>ITIL V4</i>	Studi literatur dan analisis	COBIT lebih unggul secara strategis; <i>ITIL</i> di layanan operasional	Memberikan wawasan integrasi <i>framework</i> I&T	Bukan penelitian empiris dan tidak fokus pada risiko	Bagus untuk landasan teori dan pembandingan Menambah alasan menggunakan COBIT untuk mengukur risiko I&T
13	Emeka Elue, CISA, CDPSE	<i>Effective Capability and Maturity Assessment</i>	Penilaian kapabilitas dan maturitas dengan COBIT 2019	<i>Framework</i> presentation	<i>Best practice</i> kapabilitas	Referensi resmi COBIT	Bukan studi ilmiah berbasis data	Penting untuk dukung teori kapabilitas

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
	(Elue, 2020)	<i>Using COBIT 2019</i>						
14	Abdul Rafeq, CISA, FCA and Narasimhan Elangovan, CISA, CDPSE, FCA (Rafeq & Elangovan, 2021)	<i>A Systematic Approach to Implementing a Governance System Using COBIT 2019: A COVID-19 Case Study</i>	Memberikan pendekatan sistematis implementasi tata kelola menggunakan COBIT 2019	Kajian praktik industri dan studi lapangan	Tahapan implementasi COBIT bisa disesuaikan dengan kondisi organisasi dan kebutuhan fokus risiko	Pedoman implementasi menyeluruh, sangat berguna untuk penerapan COBIT	Bukan penelitian, tetapi panduan Tidak menyertakan studi kasus sektor publik secara lokal	Menjadi pedoman kerangka implementasi alat ukur di Diskominfo Klungkung
15	Odjie Dwianto, Imam Riadi	<i>Risk Assessment Analysis of Medical</i>	Analisis risiko sistem informasi	Studi kasus, wawancara	Proses risiko belum terdokumentasi baik	Fokus manajemen risiko	Masih pakai COBIT 5, bukan 2019	Berguna untuk pendekatan risiko meskipun bukan COBIT 2019

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
	(Dwianto & Riadi, 2022)	<i>Information System Services using COBIT 5 Framework</i>	medis dengan COBIT 5					
16	Juwina Mustaqfira, Ima Dwitawati, Muhammad Syamsu Rizal (Mustaqfirah et al., 2025)	Analisis Tata Kelola Teknologi Informasi pada Diskominfo Kota Sabang Menggunakan Framework COBIT 2019	Mengukur kapabilitas beberapa domain COBIT pada Diskominfo	Kuesioner dan pengolahan data	EDM03, APO12, DSS04 diidentifikasi dengan skor di level 3–4, namun ada gap pada manajemen data	Studi langsung pada instansi Diskominfo; domain risiko relevan	Tidak dijelaskan validasi instrumen atau teknik analisis lebih lanjut	Data mendukung pemilihan domain risiko yang relevan di Diskominfo
17	Anita Wulansari, Carena Learns	<i>E-Government Risk Optimization</i>	Risiko pada <i>e-government</i> selama pandemi	Literatur review	Identifikasi ancaman dan mitigasi <i>e-gov</i>	Membahas risiko I&T	Tidak memakai COBIT 2019	Berguna untuk memperkuat urgensi topik

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
	Prasetyo, Siti Mukaromah, Dhian Satria Yudha Kartika, Eristya Maya Safitri, Abdul Rezha Efrat Najaf (Wulansari et al., 2022)	<i>Capability Measurement</i>						
18	Achmad Jefri Assegaf, I	Evaluasi Tata Kelola Teknologi	Menilai kapabilitas domain APO	Audit dan kuisisioner terstruktur	Level APO08 meningkat dari 1 ke 2	Fokus pada peningkatan kapabilitas	Belum menyentuh	Pendekatan perbaikan bertahap bisa

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
	Putu Agus Eka Pratama, Made Ika Mandeni (Assegaf et al., 2023)	Informasi Menggunakan <i>Framework</i> COBIT 2019 (Studi Kasus: Dinas Perpustakaan dan Kearsipan Kota Denpasar)	dan BAI serta peningkatan level dalam waktu 1 bulan		setelah perbaikan selama 1 bulan	nyata dalam waktu singkat	domain risiko secara eksplisit	diterapkan pada domain risiko
19	Reski Wahyudi, Murdiyana, Ikhbaluddin (Wahyudi et al., 2024)	Penilaian Tata Kelola Teknologi Informasi Berbasis Kinerja Organisasi Menggunakan COBIT 2019 dan Balanced	Untuk mengevaluasi peran tata kelola I&T dalam meningkatkan kinerja organisasi pemerintahan.	Mixed method (kualitatif dan kuantitatif)	Domain APO02 mencapai level 3, sedangkan APO03, BAI05, dan DSS06 mencapai Level 2.	Menggunakan pendekatan mixed method yang memberikan hasil komprehensif. Fokus pada konteks lokal yang relevan.	Keterbatasan jumlah responden (hanya 10 orang) dapat mempengaruhi validitas hasil. Hasil mungkin tidak	Penelitian ini relevan dengan penelitian saya karena membahas tata kelola I&T di sektor publik dan menggunakan COBIT 2019.

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
		Scorecard (Studi pada Dinas Komunikasi, Informatika, Persandian, dan Statistik Kabupaten Kolaka Timur)			Rekomendasi untuk peningkatan tata kelola I&T.		dapat digenerasi.	
20	Amir Bagja, Zaenul Amri, Khairul Imtihan, Muhammad Rodi, Siska Yuni Rusniatun	<i>Enhancing Public Sector IT governance through COBIT 2019: A Case Study on Service Continuity and Data Management in</i>	Untuk mengevaluasi maturitas tata kelola I&T di Satpol PP dan meningkatkan kontinuitas layanan serta keamanan data.	Studi kasus menggunakan COBIT 2019	Satpol PP beroperasi pada level 3 (Defined) dalam maturitas tata kelola I&T. <i>Gaps</i> dalam otomatisasi dan manajemen	Menyajikan studi kasus konkret yang relevan dengan penerapan COBIT 2019. Menekankan pentingnya keamanan data	Fokus yang terlalu sempit pada satu instansi dapat mengurangi relevansi temuan untuk organisasi lain.	Penelitian ini berkaitan dengan penelitian saya karena membahas penerapan COBIT 2019 dalam konteks pemerintahan

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
	(Bagja et al., 2024)	<i>the Central Lombok Amir</i>			risiko proaktif.			
21	Gugus Irianto, Mirna Amirya (Irianto & Amirya, 2024)	Kendala dan Strategi Implementasi Manajemen Risiko di Pemerintah Daerah Indonesia	Mengidentifikasi kendala dan strategi penerapan manajemen risiko di pemda	Studi kualitatif (analisis kebijakan dan wawancara)	Ketiadaan pemahaman teknis dan rendahnya komitmen pimpinan jadi penghambat utama	Relevan dengan kondisi pemda	Tidak menggunakan alat ukur kapabilitas proses	Penelitian ini mengkaji faktor internal pemerintah daerah yang menghambat penerapan manajemen risiko, seperti minimnya pemahaman teknis dan lemahnya peran pimpinan. Relevan karena Diskominfo juga merupakan bagian

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
								dari pemerintah daerah, dan peneliti sedang mengukur kapabilitas proses manajemen risiko di dalamnya. Temuan bisa memperkuat latar belakang dan alasan pentingnya pengukuran, bahwa belum banyak pemda yang melaksanakan manajemen risiko secara terstruktur.

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
22	Uky Yudatama, Dwi Ekasari Harmadji (Uky & Harmadji, 2022)	<i>IT Governance Awareness: A Proposed Formula for Assessment</i>	Menyusun formula penilaian kesadaran tata kelola I&T, termasuk manajemen risiko	Studi desain model berbasis survei	Tingkat kesadaran memengaruhi kesiapan instansi terhadap manajemen risiko I&T	Menyediakan kerangka pengukuran alternatif sederhana	Belum diuji pada instansi pemerintah secara spesifik	Artikel ini fokus pada kesadaran tata kelola I&T, termasuk komponen manajemen risiko di dalamnya. Meskipun tidak menggunakan COBIT, artikel ini menyajikan kerangka penilaian yang bisa dibandingkan atau dijadikan referensi alternatif pendekatan

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
								pengukuran kapabilitas. Memberi dasar bahwa kesadaran dan kesiapan internal instansi sangat memengaruhi hasil pengukuran, cocok untuk menjadi pembanding atau penguat dalam pembahasan hasil penelitian nanti.
23	Arianto Liwang, Nur Sayidah,	Strategi Penerapan Manajemen Risiko	Menganalisis penerapan ISO 31000 untuk meningkatkan	Studi kualitatif + studi kasus	ISO 31000 membantu menyusun langkah-	Menggunakan standar nasional,	Belum dilakukan pengukuran tingkat	Penelitian ini menggunakan <i>framework</i> non-COBIT (ISO

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
	Sri Utami Ady (Liwang et al., 2024)	Berbasis SNI ISO 31000:2018 di Pemda Kaimana	manajemen risiko instansi pemerintah		langkah risiko yang terstruktur dan berkelanjutan	cocok untuk instansi publik	kapabilitas secara eksplisit	31000) untuk penerapan manajemen risiko di instansi pemerintah daerah. Meskipun tidak mengukur kapabilitas, artikel ini menjelaskan proses dan langkah-langkah penerapan manajemen risiko secara sistematis, sehingga bisa menjadi pembanding

No	Nama Penulis & Tahun	Judul	Tujuan	Metode	Temuan	Kelebihan	Kelemahan	Relevansi Penelitian
								pendekatan dengan COBIT. Cocok sebagai dasar pembahasan: <i>kenapa COBIT 2019</i> dipilih, dan apa kekuatannya dibandingkan pendekatan lain seperti ISO 31000.

Lampiran 2. Dasar Pemilihan Domain EDM03 dan APO12

Pemilihan domain dalam penelitian ini dilakukan berdasarkan studi literatur terhadap 23 artikel ilmiah yang membahas implementasi COBIT 2019 maupun COBIT 5 dalam konteks tata kelola dan manajemen risiko I&T. Dari 23 artikel tersebut, sebanyak 18 artikel menggunakan *framework* COBIT secara eksplisit dan dijadikan dasar dalam pemilihan domain penelitian.

No	Penulis (Tahun)	Domain COBIT 2019	Proses Utama yang Dibahas	APO12	EDM03
1	(Oktaviana et al., 2024)	APO12, EDM03	Manajemen risiko I&T	✓	✓
2	(Solikhah et al., 2024)	APO12, BAI09	<i>Governance & risk</i>	✓	×
3	(Gamaliel et al., 2024)	APO12, EDM03	Audit risiko aplikasi sekolah	✓	✓
4	(Putra et al., 2023)	EDM05, APO07, APO11, APO13, APO14, BAI05, BAI08, DSS02, DSS03, DSS04, DSS05	Audit sistem realisasi anggaran dan risiko	×	×
5	(Simatupang & Fianty, 2023)	APO12, DSS01, DSS02	Risiko layanan I&T	✓	×
6	(Wattimury & Faza, 2023)	BAI04, BAI05, BAI11	Tata kelola I&T institusi pendidikan	×	×
7	(Kesuma et al., 2023)	MEA03, BAI04, EDM03	Audit dan evaluasi I&T pemerintah daerah	×	✓
8	(Windasari et al., 2022)	MEA, DSS	Audit kapabilitas I&T universitas	×	×
9	(MJ, 2021)	BAI11	Evaluasi	×	×

No	Penulis (Tahun)	Domain COBIT 2019	Proses Utama yang Dibahas	APO12	EDM03
			manajemen I&T Diskominfo Malang		
10	(Sutabri et al., 2024)	APO12, EDM03	Manajemen risiko <i>e-Gov</i>	✓	✓
11	(Gouwmalan & Tanaamah, 2023)	APO12, EDM03, BAI06, DSS05, MEA01	Evaluasi <i>framework</i> COBIT di koperasi	✓	✓
12	(Aditya et al., 2019)	Perbandingan COBIT 2019 dan <i>ITIL</i> V4	Perbandingan COBIT 2019 dan <i>ITIL</i> V4	✗	✗
13	(Elue, 2020)	Tidak eksplisit	<i>Best practice</i> kapabilitas COBIT	✗	✗
14	(Rafeq & Elangovan, 2021)	EDM03, APO12, APO13, BAI10, DSS04, DSS05	<i>Risk governance</i>	✓	✓
15	(Dwianto & Riadi, 2022)	EDM03 (COBIT 5)	Tata kelola risiko sistem medis (COBIT 5)	✗	✓
16	(Mustaqfirah et al., 2025)	EDM03, APO12, APO13, BAI10, DSS03, DSS05, MEA03, MEA04	Evaluasi tata kelola I&T Diskominfo	✓	✓
17	(Wulansari et al., 2022)	EDM03	Risiko <i>e-Gov</i> (COBIT 5)	✗	✓
18	(Assegaf et al., 2023)	BAI08, BAI10, APO07, BAI09, DSS04	Evaluasi peningkatan	✗	✗

No	Penulis (Tahun)	Domain COBIT 2019	Proses Utama yang Dibahas	APO12	EDM03
			kapabilitas I&T perpustakaan		
19	(Wahyudi et al., 2024)	APO02, APO03, BAI05, DSS06	Evaluasi peran tata kelola I&T berbasis kinerja organisasi	×	×
20	(Bagja et al., 2024)	Tidak disebut spesifik, tetapi terkait service continuity dan data management; fokus maturitas keseluruhan	Evaluasi maturitas tata kelola I&T dan manajemen risiko proaktif	×	×
21	(Irianto & Amirya, 2024)	Tidak menggunakan <i>framework</i> COBIT secara eksplisit	Kendala internal implementasi manajemen risiko di Pemda	×	×
22	(Uky & Harmadji, 2022)	Tidak menggunakan domain, namun menyusun formula kesadaran TIK	Evaluasi kesadaran tata kelola risiko I&T berbasis persepsi organisasi	×	×
23	(Liwang et al., 2024)	Tidak menggunakan <i>framework</i> COBIT	Strategi penguatan proses manajemen risiko di Pemda Kaimana	×	×

Domain APO12 digunakan dalam 8 artikel.

Domain EDM03 digunakan dalam 9 artikel.

Kombinasi APO12 dan EDM03 digunakan secara bersamaan dalam 6 artikel.

5 artikel tidak menggunakan domain COBIT secara spesifik dan tidak dijadikan dasar pemilihan domain. Selain berdasarkan studi literatur, pemilihan domain EDM03 dan APO12

juga mempertimbangkan kesesuaiannya dengan Permen PANRB Nomor 5 Tahun 2020 tentang Manajemen Risiko SPBE.

Kategori Proses SPBE	Langkah	Proses dalam COBIT 2019
Proses Inti	Penetapan Konteks Risiko	APO12.01 – Define Risk Management Strategy
	Identifikasi Risiko	APO12.02 – Identify Risk
	Analisis Risiko	APO12.03 – Analyze Risk
	Evaluasi Risiko	APO12.04 – Respond to Risk
	Penanganan Risiko	APO12.04 – Respond to Risk (lanjutan)
Proses Pendukung	Komunikasi & Konsultasi	APO12.05 – Articulate Risk EDM03.01 – Evaluate Risk Management
	Pemantauan & Review	APO12.06 – Monitor Risk EDM03.03 – Monitor Risk Management
	Pencatatan & Pelaporan	APO12.05 – Articulate Risk EDM03.02 – Direct Risk Management

Berdasarkan rekapitulasi studi literatur dan kesesuaian dengan regulasi nasional, domain EDM03 dan APO12 dipilih sebagai fokus evaluasi dalam penelitian ini.

Lampiran 3. Penilaian Jawaban Informan

Kategori Penilaian (NPLF)	Definisi Umum	Kriteria Penentuan	Alasan/Justifikasi
Fully Achieved (F)	Aktivitas dilaksanakan sepenuhnya sesuai deskripsi COBIT 2019 dan didukung bukti dokumen lengkap.	Informan menjelaskan bahwa seluruh aktivitas dilakukan secara rutin dan terdokumentasi. Terdapat bukti tertulis (SOP, laporan, notulen, kebijakan, formulir, atau <i>risk register</i>) yang sesuai dan terbaru.	Dinyatakan F karena aktivitas terbukti berjalan sesuai COBIT 2019 dan memiliki dukungan dokumen lengkap.
Largely Achieved (L)	Aktivitas hampir seluruhnya dilaksanakan, tetapi masih terdapat kekurangan minor.	Praktik sudah berjalan, tetapi sebagian belum terdokumentasi secara formal atau bukti masih terbatas. Beberapa elemen COBIT (misalnya monitoring atau pelaporan) belum sepenuhnya dijalankan.	Dinyatakan L karena aktivitas sudah dilaksanakan secara substansial, namun bukti dokumentasi belum lengkap atau konsisten.
Partially	Aktivitas telah	Praktik dilakukan	Dinyatakan P karena

Kategori Penilaian (NPLF)	Definisi Umum	Kriteria Penentuan	Alasan/Justifikasi
<i>Achieved</i> (P)	dimulai, namun baru sebagian kecil indikator yang terpenuhi.	secara tidak rutin atau hanya pada situasi tertentu. Bukti dokumen tidak mendukung seluruh aspek aktivitas. Pengetahuan pelaksana belum merata.	aktivitas sudah ada, tetapi tidak konsisten, tidak formal, atau minim dukungan bukti.
<i>Not Achieved</i> (N)	Aktivitas belum dilaksanakan sama sekali atau tidak ada bukti pendukung.	Informan menyatakan aktivitas belum pernah dilakukan. Tidak ada dokumen, SOP, laporan, atau catatan yang relevan.	Dinyatakan N karena tidak ada bukti pelaksanaan ataupun indikasi aktivitas sesuai COBIT 2019.

Catatan Tambahan

1. Penilaian ini digunakan setelah FGD dan klarifikasi dokumen dilakukan.
2. Jika selama FGD informan menyebut adanya dokumen tetapi belum sempat diverifikasi, aktivitas dicatat sementara dan ditentukan nilai akhirnya setelah dokumen diverifikasi melalui studi dokumentasi.
3. Rubrik lengkap ini digunakan sebelum data diinput ke COBIT 2019 *Capability Level Assessment Tool*.

Lampiran 4. Hasil Uji Instrumen FGD dengan Validator Pertama

Form Uji Validasi Oleh Ahli Dalam Rangka Penelitian Skripsi

Nama Mahasiswa	: Ketut Ananda Dharmawati
NIM	: 2215091035
Judul Skripsi:	: Pengukuran Kapabilitas Manajemen Risiko Informasi dan Teknologi (I&T) pada Dinas Komunikasi dan Informatika Kabupaten Klungkung Menggunakan <i>Framework</i> COBIT 2019.
Tujuan Uji	: Untuk memastikan bahwa butir-butir pertanyaan dalam instrumen FGD: 1. Sudah sesuai dan mewakili indikator aktivitas dalam domain EDM03 dan APO12 pada <i>framework</i> COBIT 2019. 2. Memiliki relevansi dan kejelasan makna sesuai konteks penelitian di lingkungan instansi pemerintah, khususnya Diskominfo Klungkung. 3. Dapat mengukur kemampuan manajemen risiko I&T secara konsisten dan objektif, tanpa menimbulkan tafsir ganda bagi informan maupun peneliti. 4. Layak digunakan sebagai alat pengumpulan data melalui FGD, setelah dilakukan telaah oleh ahli di bidang tata kelola I&T (COBIT 2019).

INSTRUMEN FGD

Tujuan						
Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.			Memastikan bahwa risiko perusahaan yang terkait dengan I&T tidak melebihi selera risiko dan toleransi risiko perusahaan, dampak risiko I&T terhadap nilai perusahaan diidentifikasi dan dikelola, dan potensi kegagalan kepatuhan diminimalkan.			
EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
EDM03.01 Evaluate risk management (Mengevaluasi manajemen risiko).						
1	Understand the organization and its context related to I&T risk.	Memahami organisasi dan konteksnya terkait dengan risiko I&T.	1. Apakah organisasi memiliki dokumen yang menggambarkan risiko I&T dalam konteks pelayanan publik (misalnya Renstra Diskominfo atau Masterplan TI)? Policies: aturan tertulis, rencana strategis. 2. Bagaimana pimpinan mengidentifikasi faktor eksternal (peraturan pemerintah, ancaman siber nasional) yang dapat memengaruhi risiko I&T? Processes: prosedur evaluasi eksternal. 3. Apakah ada forum khusus untuk membahas faktor	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			internal yang menambah risiko I&T (misalnya keterbatasan SDM, anggaran, atau infrastruktur)? <i>Organizational Structures</i>: siapa yang ikut forum (Kepala Dinas, Bidang Telematika). 4. Bagaimana risiko I&T dipetakan terhadap layanan publik yang dikelola Diskominfo (contoh: <i>e-government</i>, data kependudukan)? <i>Processes</i>: cara organisasi memetakan risiko. 5. Apakah hasil identifikasi konteks risiko I&T biasanya didokumentasikan? <i>Information Items</i>: notulen rapat, <i>risk register</i>. 6. Bagaimana budaya pimpinan/staf dalam membicarakan risiko I&T, terbuka, formal, atau cenderung memiliki kecenderungan menutupi masalah? <i>Culture & Behavior</i>: kebiasaan staf/pimpinan.			
2	<i>Determine the risk appetite of the organization, i.e., the level of I&T-related</i>	Menentukan selera risiko organisasi, yaitu tingkat risiko terkait I&T yang tersedia	1. Apakah organisasi memiliki pernyataan formal tentang tingkat risiko I&T yang masih bisa ditoleransi? <i>Policies</i>: dokumen <i>risk appetite statement</i>, SK, kebijakan risiko.	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>risk that the enterprise is willing to take in its pursuit of enterprise objectives.</i>	diambil perusahaan dalam mengejar tujuan perusahaan.	2. Siapa yang berwenang menentukan <i>risk appetite</i> organisasi? <i>Organizational Structures (RACI)</i>: Kepala Dinas, Sekda, atau komite. 3. Apakah <i>risk appetite</i> berbeda untuk tiap bidang (contoh: keamanan data vs layanan jaringan)? <i>Processes</i>: cara organisasi menetapkan <i>risk appetite</i> berbeda. 4. Bagaimana <i>risk appetite</i> dikaitkan dengan tujuan strategis Diskominfo (misalnya digitalisasi layanan publik)? <i>Information Items</i>: strategi TI, KPI organisasi. 5. Apakah <i>risk appetite</i> pernah direvisi/ditinjau ulang secara berkala? <i>Processes</i>: siklus review. 6. Bagaimana pimpinan menyampaikan <i>risk appetite</i> kepada staf teknis? <i>Information Flows</i>: rapat, edaran, sosialisasi. 7. Apakah ada contoh nyata risiko yang dianggap			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			“masih bisa diterima”? <i>Culture & Behavior</i>: contoh sikap pimpinan/staf.			
3	<i>Determine risk tolerance levels against the risk appetite, i.e., temporarily acceptable deviations from the risk appetite.</i>	Menentukan tingkat toleransi risiko terhadap selera risiko, yaitu penyimpangan yang dapat diterima sementara dari selera risiko.	1. Apakah organisasi memiliki standar formal terkait toleransi risiko (misalnya <i>downtime server</i> maksimal 30 menit)? <i>Policies</i>: SLA, SOP. 2. Bagaimana proses penetapan batas toleransi risiko dilakukan? <i>Processes</i>: prosedur penetapan toleransi. 3. Apakah toleransi berbeda antara sistem kritis (contoh: data kependudukan) dan sistem pendukung (contoh: website informasi)? <i>Information Items</i>: dokumen SLA/kontrak. 4. Siapa yang memutuskan kapan suatu risiko sudah melampaui toleransi dan harus diekskalasi? <i>Organizational Structures (RACI)</i>: pejabat yang berwenang. 5. Bagaimana toleransi risiko dikomunikasikan ke staf operasional?	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Information Flows</i>: SOP, pelatihan, <i>briefing</i>. 6. Apakah pernah terjadi pelanggaran batas toleransi risiko? Bagaimana tindak lanjutnya? <i>Processes</i>: tindakan korektif. 7. Apakah toleransi risiko dipengaruhi oleh regulasi eksternal (misalnya standar keamanan nasional)? <i>Culture & Behavior</i>: kesadaran staf terhadap aturan luar. 8. Bagaimana organisasi membedakan toleransi jangka pendek (sementara) dengan <i>risk appetite</i> jangka panjang? <i>Processes</i>: mekanisme pembedaan.			
4	<i>Determine the extent of alignment of the I&T risk strategy to the enterprise risk strategy and ensure the risk appetite is below the organization's risk capacity.</i>	Menentukan tingkat keselarasan strategi risiko I&T dengan strategi risiko perusahaan dan memastikan selera risiko berada di bawah kapasitas risiko	1. Apakah strategi risiko I&T pernah dibandingkan atau diselaraskan dengan strategi risiko organisasi secara keseluruhan? <i>Processes</i>: mekanisme evaluasi strategi. 2. Siapa yang bertanggung jawab memastikan keselarasan ini? <i>Organizational Structures (RACI)</i>: Kepala Dinas, Komite Risiko.	✓		Jika pakai I&T, semua I&T jika pakai TI semua TI (agar konsisten). Dalam bahasa Indonesia istilah I&T belum populer sehingga masih

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
		organisasi.	3. Apakah ada dokumen yang menunjukkan integrasi antara strategi risiko I&T dan strategi risiko organisasi? <i>Information Items: risk strategy document, Renstra, laporan risiko.</i> 4. Bagaimana pimpinan memastikan bahwa <i>risk appetite</i> TI tidak melebihi kapasitas risiko organisasi? <i>Policies: prinsip atau batas resmi dalam dokumen.</i> 5. Apakah ada forum lintas unit (TI dan non-TI) untuk meninjau keselarasan strategi risiko? <i>Organizational Structures: kolaborasi antar-unit.</i> 6. Apakah ada contoh keputusan strategis yang memperlihatkan keterkaitan langsung antara risiko I&T dan strategi organisasi? <i>Culture & Behavior: kesadaran pimpinan.</i>			sering diterjemahkan TI. Namun jika ingin menggunakan I&T (Informasi dan Teknologi) akan lebih baik.
5	<i>Proactively evaluate I&T risk factors in advance of pending strategic enterprise decisions and ensure</i>	Mengevaluasi faktor risiko I&T secara proaktif sebelum mengambil keputusan strategis perusahaan dan	1. Apakah organisasi selalu menilai risiko I&T sebelum mengambil keputusan strategis (misalnya terkait digitalisasi layanan)? <i>Processes: risk assessment</i> pra-keputusan. 2. Siapa yang wajib memberikan masukan risiko I&T	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>that risk considerations are part of the strategic enterprise decision process.</i>	memastikan bahwa pertimbangan risiko menjadi bagian dari proses pengambilan keputusan strategis perusahaan.	dalam rapat pengambilan keputusan strategis? <i>Organizational Structures (RACI)</i>: Kepala Dinas, Bidang Telematika. 3. Apakah ada prosedur baku yang mengatur penyampaian risiko I&T sebelum keputusan dibuat? <i>Policies</i>: SOP, aturan rapat. 4. Bagaimana informasi risiko I&T disampaikan ke pimpinan sebelum keputusan? <i>Information Flows</i>: notulen, laporan, presentasi. 5. Apakah faktor risiko I&T selalu menjadi agenda dalam rapat pimpinan strategis? <i>Policies</i>: tata tertib rapat. 6. Bagaimana pimpinan merespons masukan risiko I&T dalam rapat? <i>Culture & Behavior</i>: sikap pimpinan terhadap masukan risiko. 7. Apakah ada kasus nyata di mana keputusan strategis berubah karena pertimbangan risiko I&T? <i>Processes</i>: bukti integrasi risiko ke pengambilan			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			keputusan. 8. Apakah hasil evaluasi risiko I&T terdokumentasi sebagai bahan pembelajaran untuk keputusan berikutnya? <i>Information Items:</i> laporan evaluasi, lessons learned.			
6	<i>Evaluate risk management activities to ensure alignment with the enterprise's capacity for I&T-related loss and leadership's tolerance of it.</i>	Mengevaluasi aktivitas manajemen risiko untuk memastikan keselarasan dengan kapasitas perusahaan terhadap kerugian terkait I&T dan toleransi pimpinan terhadap kerugian tersebut.	1. Apakah ada evaluasi formal terhadap kegiatan manajemen risiko I&T? <i>Processes:</i> audit internal, review tahunan. 2. Bagaimana organisasi memastikan kegiatan manajemen risiko sesuai kapasitas keuangan atau sumber daya? <i>Policies:</i> batas anggaran, pedoman alokasi SDM. 3. Apakah pimpinan menetapkan batas toleransi kerugian terkait TI (misalnya <i>downtime</i> maksimal, batas kehilangan data)? <i>Organizational Structures (RACI):</i> pimpinan, dewan. 4. Bagaimana hasil evaluasi manajemen risiko I&T dilaporkan? <i>Information Items:</i> laporan risiko, hasil audit.			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			5. Apakah kegiatan manajemen risiko I&T pernah dikoreksi karena dianggap melampaui kapasitas organisasi? <i>Processes: corrective actions.</i> 6. Bagaimana sikap pimpinan terhadap hasil evaluasi yang menunjukkan potensi kerugian besar? <i>Culture & Behavior: penerimaan pimpinan atas risiko.</i> 7. Apakah ada mekanisme eskalasi jika aktivitas manajemen risiko I&T dinilai tidak sesuai kapasitas organisasi? <i>Information Flows: jalur eskalasi resmi.</i>			
7	Attract and maintain necessary skills and personnel for I&T Risk Management.	Menarik Merekrut dan mempertahankan keterampilan dan personel yang diperlukan untuk Manajemen Risiko I&T.	1. Apakah organisasi memiliki staf khusus yang menangani manajemen risiko I&T? <i>Organizational Structures (RACI):</i> posisi formal di struktur organisasi. 2. Bagaimana organisasi mengidentifikasi kebutuhan keterampilan staf untuk manajemen risiko I&T? <i>Processes:</i> analisis kebutuhan SDM. 3. Apakah tersedia program pelatihan internal maupun	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			eksternal atau sertifikasi khusus untuk staf terkait risiko I&T? <i>People, Skills & Competencies</i>: pelatihan, <i>workshop</i>. 4. Bagaimana organisasi memastikan staf baru memahami kebijakan manajemen risiko I&T? <i>Policies</i>: materi induksi/briefing. 5. Apakah ada program retensi untuk mempertahankan staf yang kompeten di bidang risiko I&T? <i>Culture & Behavior</i>: penghargaan, promosi. 6. Bagaimana organisasi mengatasi kekurangan staf berkompeten di bidang risiko I&T? <i>Processes</i>: strategi rekrutmen, outsourcing. 7. Apakah ada perencanaan jangka panjang untuk pengembangan kompetensi staf risiko I&T? <i>Policies</i>: dokumen HR, Renstra SDM. 8. Bagaimana organisasi memanfaatkan infrastruktur (contoh: <i>e-learning</i>, <i>platform</i> pelatihan <i>online</i>) untuk mendukung pengembangan staf? <i>Services & Infrastructure</i>: sistem pendukung pelatihan.			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			9. Apakah kompetensi staf di bidang risiko I&T pernah dievaluasi secara formal (misalnya melalui asesmen)? <i>People, Skills & Competencies</i> : uji kompetensi.			
EDM03.02 Direct risk management (Manajemen risiko langsung). (Mengarahkan manajemen risiko)						Terjemahan diperbaiki
8	Direct the translation and integration of the I&T risk strategy into risk management practices and operational activities.	Mengarahkan penerjemahan dan integrasi strategi risiko I&T ke dalam praktik manajemen risiko dan aktivitas operasional.	1. Apakah strategi risiko I&T yang dimiliki organisasi sudah diterjemahkan menjadi praktik operasional sehari-hari? <i>Processes</i> : bukti implementasi dalam SOP atau <i>workflow</i> . 2. Siapa yang bertanggung jawab memastikan strategi risiko I&T diintegrasikan ke kegiatan operasional? <i>Organizational Structures (RACI)</i> : Kepala Dinas, Bidang Telematika, tim manajemen risiko. 3. Apakah ada dokumen yang menjelaskan bagaimana strategi risiko I&T diturunkan ke tingkat operasional? <i>Information Items</i> : pedoman, manual kerja, SOP. 4. Bagaimana organisasi memastikan staf memahami strategi risiko I&T dalam pekerjaannya sehari-hari?	✓		Semua istilah asing dicetak miring

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Culture & Behavior</i>: komunikasi & sosialisasi. 5. Apakah ada rapat rutin untuk meninjau sejauh mana strategi risiko I&T dijalankan di level operasional? <i>Information Flows</i>: laporan rapat, notulen. 6. Apakah terdapat contoh nyata kegiatan operasional yang sudah menyesuaikan strategi risiko I&T? <i>Processes</i>: contoh implementasi. 7. Bagaimana organisasi mengukur efektivitas integrasi strategi risiko I&T ke operasional? <i>Policies</i>: indikator kinerja, KPI. 8. Apakah strategi risiko I&T pernah gagal diterapkan di lapangan? Jika ya, apa penyebabnya? <i>Processes</i>: evaluasi kegagalan.			
9	<i>Direct the development of risk communication plans (covering all levels of the enterprise).</i>	Memimpin Mengarahkan pengembangan rencana komunikasi risiko (mencakup semua tingkatan perusahaan).	1. Apakah organisasi memiliki rencana komunikasi risiko yang formal dan tertulis? <i>Policies</i>: dokumen komunikasi risiko. 2. Siapa yang bertanggung jawab mengembangkan rencana komunikasi risiko? <i>Organizational Structures (RACI)</i>: Bidang Telematika,	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			Sekretariat, pimpinan. 3. Bagaimana informasi risiko disampaikan ke level pimpinan, staf teknis, dan pemangku kepentingan eksternal? <i>Information Flows</i>: jalur komunikasi resmi. 4. Apakah ada perbedaan cara komunikasi risiko untuk level manajemen dan staf operasional? <i>Processes</i>: metode komunikasi berbeda. 5. Bagaimana budaya organisasi memengaruhi keterbukaan dalam komunikasi risiko? <i>Culture & Behavior</i>: keterbukaan vs tertutup. 6. Apakah ada pelatihan atau sosialisasi mengenai komunikasi risiko? <i>People, Skills & Competencies</i>: program pelatihan. 7. Bagaimana efektivitas komunikasi risiko dievaluasi? <i>Processes</i>: feedback, survei kepuasan komunikasi.			
10	<i>Direct implementation of the appropriate mechanisms to respond</i>	Mengarahkan penerapan langsung mekanisme yang tepat untuk	1. Apakah organisasi memiliki mekanisme resmi untuk merespons perubahan risiko I&T secara cepat? <i>Processes</i>: prosedur tanggap risiko.	✓		Semua istilah asing ditulis miring (Italic)

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>quickly to changing risk and report immediately to appropriate levels of management, supported by agreed principles of escalation (what to report, when, where and how).</i>	merespons perubahan risiko dengan cepat dan segera melaporkannya ke tingkat manajemen yang sesuai, didukung oleh prinsip-prinsip eskalasi yang disepakati (apa yang harus dilaporkan, kapan, di mana, dan bagaimana).	2. Bagaimana staf melaporkan risiko baru atau perubahan risiko yang muncul? <i>Information Flows</i>: jalur pelaporan resmi. 3. Siapa yang bertugas menerima dan menindaklanjuti laporan risiko baru? <i>Organizational Structures (RACI)</i>: pejabat pengelola risiko. 4. Apakah ada prinsip eskalasi yang jelas (apa yang dilaporkan, kapan, kepada siapa)? <i>Policies</i>: pedoman eskalasi. 5. Bagaimana organisasi memastikan laporan risiko segera sampai ke pimpinan terkait? <i>Processes</i>: mekanisme komunikasi cepat. 6. Apakah tersedia media khusus untuk laporan risiko darurat (misalnya <i>hotline</i>, aplikasi internal)? <i>Services & Infrastructure</i>: sistem pelaporan. 7. Apakah ada contoh kasus nyata di mana eskalasi risiko berhasil dilakukan dengan cepat? <i>Processes</i>: studi kasus.			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			8. Bagaimana pimpinan biasanya menanggapi laporan eskalasi risiko? <i>Culture & Behavior</i>: respons pimpinan. 9. Apakah efektivitas mekanisme eskalasi risiko pernah dievaluasi secara formal? <i>Information Items</i>: laporan evaluasi.			
11	<i>Direct that risk, opportunities, issues and concerns may be identified and reported by anyone to the appropriate party at any time. Risk should be managed in accordance with published policies and procedures and escalated to the relevant decision</i>	Pastikan Mengarahkan agar risiko, peluang, isu, dan kekhawatiran dapat diidentifikasi dan dilaporkan oleh siapa pun kepada pihak yang tepat kapan saja. Risiko harus dikelola sesuai dengan kebijakan dan prosedur yang dipublikasikan dan dieskalasikan kepada para pengambil	1. Apakah ada kebijakan yang memperbolehkan semua pegawai melaporkan risiko atau isu tanpa batasan hierarki? <i>Policies</i>: aturan open reporting. 2. Bagaimana staf biasanya menyampaikan risiko, peluang, atau isu yang mereka temukan? <i>Information Flows</i>: jalur komunikasi resmi maupun informal. 3. Siapa yang menerima laporan risiko dari staf? <i>Organizational Structures (RACI)</i>: pejabat penerima laporan. 4. Apakah laporan risiko bisa dilakukan secara anonim untuk menghindari hambatan budaya?	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>makers.</i>	keputusan yang relevan.	<i>Culture & Behavior:</i> keberanian/keterbukaan staf. 5. Apakah organisasi menyediakan media resmi untuk laporan terbuka (aplikasi, kotak saran, hotline)? <i>Services & Infrastructure:</i> sarana pelaporan. 6. Apakah ada prosedur bagaimana laporan staf ditindaklanjuti? <i>Processes:</i> alur tindak lanjut. 7. Apakah peluang yang dilaporkan staf juga dipertimbangkan sebagai masukan strategis? <i>Processes:</i> integrasi peluang ke strategi. 8. Apakah ada contoh nyata risiko/isu dari staf yang berhasil mencegah masalah besar di organisasi? <i>Information Items:</i> catatan kasus.			
12	<i>Identify key goals and metrics of the risk governance and management processes to be monitored, and approve the</i>	Mengidentifikasi tujuan dan metrik utama dari proses tata kelola dan manajemen risiko yang akan dipantau, dan menyetujui pendekatan,	1. Apakah organisasi memiliki tujuan utama yang jelas untuk tata kelola risiko I&T? <i>Policies:</i> dokumen tujuan risiko. 2. Bagaimana indikator keberhasilan manajemen risiko I&T ditentukan? <i>Processes:</i> penetapan KPI.	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>approaches, methods, techniques and processes for capturing and reporting the measurement information.</i>	metode, teknik, dan proses untuk menangkap dan melaporkan informasi pengukuran.	3. Siapa yang menyetujui metrik dan indikator risiko yang digunakan? <i>Organizational Structures (RACI)</i>: pimpinan, komite risiko. 4. Apakah ada metode formal untuk mengukur kinerja manajemen risiko? <i>Processes</i>: teknik pengukuran, audit. 5. Bagaimana informasi hasil pengukuran risiko disampaikan ke pimpinan? <i>Information Flows</i>: laporan kinerja. 6. Apakah organisasi menggunakan sistem/<i>tools</i> untuk mengumpulkan data metrik risiko? <i>Services & Infrastructure</i>: aplikasi monitoring. 7. Bagaimana pimpinan menilai apakah indikator risiko sesuai dengan tujuan strategis? <i>Culture & Behavior</i>: kesadaran pimpinan. 8. Apakah hasil <i>monitoring</i> indikator risiko terdokumentasi secara rutin? <i>Information Items</i>: laporan bulanan, tahunan.			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			9. Apakah metrik risiko pernah direvisi karena dianggap tidak relevan? <i>Processes</i> : siklus perbaikan metrik.			
EDM03.03 Monitor risk management (Memantau manajemen risiko).						
13	<i>Report any risk management issues to the board or executive committee.</i>	Melaporkan setiap masalah manajemen risiko kepada Dewan Komisaris atau komite eksekutif.	1. Apakah organisasi memiliki mekanisme resmi untuk melaporkan isu manajemen risiko ke pimpinan/komite eksekutif? <i>Policies</i>: aturan pelaporan risiko. 2. Siapa yang bertanggung jawab menyusun laporan isu manajemen risiko ke pimpinan? <i>Organizational Structures (RACI)</i>: Bidang Telematika, Kepala Dinas. 3. Bagaimana laporan isu manajemen risiko biasanya disampaikan? (tertulis, presentasi, rapat) <i>Information Flows</i>: media komunikasi. 4. Apakah laporan isu manajemen risiko terdokumentasi secara formal? <i>Information Items</i>: notulen, laporan resmi. 5. Bagaimana sikap pimpinan saat menerima laporan isu	✓		Jika menggunakan isu, semua isu. Jika menggunakan masalah, semua masalah (agar konsisten). Saran, sebaiknya menggunakan “permasalahan terkait manajemen risiko” untuk terjemahan <i>risk management issues</i>

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			manajemen risiko? <i>Culture & Behavior</i>: keseriusan pimpinan menindaklanjuti.			
14	<i>Monitor the extent to which the risk profile is managed within the enterprise's risk appetite and tolerance thresholds.</i>	Memantau sejauh mana profil risiko dikelola dalam selera risiko dan ambang batas toleransi perusahaan.	1. Apakah organisasi memantau apakah profil risiko I&T sesuai dengan <i>risk appetite</i> dan <i>tolerance</i> yang telah ditetapkan? <i>Processes</i>: mekanisme monitoring. 2. Siapa yang memantau kesesuaian profil risiko terhadap <i>risk appetite</i>? <i>Organizational Structures (RACI)</i>: pejabat <i>risk owner</i>. 3. Apakah ada sistem/<i>tools</i> yang digunakan untuk memantau profil risiko? <i>Services & Infrastructure</i>: aplikasi <i>monitoring</i>. 4. Bagaimana hasil pemantauan disampaikan ke pimpinan? <i>Information Flows</i>: laporan periodik. 5. Apakah profil risiko pernah melebihi batas <i>appetite</i> atau <i>tolerance</i>? <i>Information Items</i>: bukti laporan pelanggaran.	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			6. Bagaimana budaya organisasi ketika terjadi pelanggaran <i>risk appetite/tolerance</i>? <i>Culture & Behavior</i>: reaksi staf/pimpinan. 7. Apakah hasil monitoring digunakan untuk memperbarui strategi risiko I&T? <i>Processes</i>: siklus perbaikan.			
15	<i>Monitor key goals and metrics of risk governance and management processes against targets, analyze the cause of any deviations, and initiate remedial actions to address the underlying causes.</i>	Memantau tujuan dan metrik utama tata kelola risiko dan proses manajemen terhadap target, menganalisis penyebab penyimpangan, dan mengambil tindakan perbaikan untuk mengatasi penyebab yang mendasarinya.	1. Apakah organisasi memiliki target jelas untuk tujuan & dan metrik tata kelola risiko I&T? <i>Policies</i>: dokumen KPI risiko. 2. Bagaimana kinerja tata kelola risiko I&T dipantau dan dibandingkan terhadap terhadap target? <i>Processes</i>: metode <i>monitoring</i>. 3. Siapa yang melakukan analisis jika ada penyimpangan dari target? <i>Organizational Structures (RACI)</i>: unit analisis, pimpinan. 4. Apakah hasil monitoring metrik risiko terdokumentasi? <i>Information Items</i>: laporan kinerja risiko.	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			5. Apakah penyebab penyimpangan risiko biasanya dicatat dan dianalisis? <i>Processes: root cause analysis.</i> 6. Bagaimana budaya pimpinan saat membahas penyimpangan risiko? Apakah mencari solusi atau menyalahkan? <i>Culture & Behavior: sikap pimpinan.</i> 7. Apakah organisasi memiliki prosedur untuk tindakan korektif bila metrik risiko menyimpang jauh dari target? <i>Policies: pedoman tindakan korektif.</i> 8. Apakah remedial action pernah berhasil mengembalikan kinerja risiko ke target? <i>Processes: contoh nyata corrective action.</i>			
16	<i>Enable key stakeholders' review of the enterprise's progress toward identified goals.</i>	Memungkinkan peninjauan oleh pemangku kepentingan utama atas kemajuan perusahaan terhadap tujuan yang	1. Apakah pemangku kepentingan (internal maupun eksternal) dilibatkan dalam review peninjauan kemajuan pencapaian tujuan risiko I&T? <i>Organizational Structures (RACI): stakeholder utama.</i> 2. Apakah ada forum khusus untuk melakukan review peninjauan bersama pemangku kepentingan?	✓		Konsisten saja mau pakai review atau peninjauan. Saran, pakai peninjauan saja. Hal yang sama untuk

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
		diidentifikasi telah ditetapkan.	<i>Processes:</i> rapat evaluasi, forum koordinasi. 3. Bagaimana hasil review peninjauan <i>stakeholder</i> didokumentasikan? <i>Information Items:</i> notulen, laporan hasil review peninjauan . 4. Apakah masukan <i>stakeholder</i> digunakan untuk memperbaiki manajemen risiko I&T? <i>Processes:</i> siklus perbaikan. 5. Bagaimana budaya organisasi dalam menerima masukan dari <i>stakeholder</i>? <i>Culture & Behavior:</i> keterbukaan terhadap kritik. 6. Apakah organisasi menggunakan laporan khusus untuk menunjukkan progres kepada <i>stakeholder</i>? <i>Information Flows:</i> laporan publik, <i>dashboard</i>.			stakeholder. Mau pakai pemangku kepentingan atau stakeholder boleh asal konsisten.

Tujuan

<i>Integrate the management of I&T-related enterprise risk with overall enterprise risk management (ERM) and balance the costs and benefits of managing I&T-related enterprise risk.</i>	Integrasikan Mengintegrasikan pengelolaan risiko perusahaan terkait I&T dengan manajemen risiko perusahaan (ERM) secara keseluruhan dan seimbangkan biaya dan manfaat pengelolaan risiko perusahaan terkait I&T.
--	---

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
APO12.01 Collect data (Mengumpulkan data).						
1	Establish and maintain a method for the collection, classification and analysis of I&T risk-related data.	Menetapkan Membangun dan memelihara metode untuk pengumpulan, klasifikasi, dan analisis data terkait risiko I&T.	1. Apakah organisasi memiliki metode resmi untuk mengumpulkan dan menganalisis data risiko I&T? Policies: SOP atau pedoman resmi pengumpulan risiko 2. Apakah klasifikasi data risiko sudah ditetapkan (misalnya insiden keamanan, downtime, kesalahan manusia)? Processes: mekanisme klasifikasi risiko 3. Bagaimana prosedur memastikan data yang dikumpulkan valid dan konsisten? Processes: verifikasi data risiko 4. Apakah metode ini didokumentasikan dalam bentuk SOP atau pedoman resmi? Information Items: dokumen SOP, pedoman risiko	✓		
2	Record relevant and	Mencatat data risiko	1. Jenis data risiko I&T apa saja yang biasanya dicatat			

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>significant I&T risk-related data on the enterprise's internal and external operating environment.</i>	I&T yang relevan dan signifikan pada lingkungan operasi internal dan eksternal perusahaan.	(internal vs eksternal)? <i>Information Items:</i> risk log, laporan eksternal 2. Apakah ada format baku untuk pencatatan data risiko? <i>Policies:</i> format standar pencatatan risiko 3. Siapa yang biasanya mencatat data risiko I&T? <i>Organizational Structures:</i> staf Bidang Telematika / manajemen risiko 4. Bagaimana data eksternal (misalnya regulasi pemerintah, tren industri) ikut didokumentasikan? <i>Processes:</i> integrasi data eksternal ke pencatatan			
3	<i>Adopt or define a risk taxonomy for consistent definitions of risk scenarios and impact and likelihood categories.</i>	Mengadopsi atau menetapkan taksonomi risiko untuk definisi skenario risiko dan kategori dampak serta kemungkinan yang konsisten.	1. Apakah organisasi memiliki taksonomi risiko I&T (misalnya kategori dampak: finansial, reputasi, layanan publik)? <i>Policies:</i> dokumen taksonomi risiko 2. Apakah kategori risiko dan probabilitasnya konsisten dipakai semua bidang? <i>Processes:</i> penerapan klasifikasi risiko 3. Bagaimana taksonomi risiko ini dikomunikasikan kepada staf yang terlibat?	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Information Flows</i> : sosialisasi taksonomi risiko 4. Apakah pernah ada revisi/penyesuaian taksonomi risiko? <i>Culture & Behavior</i> : kesadaran untuk memperbarui taksonomi			
4	<i>Record data on risk events that have caused or may cause business impacts as per the impact categories defined in the risk taxonomy. Capture relevant data from related issues, incidents, problems and investigations.</i>	Mencatat data tentang peristiwa risiko yang telah menyebabkan atau mungkin menyebabkan dampak bisnis sesuai kategori dampak yang ditetapkan dalam taksonomi risiko. Menangkap data yang relevan dari isu, insiden, masalah, dan investigasi terkait.	1. Apakah insiden risiko I&T (<i>downtime</i> , serangan siber) selalu dicatat sesuai kategori dampak? <i>Processes</i> : pencatatan insiden sesuai kategori risiko 2. Apakah ada integrasi data dari laporan insiden, problem, atau investigasi? <i>Information Items</i> : laporan insiden, investigasi 3. Siapa yang bertanggung jawab memastikan pencatatan insiden sesuai kategori risiko? <i>Organizational Structures</i> : tim TI / manajemen risiko 4. Apakah catatan insiden digunakan untuk perbaikan layanan? <i>Processes</i> : <i>feedback loop</i> ke perbaikan layanan	✓		
5	<i>Survey and analyze the historical I&T risk</i>	Melakukan survei dan analisis data risiko I&T	1. Apakah organisasi menganalisis data risiko historis internal?	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>data and loss experience from externally available data and trends, industry peers through industry-based event logs, databases, and industry agreements for common event disclosure.</i>	historis dan pengalaman kerugian dari data dan tren yang tersedia secara eksternal, rekan industri melalui log peristiwa berbasis industri, basis data, dan perjanjian industri untuk pengungkapan peristiwa umum.	<i>Processes:</i> analisis data historis 2. Apakah data eksternal (tren industri, data asosiasi pemerintah/kominfo) juga digunakan? <i>Information Items:</i> laporan tren eksternal 3. Bagaimana data eksternal dibandingkan dengan kondisi internal organisasi? <i>Processes:</i> benchmarking internal-eksternal 4. Apakah ada contoh perbaikan kebijakan/teknis yang diambil dari analisis tren eksternal? <i>Culture & Behavior:</i> keterbukaan untuk belajar dari eksternal			
6	<i>For similar classes of events, organize the collected data and highlight contributing factors. Determine common contributing factors across multiple events.</i>	Untuk kelas kejadian yang serupa, menyusun data yang terkumpul dan soroti faktor-faktor yang berkontribusi. Tentukan faktor-faktor yang berkontribusi secara umum pada beberapa	1. Apakah organisasi mengelompokkan insiden serupa (misalnya serangan <i>malware</i> berulang)? <i>Processes:</i> klasifikasi insiden serupa 2. Faktor penyebab umum apa saja yang biasanya diidentifikasi? <i>Information Items:</i> catatan faktor penyebab 3. Apakah hasil analisis faktor penyebab digunakan untuk mencegah kejadian serupa?	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
		kejadian.	<i>Culture & Behavior</i> : kesadaran mencegah insiden berulang			
7	<i>Determine the specific conditions that existed or were absent when risk events occurred and the way the conditions affected event frequency and loss magnitude.</i>	Menentukan kondisi spesifik yang ada atau tidak ada saat peristiwa risiko terjadi dan cara kondisi tersebut memengaruhi frekuensi peristiwa dan besarnya kerugian.	1. Apakah kondisi tertentu (misalnya kurang staf, beban server tinggi) selalu dicatat saat insiden terjadi? <i>Processes</i> : pencatatan kondisi insiden 2. Bagaimana kondisi tersebut memengaruhi frekuensi kejadian/tingkat kerugian? <i>Information Items</i> : laporan analisis insiden 3. Apakah organisasi melakukan analisis <i>root cause</i> berbasis kondisi lingkungan/operasional? <i>Processes</i> : <i>root cause analysis</i> <i>Root cause</i> = penyebab paling mendasar suatu masalah/insiden, bukan sekadar gejala permukaan.	✓		
8	<i>Perform periodic event and risk factor analysis to identify new or emerging risk issues and to gain an understanding of the</i>	Melakukan analisis kejadian dan faktor risiko secara berkala untuk mengidentifikasi masalah risiko baru atau yang muncul dan untuk	1. Seberapa sering dilakukan analisis risiko I&T berkala? <i>Policies</i> : kebijakan <i>review</i> berkala 2. Siapa yang terlibat dalam analisis berkala ini? <i>Organizational Structures</i> : tim risk management Manajemen Risiko, Bidang Telematika	✓		Konsistem menggunakan rejemahan Manajemen Risiko

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>associated internal and external risk factors.</i>	memperoleh pemahaman tentang faktor risiko internal dan eksternal terkait.	3. Apakah hasil analisis digunakan untuk memperbarui daftar risiko organisasi? <i>Processes:</i> pembaruan daftar risiko 4. Apakah ada contoh risiko baru yang teridentifikasi dari analisis periodik (misalnya tren <i>ransomware</i>)? <i>Information Items:</i> laporan analisis risiko			
APO12.02 Analyze risk (Menganalisis risiko).						
9	<i>Define the appropriate scope of risk analysis efforts, considering all risk factors and/or the business criticality of assets.</i>	Menentukan cakupan upaya analisis risiko yang tepat, dengan mempertimbangkan semua faktor risiko dan/atau kekritisian aset dalam bisnis.	1. Bagaimana organisasi menentukan lingkup analisis risiko I&T (misalnya hanya pada aplikasi tertentu atau seluruh layanan publik)? <i>Processes:</i> prosedur penetapan lingkup analisis. 2. Siapa yang memutuskan ruang lingkup analisis risiko? <i>Organizational Structures (RACI):</i> Kepala Dinas, Bidang Telematika, Tim Manajemen Risiko. 3. Apakah ada kriteria formal untuk memilih aset mana yang dianggap kritis dalam analisis risiko? <i>Policies:</i> pedoman kritikalitas aset. 4. Bagaimana hasil penentuan lingkup analisis risiko didokumentasikan?	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Information Items: risk analysis scope document.</i>			
10	<i>Build and regularly update I&T risk scenarios; I&T-related loss exposures; and scenarios regarding reputational risk, including compound scenarios of cascading and/or coincidental threat types and events. Develop expectations for specific control activities and capabilities to detect.</i>	Menyusun dan memperbarui skenario risiko I&T secara berkala; paparan kerugian terkait I&T; dan skenario terkait risiko reputasi, termasuk skenario gabungan dari jenis dan peristiwa ancaman yang berjenjang dan/atau bersamaan. Mengembangkan ekspektasi untuk aktivitas dan kemampuan kontrol tertentu untuk mendeteksi.	1. Apakah organisasi memiliki daftar atau katalog skenario risiko I&T yang terdokumentasi? <i>Policies: dokumen risk scenario register.</i> Risk scenario = gambaran terstruktur tentang kemungkinan kejadian risiko, dampak, dan penyebabnya. 2. Seberapa sering skenario risiko diperbarui (tahunan, per proyek besar, setelah insiden)? <i>Processes: siklus update skenario.</i> 3. Apakah organisasi pernah menyusun skenario gabungan (contoh: serangan siber + kegagalan infrastruktur jaringan terjadi bersamaan)? <i>Processes: penyusunan skenario multi-event.</i> 4. Siapa yang terlibat dalam penyusunan dan pembaruan skenario risiko I&T? <i>Organizational Structures (RACI):</i> Bidang Telematika, Kepala Dinas, tim keamanan informasi. 5. Apakah ada metode standar dalam memperkirakan	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			dampak reputasi dari sebuah skenario risiko I&T? <i>Policies:</i> panduan analisis reputasi. 6. Bagaimana informasi dari insiden nyata sebelumnya dipakai untuk memperkaya skenario risiko baru? <i>Information Items:</i> catatan insiden, laporan audit. 7. Bagaimana organisasi menentukan kontrol apa saja yang harus tersedia untuk setiap skenario risiko? <i>Processes:</i> <i>mapping</i> skenario ke kontrol. Control = mekanisme/prosedur untuk mengurangi atau mendeteksi risiko. 8. Apakah pimpinan atau <i>stakeholder</i> pernah dilibatkan dalam validasi skenario risiko sebelum dipakai dalam analisis formal? <i>Culture & Behavior:</i> keterlibatan pimpinan, tingkat keseriusan validasi.			
11	<i>Estimate the frequency (or likelihood) and magnitude of loss or gain associated with</i>	Memperkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau	1. Bagaimana organisasi memperkirakan seberapa sering risiko I&T bisa terjadi? <i>Processes:</i> metode estimasi frekuensi. 2. Bagaimana memperkirakan besarnya kerugian (atau	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>I&T risk scenarios. Take into account all applicable risk factors and evaluate known operational controls.</i>	keuntungan yang terkait dengan skenario risiko I&T. Mempertimbangkan semua faktor risiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.	keuntungan) bila risiko terjadi? <i>Information Items:</i> data historis, perhitungan biaya. 3. Apakah faktor-faktor risiko eksternal (misalnya regulasi, tren siber) ikut dipertimbangkan? <i>Policies:</i> pedoman analisis risiko. 4. Bagaimana pengendalian yang ada dievaluasi saat memperkirakan dampak risiko? <i>Processes:</i> evaluasi kontrol.			
12	<i>Compare current risk (I&T-related loss exposure) to risk appetite and acceptable risk tolerance. Identify unacceptable or elevated risk.</i>	Membandingkan risiko saat ini (paparan kerugian terkait I&T) dengan selera risiko dan toleransi risiko yang dapat diterima. Mengidentifikasi risiko yang tidak dapat diterima atau tinggi.	1. Apakah organisasi pernah membandingkan profil risiko saat ini dengan <i>risk appetite</i> yang sudah ditetapkan? <i>Processes: risk profile vs appetite.</i> 2. Siapa yang berwenang menyatakan risiko melebihi batas <i>appetite/tolerance</i> ? <i>Organizational Structures (RACI):</i> pimpinan, komite risiko. 3. Apakah ada format laporan resmi untuk	✓		Deskripsi aktivitas bukan kata perintah melainkan kata kerja

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			menyampaikan risiko yang tidak dapat diterima? <i>Information Items:</i> laporan eksposur risiko. 4. Bagaimana pimpinan menindaklanjuti risiko yang melebihi toleransi? <i>Culture & Behavior:</i> reaksi pimpinan terhadap pelanggaran batas.			
13	<i>Propose risk responses for risk exceeding risk appetite and tolerance levels.</i>	Mengusulkan respons risiko untuk risiko yang melampaui selera risiko dan tingkat toleransi.	1. Bagaimana organisasi menentukan opsi respons (menghindari, mengurangi, transfer, menerima)? <i>Processes: risk response planning.</i> 2. Siapa yang berwenang mengusulkan atau memilih opsi respons risiko? <i>Organizational Structures (RACI):</i> pimpinan, tim manajemen risiko. 3. Apakah ada dokumen yang mencatat usulan respons risiko? <i>Information Items: risk response proposal.</i> 4. Bagaimana respons risiko disesuaikan dengan kebijakan organisasi?	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Policies</i> : pedoman respons risiko.			
14	<i>Specify high-level requirements for projects or programs that will implement the selected risk responses. Identify requirements and expectations for appropriate key controls for risk mitigation responses.</i>	Menetapkan persyaratan tingkat tinggi untuk proyek atau program yang akan menerapkan respons risiko yang dipilih. Identifikasi persyaratan dan harapan untuk kontrol utama yang sesuai untuk respons mitigasi risiko.	1. Bagaimana organisasi menentukan proyek/program untuk mengurangi risiko I&T? <i>Processes</i> : perencanaan proyek mitigasi. 2. Apakah ada dokumen resmi yang menjelaskan kebutuhan & harapan kontrol utama? <i>Information Items</i> : <i>project charter</i> , <i>TOR</i> , <i>Business Case</i> <i>Project Charter</i> = dokumen awal proyek yang memuat tujuan, scope, risiko, dan high-level requirement. <i>TOR (Terms of Reference)</i> = dokumen yang menjelaskan detail kebutuhan, ruang lingkup, dan harapan dari suatu program/proyek. Dokumen <i>Business Case</i> = justifikasi proyek, sering kali berisi requirement kontrol risiko. 3. Siapa yang menyetujui requirement mitigasi risiko I&T? <i>Organizational Structures (RACI)</i> : pimpinan proyek, Kepala Dinas. 4. Bagaimana requirement tersebut dikomunikasikan ke	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			tim pelaksana? <i>Information Flows</i> : rapat, dokumen tertulis.			
15	<i>Validate the risk analysis and business impact analysis (BIA) results before using them in decision making. Confirm that the analysis aligns with enterprise requirements and verify that estimations were properly calibrated and scrutinized for bias.</i>	Memvalidasi hasil analisis risiko dan analisis dampak bisnis (BIA) sebelum menggunakannya dalam pengambilan keputusan. Pastikan analisis tersebut sesuai dengan persyaratan perusahaan dan verifikasi bahwa estimasi telah dikalibrasi dengan benar dan diteliti untuk mengetahui biasnya.	1. Apakah hasil analisis risiko/BIA pernah diverifikasi ulang sebelum dipakai untuk keputusan? <i>Processes</i> : validasi analisis. BIA = analisis dampak bisnis, menilai seberapa parah dampak jika layanan terganggu. 2. Siapa yang melakukan validasi hasil analisis risiko? <i>Organizational Structures (RACI)</i> : tim independen, pimpinan. 3. Bagaimana memastikan hasil analisis bebas bias? <i>Policies</i> : prinsip validasi objektif. 4. Apakah ada bukti dokumentasi validasi (notulen, laporan)? <i>Information Items</i> : dokumen validasi.	✓		
16	<i>Analyze cost/benefit of potential risk response</i>	Menganalisis biaya/manfaat dari opsi	1. Apakah organisasi memiliki prosedur formal dalam membandingkan biaya dan manfaat dari berbagai opsi	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>options such as avoid, reduce/mitigate, transfer/share, and accept and exploit/seize. Confirm the optimal risk response.</i>	respons risiko potensial seperti menghindari, mengurangi/meringankan, mentransfer/membagi, dan menerima serta memanfaatkan/merebut. Mengonfirmasikan respons risiko yang optimal.	respons risiko? <i>Policies:</i> pedoman analisis <i>cost and benefit</i>. 2. Bagaimana cara organisasi menilai manfaat dari suatu respons risiko (misalnya pengurangan <i>downtime</i>, peningkatan kepercayaan publik)? <i>Processes:</i> metode analisis manfaat. 3. Apakah ada standar atau indikator keuangan yang digunakan dalam menghitung biaya (contoh: ROI, <i>payback period</i>)? <i>Information Items:</i> laporan keuangan, proyeksi biaya. 4. Siapa yang biasanya memutuskan opsi respons risiko yang dipilih (misalnya Kepala Dinas, komite risiko, atau bagian keuangan)? <i>Organizational Structures (RACI):</i> pengambil keputusan. 5. Bagaimana organisasi memastikan bahwa opsi respons risiko yang dipilih sesuai dengan <i>risk appetite</i> dan <i>tolerance</i> yang berlaku? <i>Processes:</i> alignment dengan <i>risk appetite</i>.			

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			6. Apakah organisasi pernah menggunakan pendekatan transfer risiko (misalnya asuransi, outsourcing) dan bagaimana analisis biayanya dibanding mitigasi internal? <i>Processes:</i> evaluasi opsi transfer. 7. Apakah budaya organisasi cenderung lebih memilih menghindari risiko (<i>risk averse</i>) atau berani mengambil risiko untuk peluang strategis (<i>risk seeking</i>)? <i>Culture & Behavior:</i> sikap organisasi terhadap risiko. 8. Apakah hasil analisis <i>cost/benefit</i> didokumentasikan dan dilaporkan secara formal untuk mendukung keputusan manajemen? <i>Information Flows:</i> laporan analisis risiko ke pimpinan.			
APO12.03 Maintain a risk profile (Pertahankan profil risiko). (Memelihara profile risiko)						
17	<i>Inventory business processes and document their dependency on I&T service management</i>	Menginventarisasi proses bisnis dan dokumentasikan ketergantungannya pada proses manajemen	1. Apakah organisasi memiliki inventaris proses bisnis yang terdokumentasi? <i>Information Items:</i> dokumen inventaris proses bisnis. 2. Bagaimana ketergantungan proses bisnis pada sistem TI dicatat?	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>processes and IT infrastructure resources. Identify supporting personnel, applications, infrastructure, facilities, critical manual records, vendors, suppliers and outsourcers.</i>	layanan I&T dan sumber daya infrastruktur I&T. Mengidentifikasi personel pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan pihak yang melakukan alih daya.	<i>Processes:</i> pemetaan <i>dependency</i> . 3. Apakah personel pendukung, aplikasi, infrastruktur, vendor juga dicatat dalam inventaris ini? <i>Policies:</i> aturan kelengkapan inventaris. 4. Siapa yang bertanggung jawab memelihara inventaris tersebut? <i>Organizational Structures (RACI):</i> Bidang Telematika, unit perencanaan.			
18	<i>Determine and agree on which I&T services and IT infrastructure resources are essential to sustain the operation of business processes. Analyze dependencies and identify weak links.</i>	Menentukan dan menyetujui layanan I&T dan sumber daya infrastruktur I&T mana yang penting untuk mempertahankan operasi proses bisnis. Menganalisis ketergantungan dan	1. Bagaimana organisasi menentukan layanan I&T mana yang sangat kritis untuk layanan publik? <i>Processes:</i> analisis layanan esensial. 2. Apakah ada dokumen resmi yang menyatakan layanan/infrastruktur esensial? <i>Information Items:</i> daftar layanan kritis, BCP. 3. Siapa yang menyetujui daftar layanan/infrastruktur esensial? <i>Organizational Structures (RACI):</i> pimpinan,	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
		mengidentifikasi titik lemah.	manajemen risiko. 4. Bagaimana titik lemah dalam ketergantungan layanan dianalisis? <i>Processes: weak link analysis.</i>			
19	<i>Aggregate current risk scenarios by category, business line and functional area.</i>	Mengumpulkan skenario risiko saat ini berdasarkan kategori, lini bisnis, dan area fungsional.	1. Apakah skenario risiko I&T pernah dikategorikan (contoh: operasional, keamanan data, layanan publik)? <i>Processes: risk categorization.</i> 2. Bagaimana skenario risiko dikonsolidasikan lintas unit? <i>Information Flows: laporan konsolidasi.</i> 3. Siapa yang menyetujui agregasi risiko lintas fungsi? <i>Organizational Structures (RACI): komite risiko, pimpinan.</i>	✓		
20	<i>Regularly capture all risk profile information and consolidate it into an aggregated risk profile.</i>	Secara berkala menangkap semua informasi profil risiko dan menggabungkannya menjadi profil risiko agregat.	1. Bagaimana organisasi menyatukan seluruh informasi risiko ke dalam profil risiko terkini? <i>Processes: konsolidasi profil risiko.</i> 2. Apakah ada sistem/ <i>tools</i> yang digunakan untuk mengelola profil risiko? <i>Services & Infrastructure: aplikasi GRC, spreadsheet,</i>	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			dsb. 3. Bagaimana hasil konsolidasi dibagikan ke <i>stakeholder</i> ? <i>Information Flows</i> : laporan <i>risk profile</i> .			
21	<i>Capture information on the status of the risk action plan for inclusion in the I&T risk profile of the enterprise.</i>	Menangkap informasi tentang status rencana tindakan risiko untuk dimasukkan dalam profil risiko I&T perusahaan.	1. Apakah setiap tindakan mitigasi risiko memiliki <i>action plan</i> resmi? <i>Policies</i> : pedoman penyusunan <i>action plan</i> . 2. Bagaimana status pelaksanaan <i>action plan</i> dipantau? <i>Processes</i> : monitoring rencana aksi. 3. Siapa yang bertanggung jawab melaporkan progres <i>action plan</i> ? <i>Organizational Structures (RACI)</i> : pemilik risiko, pimpinan unit.	✓		
22	<i>Based on all risk profile data, define a set of risk indicators that allow the quick identification and monitoring of current</i>	Berdasarkan semua data profil risiko, tentukan serangkaian indikator risiko yang memungkinkan identifikasi dan	1. Apakah organisasi memiliki indikator risiko utama (KRI) untuk memantau tren risiko? <i>Policies</i> : definisi KRI. 2. Bagaimana KRI ditentukan dari data profil risiko? <i>Processes</i> : metode penetapan indikator. 3. Apakah indikator risiko digunakan secara rutin dalam	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>risk and risk trends.</i>	pemantauan cepat risiko terkini dan tren risiko.	rapat pimpinan? <i>Information Items:</i> laporan KRI. 4. Siapa yang menyetujui indikator risiko sebelum digunakan? <i>Organizational Structures (RACI):</i> pimpinan, komite risiko. KRI (Key Risk Indicator) = indikator pengukuran kuantitatif atau kualitatif yang digunakan organisasi			
23	<i>Capture information on I&T risk events that have materialized for inclusion in the IT risk profile of the enterprise.</i>	Menangkap informasi tentang peristiwa risiko I&T yang telah terwujud untuk dimasukkan dalam profil risiko I&T perusahaan.	1. Apakah organisasi memiliki catatan formal untuk insiden atau peristiwa risiko I&T? <i>Information Items:</i> log insiden, laporan keamanan. 2. Bagaimana data insiden dikumpulkan (manual, sistem otomatis)? <i>Processes:</i> mekanisme pencatatan insiden. 3. Siapa yang bertanggung jawab melaporkan insiden risiko I&T? <i>Organizational Structures (RACI):</i> unit operasional, helpdesk TI.	✓		
APO12.04 Articulate risk (Risiko yang diartikulasikan). (Mengartikulasikan Risiko)						

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
24	<i>Report the results of risk analysis to all affected stakeholders in terms and formats useful to support enterprise decisions. Whenever possible, include probabilities and ranges of loss or gain along with confidence levels, to enable management to balance risk-return.</i>	Melaporkan hasil analisis risiko kepada semua pemangku kepentingan yang terpengaruh dalam bentuk dan format yang berguna untuk mendukung keputusan perusahaan. Jika memungkinkan, sertakan probabilitas dan rentang kerugian atau keuntungan beserta tingkat keyakinan, untuk memungkinkan manajemen menyeimbangkan risiko-imbal hasil.	1. Bagaimana hasil analisis risiko disampaikan ke stakeholder? <i>Information Flows</i> : laporan, dashboard. 2. Apakah laporan analisis risiko mencantumkan probabilitas dan range kerugian? <i>Information Items</i> : format laporan risiko. 3. Siapa yang meninjau laporan analisis risiko sebelum didistribusikan? <i>Organizational Structures (RACI)</i> : pimpinan, tim analisis.	✓		
25	<i>Provide decision</i>	Memberikan para	1. Bagaimana pengambil keputusan mendapat gambaran	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>makers with an understanding of worst-case and most-probable scenarios, I&T-related loss exposures and significant reputation, legal and regulatory considerations, or any other impact category as per the risk taxonomy.</i>	pengambil keputusan pemahaman tentang skenario terburuk dan paling mungkin, paparan kerugian terkait I&T, serta reputasi signifikan, pertimbangan hukum dan peraturan, atau kategori dampak lainnya sesuai taksonomi risiko.	skenario terburuk/terbaik dari risiko I&T? <i>Processes:</i> briefing risiko. 2. Apakah aspek reputasi, hukum, dan regulasi juga disampaikan dalam laporan risiko? <i>Policies:</i> pedoman laporan risiko. 3. Bagaimana kejelasan laporan disesuaikan dengan kebutuhan pimpinan? <i>Culture & Behavior:</i> komunikasi yang dipahami non-teknis.			
26	<i>Report the current risk profile to all stakeholders. Include information on the effectiveness of the risk management process, control effectiveness,</i>	Melaporkan profil risiko terkini kepada semua pemangku kepentingan. Sertakan informasi tentang efektivitas proses manajemen risiko, efektivitas	1. Apakah organisasi secara rutin melaporkan profil risiko terkini ke <i>stakeholder</i>? <i>Processes:</i> siklus pelaporan risiko. 2. Apa saja informasi yang disertakan (efektivitas kontrol, kesenjangan, status remediasi)? <i>Information Items:</i> laporan profil risiko. 3. Siapa yang menerima laporan profil risiko?	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>gaps, inconsistencies, redundancies, remediation status and their impacts on the risk profile.</i>	pengendalian, kesenjangan, inkonsistensi, redundansi, status perbaikan, dan dampaknya terhadap profil risiko.	<i>Organizational Structures (RACI): pimpinan, auditor, regulator.</i>			
27	<i>On a periodic basis, for areas with relative risk and risk capacity parity, identify I&T-related opportunities that would allow the acceptance of greater risk and enhanced growth and return.</i>	Secara berkala, untuk area dengan risiko relatif dan paritas kapasitas risiko, mengidentifikasi peluang terkait I&T yang akan memungkinkan penerimaan risiko lebih besar dan peningkatan pertumbuhan dan laba.	1. Apakah organisasi pernah mengidentifikasi peluang TI saat risiko relatif rendah? <i>Processes:</i> analisis peluang risiko. 2. Bagaimana peluang tersebut dievaluasi terhadap kapasitas risiko organisasi? <i>Policies:</i> pedoman evaluasi peluang. 3. Apakah ada contoh peluang TI yang dimanfaatkan untuk pertumbuhan? <i>Information Items:</i> studi kasus peluang.	✓		
28	<i>Review the results of objective third-party</i>	Meninjau hasil penilaian pihak ketiga yang	1. Apakah hasil audit eksternal/asesmen pihak ketiga dimasukkan ke dalam profil risiko?	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>assessments and internal audit and quality assurance reviews. Include them in the risk profile. Review identified gaps and I&T-related loss exposures to determine the need for additional risk analysis.</i>	objektif dan tinjauan audit internal serta jaminan kualitas. Sertakan hasil tersebut dalam profil risiko. Tinjau kesenjangan yang teridentifikasi dan paparan kerugian terkait I&T untuk menentukan perlunya analisis risiko tambahan.	<i>Processes: integrasi hasil audit.</i> 2. Bagaimana kesenjangan yang ditemukan ditindaklanjuti? <i>Processes: corrective action.</i> 3. Siapa yang meninjau hasil asesmen tersebut? <i>Organizational Structures (RACI): pimpinan, auditor internal.</i>			
APO12.05 Define a risk management action portfolio (Menentukan portofolio tindakan manajemen risiko)						
29	<i>Maintain an inventory of control activities that are in place to mitigate risk and that enable risk to be taken in line with the risk appetite and tolerance.</i>	Mengelola Memelihara inventaris aktivitas pengendalian yang ada untuk mengurangi risiko dan yang memungkinkan risiko ditangani sesuai dengan	1. Apakah organisasi memiliki daftar resmi kontrol mitigasi risiko? <i>Information Items: control inventory.</i> 2. Bagaimana kontrol diklasifikasikan dan dipetakan ke skenario risiko? <i>Processes: kontrol mapping.</i> 3. Siapa yang bertanggung jawab memperbarui	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>Classify control activities and map them to specific I&T risk scenarios and aggregations of I&T risk scenarios.</i>	selera dan toleransi risiko. Mengklasifikasikan aktivitas pengendalian dan memetakannya ke skenario risiko I&T tertentu dan agregasi skenario risiko I&T.	inventaris kontrol? <i>Organizational Structures (RACI)</i> : tim pengendalian internal, Bidang Telematika.			
30	<i>Determine whether each organizational entity monitors risk and accepts accountability for operating within its individual and portfolio tolerance levels.</i>	Menentukan apakah setiap entitas organisasi memantau risiko dan menerima akuntabilitas untuk beroperasi dalam tingkat toleransi individu dan portofolionya.	1. Apakah tiap unit organisasi diminta memantau risiko sendiri? <i>Policies</i> : aturan akuntabilitas risiko. 2. Bagaimana akuntabilitas risiko dibuktikan? <i>Information Items</i> : laporan risiko unit. 3. Siapa yang menilai apakah unit sudah sesuai toleransi? <i>Organizational Structures (RACI)</i> : manajemen risiko, pimpinan.	✓		
31	<i>Define a balanced set</i>	Menentukan	4. Bagaimana organisasi menilai proyek mitigasi risiko			

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>of project proposals designed to reduce risk and/or projects that enable strategic enterprise opportunities, considering costs, benefits, effect on current risk profile and regulations.</i>	serangkaian proposal proyek yang seimbang yang dirancang untuk mengurangi risiko dan/atau proyek yang memungkinkan peluang perusahaan strategis, dengan mempertimbangkan biaya, manfaat, dampak pada profil risiko dan peraturan saat ini.	vs proyek peluang? <i>Processes:</i> penilaian biaya-manfaat proyek. 5. Apakah biaya, manfaat, dan regulasi dijadikan pertimbangan formal? <i>Policies:</i> pedoman seleksi proyek. 6. Siapa yang memutuskan proposal proyek mana yang dijalankan? <i>Organizational Structures (RACI):</i> pimpinan, tim perencanaan.			
APO12.06 Respond to risk (Menanggapi risiko)						
32	<i>Prepare, maintain and test plans that document the specific steps to take when a risk event may cause a significant operational</i>	Menyiapkan, memelihara, dan menguji rencana yang mendokumentasikan langkah-langkah spesifik yang harus	1. Apakah organisasi memiliki dokumen rencana penanganan insiden risiko I&T yang formal? <i>Policies: disaster recovery plan (DRP), business continuity plan (BCP).</i> 2. Bagaimana rencana penanganan insiden tersebut disusun? Apakah ada prosedur baku?	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>or development incident with serious business impact. Ensure that plans include pathways of escalation across the enterprise.</i>	diambil ketika suatu peristiwa risiko dapat menyebabkan insiden operasional atau pengembangan yang signifikan dengan dampak bisnis yang serius. Pastikan bahwa rencana tersebut mencakup jalur eskalasi di seluruh perusahaan.	<i>Processes:</i> mekanisme penyusunan rencana. 3. Siapa yang terlibat dalam penyusunan dan pemeliharaan rencana ini? <i>Organizational Structures (RACI):</i> tim TI, pimpinan, manajemen risiko, pihak eksternal. 4. Apakah rencana ini secara berkala diuji melalui simulasi/drill? Jika ya, seberapa sering? <i>Processes:</i> uji coba dan review periodik. 5. Apakah tersedia jalur eskalasi resmi bila insiden signifikan terjadi (contoh: siapa yang dihubungi pertama, siapa yang memberi keputusan)? <i>Information Flows:</i> diagram eskalasi, SOP eskalasi. 6. Apakah ada sarana/infrastruktur khusus untuk mendukung eksekusi rencana (misalnya backup site, hotline darurat)? <i>Services & Infrastructure:</i> fasilitas pendukung. 7. Bagaimana budaya staf dan pimpinan dalam mengikuti simulasi atau uji coba rencana (serius, formalitas, atau kurang antusias)?			

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Culture & Behavior:</i> keterlibatan dalam simulasi. 8. Apakah hasil uji coba rencana (misalnya drill bencana TI) selalu didokumentasikan dan dipakai untuk perbaikan rencana berikutnya? <i>Information Items:</i> laporan hasil <i>drill</i> , <i>corrective action</i> .			
33	<i>Apply the appropriate response plan to minimize the impact when risk incidents occur.</i>	Menerapkan rencana respons yang tepat untuk meminimalkan dampak saat insiden risiko terjadi.	1. Apakah organisasi pernah benar-benar menerapkan rencana respons risiko I&T saat terjadi insiden besar (misalnya server <i>down</i> , kebocoran data)? <i>Information Items:</i> laporan insiden, catatan tindak lanjut. 2. Siapa yang biasanya mengambil keputusan utama ketika insiden risiko terjadi? <i>Organizational Structures (RACI):</i> Kepala Dinas, Bidang Telematika, tim tanggap darurat. 3. Bagaimana proses koordinasi antar-unit dilakukan saat rencana respons dijalankan? <i>Processes:</i> mekanisme koordinasi lintas unit. 4. Apakah tersedia sarana pendukung untuk memfasilitasi eksekusi respons (contoh: sistem	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			monitoring <i>real-time</i>, ruang kendali)? <i>Services & Infrastructure</i>: tools dan fasilitas darurat. 5. Bagaimana budaya staf saat menghadapi insiden – apakah tenang dan mengikuti prosedur, atau panik dan improvisasi? <i>Culture & Behavior</i>: reaksi nyata staf/pimpinan. 6. Apakah hasil penerapan rencana respons dievaluasi untuk memperbaiki SOP atau prosedur yang ada? <i>Processes</i>: siklus pembelajaran pasca-insiden.			
34	<i>Categorize incidents and compare I&T-related loss exposures against risk tolerance thresholds.</i> <i>Communicate business impacts to decision makers as part of reporting and update the risk profile.</i>	Mengategorikan insiden dan bandingkan paparan kerugian terkait I&T terhadap ambang batas toleransi risiko. Komunikasikan dampak bisnis kepada para pengambil keputusan sebagai bagian dari pelaporan dan perbarui	1. Apakah insiden TI (misalnya <i>downtime</i> aplikasi, serangan siber, kebocoran data) dikategorikan secara resmi menurut tingkat keparahan? <i>Policies</i>: SOP kategorisasi insiden. 2. Bagaimana organisasi menentukan apakah suatu insiden sudah melewati ambang batas toleransi risiko? <i>Processes</i>: mekanisme penilaian toleransi. 3. Siapa yang berwenang melakukan validasi kategori insiden dan memutuskan langkah eskalasi? <i>Organizational Structures (RACI)</i>: pejabat <i>risk owner</i>,	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
		profil risiko.	Kepala Dinas, tim TI. 4. Apakah hasil perbandingan insiden dengan toleransi risiko terdokumentasi dan masuk ke profil risiko organisasi? <i>Information Items:</i> risk register, laporan insiden. 5. Bagaimana dampak bisnis dari insiden TI dikomunikasikan kepada pengambil keputusan? <i>Information Flows:</i> laporan resmi, rapat pimpinan, dashboard. 6. Bagaimana budaya organisasi dalam menyikapi insiden yang melewati toleransi risiko, apakah terbuka membahasnya atau cenderung menutupinya? <i>Culture & Behavior:</i> keterbukaan pimpinan/staf.			
35	<i>Examine past adverse events/losses and missed opportunities and determine root causes.</i>	Memeriksa kejadian/kerugian buruk di masa lalu dan kesempatan yang hilang, serta menentukan akar penyebabnya.	1. Apakah organisasi memiliki catatan resmi terkait insiden atau kerugian TI di masa lalu (misalnya <i>downtime</i> panjang, kebocoran data, proyek TI gagal)? <i>Information Items:</i> laporan insiden, audit, <i>lessons learned</i>. 2. Bagaimana organisasi menganalisis akar penyebab	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			(<i>root cause</i>) dari insiden atau kerugian tersebut? <i>Processes</i>: metode <i>root cause analysis</i> (misalnya <i>fishbone</i>, <i>5-why</i>). 3. Siapa saja yang biasanya dilibatkan dalam proses investigasi akar penyebab insiden TI? <i>Organizational Structures (RACI)</i>: tim TI, manajemen risiko, pimpinan. 4. Apakah ada prosedur formal untuk melakukan evaluasi pasca-insiden (<i>post-mortem review</i>)? <i>Policies</i>: SOP evaluasi insiden. 5. Apakah faktor eksternal (regulasi, vendor, cuaca, tren industri) juga dipertimbangkan dalam analisis kerugian masa lalu? <i>Processes</i>: analisis faktor eksternal. 6. Bagaimana budaya organisasi dalam menyikapi insiden masa lalu, apakah terbuka mencari solusi atau cenderung menyalahkan pihak tertentu? <i>Culture & Behavior</i>: sikap staf/pimpinan. 7. Apakah hasil analisis insiden masa lalu digunakan			

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			sebagai bahan pembelajaran untuk memperbaiki kebijakan atau SOP? <i>Processes:</i> siklus perbaikan berkelanjutan.			
36	<i>Communicate root cause, additional risk response requirements and process improvements to appropriate decision makers. Ensure that the cause, response requirements and process improvement are included in risk governance processes.</i>	Mengomunikasikan akar permasalahan, persyaratan respons risiko tambahan, dan perbaikan proses kepada para pengambil keputusan yang tepat. Pastikan bahwa penyebab, persyaratan respons, dan perbaikan proses disertakan dalam proses tata kelola risiko.	1. Apakah hasil analisis akar penyebab (<i>root cause</i>) insiden TI secara rutin disampaikan ke pimpinan atau pengambil keputusan? <i>Information Flows:</i> laporan resmi, rapat evaluasi. 2. Bagaimana organisasi memastikan bahwa kebutuhan respons tambahan (misalnya kontrol baru, peningkatan keamanan) disampaikan dengan jelas kepada pengambil keputusan? <i>Processes:</i> mekanisme eskalasi kebutuhan respons. 3. Siapa yang bertanggung jawab mengomunikasikan hasil analisis akar penyebab dan rekomendasi perbaikan? <i>Organizational Structures (RACI):</i> manajemen risiko, Kepala Bidang Telematika, tim investigasi. 4. Apakah ada kebijakan formal yang mewajibkan penyampaian hasil analisis akar penyebab kepada level	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			manajemen tertentu? <i>Policies:</i> aturan eskalasi hasil investigasi. 5. Bagaimana budaya organisasi dalam menerima rekomendasi perbaikan, apakah proaktif untuk memperbaiki atau cenderung menunda? <i>Culture & Behavior:</i> sikap pimpinan dan staf. 6. Apakah hasil rekomendasi perbaikan biasanya diintegrasikan ke dalam kebijakan atau prosedur manajemen risiko? <i>Processes:</i> pembaruan SOP, kebijakan risiko. 7. Apakah organisasi pernah mengevaluasi efektivitas perbaikan proses setelah implementasi rekomendasi? <i>Information Items:</i> laporan evaluasi, hasil audit tindak lanjut.			

Keterangan:

R: Relevan

TR: Tidak Relevan

Hasil Validasi Uji Instrumen FGD Oleh Ahli
Dalam Rangka Penelitian Skripsi Pengukuran Kapabilitas Manajemen Risiko
Informasi dan Teknologi (I&T) pada Dinas Komunikasi dan Informatika Kabupaten
Klungkung Menggunakan *Framework* COBIT 2019

Data Penguji Ahli

Nama	: Ir. I Nyoman Sujana Saputra, S.T., M.TI., IPU.
Instansi	: PT. Tigatra Infokom
Jabatan	: Ahli COBIT 2019 – Sr. Manager Digital Transformation and I&T Solution
NIK	: 36201911089

Hasil Instrumen FGD

1. Detail pertanyaan secara umum sudah Relevan
2. Terjemahan pada Deskripsi Aktivitas bukan kata perintah, melainkan kata kerja (dengan imbuhan)
3. Konsistensi dalam menerjemahkan istilah seperti issue, review, stakeholder, serta penyeragaman antara istilah “TI” dan “I&T”.
4. Validator telah melakukan penyesuaian langsung (dengan font hijau) terhadap beberapa istilah agar lebih sesuai dengan terminologi COBIT 2019 dan konteks instansi pemerintah.
5. Pada saran sudah dituliskan masukan-masukan untuk perbaikan

Semarang, 18 Oktober 2025

Penguji Ahli,

Peneliti,

Ir. I Nyoman Sujana Saputra, S.T., M.TI., IPU.

Ketut Ananda Dharmawati

NIK. 36201911089

NIM 2215091035

Form Uji Validasi Oleh Ahli
Dalam Rangka Penelitian Skripsi

Nama Mahasiswa	: Ketut Ananda Dharmawati
NIM	: 2215091035
Judul Skripsi:	: Pengukuran Kapabilitas Manajemen Risiko Informasi dan Teknologi (I&T) pada Dinas Komunikasi dan Informatika Kabupaten Klungkung Menggunakan <i>Framework</i> COBIT 2019.
Tujuan Uji	: Untuk memastikan bahwa butir-butir pertanyaan dalam instrumen FGD: 1. Sudah sesuai dan mewakili indikator aktivitas dalam domain EDM03 dan APO12 pada <i>framework</i> COBIT 2019. 2. Memiliki relevansi dan kejelasan makna sesuai konteks penelitian di lingkungan instansi pemerintah, khususnya Diskominfo Klungkung. 3. Dapat mengukur kemampuan manajemen risiko I&T secara konsisten dan objektif, tanpa menimbulkan tafsir ganda bagi informan maupun peneliti. 4. Layak digunakan sebagai alat pengumpulan data melalui FGD, setelah dilakukan telaah oleh ahli di bidang tata kelola I&T (COBIT 2019).

INSTRUMEN FGD

Tujuan					
Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.			Memastikan bahwa risiko perusahaan yang terkait dengan I&T tidak melebihi selera risiko dan toleransi risiko perusahaan, dampak risiko I&T terhadap nilai perusahaan diidentifikasi dan dikelola, dan potensi kegagalan kepatuhan diminimalkan.		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
EDM03.01 Evaluate risk management (Mengevaluasi manajemen risiko).						
1	Understand the organization and its context related to I&T risk.	Memahami organisasi dan konteksnya terkait dengan risiko I&T.	1. Apakah organisasi memiliki dokumen yang menggambarkan risiko I&T dalam konteks pelayanan publik (misalnya Renstra Diskominfo atau Masterplan I&T)? Policies: aturan tertulis, rencana strategis. 2. Bagaimana pimpinan mengidentifikasi faktor eksternal (peraturan pemerintah, ancaman siber nasional) yang dapat memengaruhi risiko I&T? Processes: prosedur evaluasi eksternal. 3. Apakah ada forum khusus untuk membahas faktor	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			internal yang menambah risiko I&T (misalnya keterbatasan SDM, anggaran, atau infrastruktur)? <i>Organizational Structures</i>: siapa yang ikut forum (Kepala Dinas, Bidang Telematika). 4. Bagaimana risiko I&T dipetakan terhadap layanan publik yang dikelola Diskominfo (contoh: <i>e-government</i>, data kependudukan)? <i>Processes</i>: cara organisasi memetakan risiko. 5. Apakah hasil identifikasi konteks risiko I&T biasanya didokumentasikan? <i>Information Items</i>: notulen rapat, <i>risk register</i>. 6. Bagaimana budaya pimpinan/staf dalam membicarakan risiko I&T, terbuka, formal, atau memiliki kecenderungan menutupi masalah? <i>Culture & Behavior</i>: kebiasaan staf/pimpinan.			
2	<i>Determine the risk appetite of the organization, i.e., the level of I&T-related</i>	Menentukan selera risiko organisasi, yaitu tingkat risiko terkait I&T yang tersedia	1. Apakah organisasi memiliki pernyataan formal tentang tingkat risiko I&T yang masih bisa ditoleransi? <i>Policies</i>: dokumen <i>risk appetite statement</i>, SK, kebijakan risiko.	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>risk that the enterprise is willing to take in its pursuit of enterprise objectives.</i>	diambil perusahaan dalam mengejar tujuan perusahaan.	2. Siapa yang berwenang menentukan <i>risk appetite</i> organisasi? <i>Organizational Structures (RACI)</i>: Kepala Dinas, Sekda, atau komite. 3. Apakah <i>risk appetite</i> berbeda untuk tiap bidang (contoh: keamanan data vs layanan jaringan)? <i>Processes</i>: cara organisasi menetapkan <i>risk appetite</i> berbeda. 4. Bagaimana <i>risk appetite</i> dikaitkan dengan tujuan strategis Diskominfo (misalnya digitalisasi layanan publik)? <i>Information Items</i>: strategi TI, KPI organisasi. 5. Apakah <i>risk appetite</i> pernah direvisi/ditinjau ulang secara berkala? <i>Processes</i>: siklus review. 6. Bagaimana pimpinan menyampaikan <i>risk appetite</i> kepada staf teknis? <i>Information Flows</i>: rapat, edaran, sosialisasi. 7. Apakah ada contoh nyata risiko yang dianggap			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			“masih bisa diterima”? <i>Culture & Behavior</i>: contoh sikap pimpinan/staf.			
3	<i>Determine risk tolerance levels against the risk appetite, i.e., temporarily acceptable deviations from the risk appetite.</i>	Menentukan tingkat toleransi risiko terhadap selera risiko, yaitu penyimpangan yang dapat diterima sementara dari selera risiko.	1. Apakah organisasi memiliki standar formal terkait toleransi risiko (misalnya <i>downtime server</i> maksimal 30 menit)? <i>Policies</i>: SLA, SOP. 2. Bagaimana proses penetapan batas toleransi risiko dilakukan? <i>Processes</i>: prosedur penetapan toleransi. 3. Apakah toleransi berbeda antara sistem kritis (contoh: data kependudukan) dan sistem pendukung (contoh: website informasi)? <i>Information Items</i>: dokumen SLA/kontrak. 4. Siapa yang memutuskan kapan suatu risiko sudah melampaui toleransi dan harus diekskalasi? <i>Organizational Structures (RACI)</i>: pejabat yang berwenang. 5. Bagaimana toleransi risiko dikomunikasikan ke staf operasional?	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Information Flows</i>: SOP, pelatihan, <i>briefing</i>. 6. Apakah pernah terjadi pelanggaran batas toleransi risiko? Bagaimana tindak lanjutnya? <i>Processes</i>: tindakan korektif. 7. Apakah toleransi risiko dipengaruhi oleh regulasi eksternal (misalnya standar keamanan nasional)? <i>Culture & Behavior</i>: kesadaran staf terhadap aturan luar. 8. Bagaimana organisasi membedakan toleransi jangka pendek (sementara) dengan <i>risk appetite</i> jangka panjang? <i>Processes</i>: mekanisme perbedaan.			
4	<i>Determine the extent of alignment of the I&T risk strategy to the enterprise risk strategy and ensure the risk appetite is below the organization's risk capacity.</i>	Menentukan tingkat keselarasan strategi risiko I&T dengan strategi risiko perusahaan dan memastikan selera risiko berada di bawah kapasitas risiko	1. Apakah strategi risiko I&T pernah dibandingkan atau diselaraskan dengan strategi risiko organisasi secara keseluruhan? <i>Processes</i>: mekanisme evaluasi strategi. 2. Siapa yang bertanggung jawab memastikan keselarasan ini? <i>Organizational Structures (RACI)</i>: Kepala Dinas, Komite Risiko.	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
		organisasi.	3. Apakah ada dokumen yang menunjukkan integrasi antara strategi risiko I&T dan strategi risiko organisasi? <i>Information Items: risk strategy document, Renstra, laporan risiko.</i> 4. Bagaimana pimpinan memastikan bahwa <i>risk appetite</i> I&T tidak melebihi kapasitas risiko organisasi? <i>Policies: prinsip atau batas resmi dalam dokumen.</i> 5. Apakah ada forum lintas unit (I&T dan non-I&T) untuk meninjau keselarasan strategi risiko? <i>Organizational Structures: kolaborasi antar-unit.</i> 6. Apakah ada contoh keputusan strategis yang memperlihatkan keterkaitan langsung antara risiko I&T dan strategi organisasi? <i>Culture & Behavior: kesadaran pimpinan.</i>			
5	<i>Proactively evaluate I&T risk factors in advance of pending strategic enterprise decisions and ensure</i>	Mengevaluasi faktor risiko I&T secara proaktif sebelum mengambil keputusan strategis perusahaan dan	1. Apakah organisasi selalu menilai risiko I&T sebelum mengambil keputusan strategis (misalnya terkait digitalisasi layanan)? <i>Processes: risk assessment pra-keputusan.</i> 2. Siapa yang wajib memberikan masukan risiko I&T	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>that risk considerations are part of the strategic enterprise decision process.</i>	memastikan bahwa pertimbangan risiko menjadi bagian dari proses pengambilan keputusan strategis perusahaan.	dalam rapat pengambilan keputusan strategis? <i>Organizational Structures (RACI)</i>: Kepala Dinas, Bidang Telematika. 3. Apakah ada prosedur baku yang mengatur penyampaian risiko I&T sebelum keputusan dibuat? <i>Policies</i>: SOP, aturan rapat. 4. Bagaimana informasi risiko I&T disampaikan ke pimpinan sebelum keputusan? <i>Information Flows</i>: notulen, laporan, presentasi. 5. Apakah faktor risiko I&T selalu menjadi agenda dalam rapat pimpinan strategis? <i>Policies</i>: tata tertib rapat. 6. Bagaimana pimpinan merespons masukan risiko I&T dalam rapat? <i>Culture & Behavior</i>: sikap pimpinan terhadap masukan risiko. 7. Apakah ada kasus nyata di mana keputusan strategis berubah karena pertimbangan risiko I&T? <i>Processes</i>: bukti integrasi risiko ke pengambilan			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			keputusan. 8. Apakah hasil evaluasi risiko I&T terdokumentasi sebagai bahan pembelajaran untuk keputusan berikutnya? <i>Information Items:</i> laporan evaluasi, lessons learned.			
6	<i>Evaluate risk management activities to ensure alignment with the enterprise's capacity for I&T-related loss and leadership's tolerance of it.</i>	Mengevaluasi aktivitas manajemen risiko untuk memastikan keselarasan dengan kapasitas perusahaan terhadap kerugian terkait I&T dan toleransi pimpinan terhadap kerugian tersebut.	1. Apakah ada evaluasi formal terhadap kegiatan manajemen risiko I&T? <i>Processes:</i> audit internal, review tahunan. 2. Bagaimana organisasi memastikan kegiatan manajemen risiko sesuai kapasitas keuangan atau sumber daya? <i>Policies:</i> batas anggaran, pedoman alokasi SDM. 3. Apakah pimpinan menetapkan batas toleransi kerugian terkait I&T (misalnya <i>downtime</i> maksimal, batas kehilangan data)? <i>Organizational Structures (RACI):</i> pimpinan, dewan. 4. Bagaimana hasil evaluasi manajemen risiko I&T dilaporkan? <i>Information Items:</i> laporan risiko, hasil audit.			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			5. Apakah kegiatan manajemen risiko I&T pernah dikoreksi karena dianggap melampaui kapasitas organisasi? <i>Processes: corrective actions.</i> 6. Bagaimana sikap pimpinan terhadap hasil evaluasi yang menunjukkan potensi kerugian besar? <i>Culture & Behavior: penerimaan pimpinan atas risiko.</i> 7. Apakah ada mekanisme eskalasi jika aktivitas manajemen risiko I&T dinilai tidak sesuai kapasitas organisasi? <i>Information Flows: jalur eskalasi resmi.</i>			
7	<i>Attract and maintain necessary skills and personnel for I&T Risk Management.</i>	Merekrut dan mempertahankan keterampilan dan personel yang diperlukan untuk Manajemen Risiko I&T.	1. Apakah organisasi memiliki staf khusus yang menangani manajemen risiko I&T? <i>Organizational Structures (RACI):</i> posisi formal di struktur organisasi. 2. Bagaimana organisasi mengidentifikasi kebutuhan keterampilan staf untuk manajemen risiko I&T? <i>Processes: analisis kebutuhan SDM.</i> 3. Apakah tersedia program pelatihan internal maupun	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			eksternal atau sertifikasi khusus untuk staf terkait risiko I&T? <i>People, Skills & Competencies</i> : pelatihan, <i>workshop</i> . 4. Bagaimana organisasi memastikan staf baru memahami kebijakan manajemen risiko I&T? <i>Policies</i> : materi induksi/briefing. 5. Apakah ada program retensi untuk mempertahankan staf yang kompeten di bidang risiko I&T? <i>Culture & Behavior</i> : penghargaan, promosi. 6. Bagaimana organisasi mengatasi kekurangan staf berkompeten di bidang risiko I&T? <i>Processes</i> : strategi rekrutmen, outsourcing. 7. Apakah ada perencanaan jangka panjang untuk pengembangan kompetensi staf risiko I&T? <i>Policies</i> : dokumen HR, Renstra SDM. 8. Bagaimana organisasi memanfaatkan infrastruktur (contoh: <i>e-learning</i> , <i>platform</i> pelatihan <i>online</i>) untuk mendukung pengembangan staf? <i>Services & Infrastructure</i> : sistem pendukung pelatihan.			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			9. Apakah kompetensi staf di bidang risiko I&T pernah dievaluasi secara formal (misalnya melalui asesmen)? <i>People, Skills & Competencies</i> : uji kompetensi.			
EDM03.02 Direct risk management (Mengarahkan manajemen risiko).						
8	<i>Direct the translation and integration of the I&T risk strategy into risk management practices and operational activities.</i>	Mengarahkan penerjemahan dan integrasi strategi risiko I&T ke dalam praktik manajemen risiko dan aktivitas operasional.	1. Apakah strategi risiko I&T yang dimiliki organisasi sudah diterjemahkan menjadi praktik operasional sehari-hari? <i>Processes</i>: bukti implementasi dalam SOP atau <i>workflow</i>. 2. Siapa yang bertanggung jawab memastikan strategi risiko I&T diintegrasikan ke kegiatan operasional? <i>Organizational Structures (RACI)</i>: Kepala Dinas, Bidang Telematika, tim manajemen risiko. 3. Apakah ada dokumen yang menjelaskan bagaimana strategi risiko I&T diturunkan ke tingkat operasional? <i>Information Items</i>: pedoman, manual kerja, SOP. 4. Bagaimana organisasi memastikan staf memahami strategi risiko I&T dalam pekerjaannya sehari-hari? <i>Culture & Behavior</i>: komunikasi & sosialisasi.	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			5. Apakah ada rapat rutin untuk meninjau sejauh mana strategi risiko I&T dijalankan di <i>level</i> operasional? <i>Information Flows</i>: laporan rapat, notulen. 6. Apakah terdapat contoh nyata kegiatan operasional yang sudah menyesuaikan strategi risiko I&T? <i>Processes</i>: contoh implementasi. 7. Bagaimana organisasi mengukur efektivitas integrasi strategi risiko I&T ke operasional? <i>Policies</i>: indikator kinerja, KPI. 8. Apakah strategi risiko I&T pernah gagal diterapkan di lapangan? Jika ya, apa penyebabnya? <i>Processes</i>: evaluasi kegagalan.			
9	<i>Direct the development of risk communication plans (covering all levels of the enterprise).</i>	Mengarahkan pengembangan rencana komunikasi risiko (mencakup semua tingkatan perusahaan).	1. Apakah organisasi memiliki rencana komunikasi risiko yang formal dan tertulis? <i>Policies</i>: dokumen komunikasi risiko. 2. Siapa yang bertanggung jawab mengembangkan rencana komunikasi risiko? <i>Organizational Structures (RACI)</i>: Bidang Telematika, Sekretariat, pimpinan.	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			3. Bagaimana informasi risiko disampaikan ke level pimpinan, staf teknis, dan pemangku kepentingan eksternal? <i>Information Flows</i>: jalur komunikasi resmi. 4. Apakah ada perbedaan cara komunikasi risiko untuk level manajemen dan staf operasional? <i>Processes</i>: metode komunikasi berbeda. 5. Bagaimana budaya organisasi memengaruhi keterbukaan dalam komunikasi risiko? <i>Culture & Behavior</i>: keterbukaan vs tertutup. 6. Apakah ada pelatihan atau sosialisasi mengenai komunikasi risiko? <i>People, Skills & Competencies</i>: program pelatihan. 7. Bagaimana efektivitas komunikasi risiko dievaluasi? <i>Processes</i>: feedback, survei kepuasan komunikasi.			
10	<i>Direct implementation of the appropriate mechanisms to respond quickly to changing</i>	Mengarahkan penerapan mekanisme yang tepat untuk merespons perubahan risiko dengan	1. Apakah organisasi memiliki mekanisme resmi untuk merespons perubahan risiko I&T secara cepat? <i>Processes</i>: prosedur tanggap risiko. 2. Bagaimana staf melaporkan risiko baru atau	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>risk and report immediately to appropriate levels of management, supported by agreed principles of escalation (what to report, when, where and how).</i>	cepat dan segera melaporkannya ke tingkat manajemen yang sesuai, didukung oleh prinsip-prinsip eskalasi yang disepakati (apa yang harus dilaporkan, kapan, di mana, dan bagaimana).	perubahan risiko yang muncul? <i>Information Flows</i>: jalur pelaporan resmi. 3. Siapa yang bertugas menerima dan menindaklanjuti laporan risiko baru? <i>Organizational Structures (RACI)</i>: pejabat pengelola risiko. 4. Apakah ada prinsip eskalasi yang jelas (apa yang dilaporkan, kapan, kepada siapa)? <i>Policies</i>: pedoman eskalasi. 5. Bagaimana organisasi memastikan laporan risiko segera sampai ke pimpinan terkait? <i>Processes</i>: mekanisme komunikasi cepat. 6. Apakah tersedia media khusus untuk laporan risiko darurat (misalnya <i>hotline</i>, aplikasi <i>internal</i>)? <i>Services & Infrastructure</i>: sistem pelaporan. 7. Apakah ada contoh kasus nyata di mana eskalasi risiko berhasil dilakukan dengan cepat? <i>Processes</i>: studi kasus. 8. Bagaimana pimpinan biasanya menanggapi laporan			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			eskalasi risiko? <i>Culture & Behavior</i> : respons pimpinan. 9. Apakah efektivitas mekanisme eskalasi risiko pernah dievaluasi secara formal? <i>Information Items</i> : laporan evaluasi.			
11	<i>Direct that risk, opportunities, issues and concerns may be identified and reported by anyone to the appropriate party at any time. Risk should be managed in accordance with published policies and procedures and escalated to the relevant decision makers.</i>	Mengarahkan agar risiko, peluang, isu, dan kekhawatiran dapat diidentifikasi dan dilaporkan oleh siapa pun kepada pihak yang tepat kapan saja. Risiko harus dikelola sesuai dengan kebijakan dan prosedur yang dipublikasikan dan dieskalasikan kepada para pengambil keputusan yang relevan.	1. Apakah ada kebijakan yang memperbolehkan semua pegawai melaporkan risiko atau isu tanpa batasan hierarki? <i>Policies</i> : aturan open reporting. 2. Bagaimana staf biasanya menyampaikan risiko, peluang, atau isu yang mereka temukan? <i>Information Flows</i> : jalur komunikasi resmi maupun informal. 3. Siapa yang menerima laporan risiko dari staf? <i>Organizational Structures (RACI)</i> : pejabat penerima laporan. 4. Apakah laporan risiko bisa dilakukan secara anonim untuk menghindari hambatan budaya? <i>Culture & Behavior</i> : keberanian/keterbukaan staf.	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			5. Apakah organisasi menyediakan media resmi untuk laporan terbuka (aplikasi, kotak saran, hotline)? <i>Services & Infrastructure</i>: sarana pelaporan. 6. Apakah ada prosedur bagaimana laporan staf ditindaklanjuti? <i>Processes</i>: alur tindak lanjut. 7. Apakah peluang yang dilaporkan staf juga dipertimbangkan sebagai masukan strategis? <i>Processes</i>: integrasi peluang ke strategi. 8. Apakah ada contoh nyata risiko/isu dari staf yang berhasil mencegah masalah besar di organisasi? <i>Information Items</i>: catatan kasus.			
12	<i>Identify key goals and metrics of the risk governance and management processes to be monitored, and approve the approaches, methods,</i>	Mengidentifikasi tujuan dan metrik utama dari proses tata kelola dan manajemen risiko yang akan dipantau, dan menyetujui pendekatan, metode, teknik, dan	1. Apakah organisasi memiliki tujuan utama yang jelas untuk tata kelola risiko I&T? <i>Policies</i>: dokumen tujuan risiko. 2. Bagaimana indikator keberhasilan manajemen risiko I&T ditentukan? <i>Processes</i>: penetapan KPI. 3. Siapa yang menyetujui metrik dan indikator risiko	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>techniques and processes for capturing and reporting the measurement information.</i>	proses untuk menangkap dan melaporkan informasi pengukuran.	yang digunakan? <i>Organizational Structures (RACI)</i> : pimpinan, komite risiko. 4. Apakah ada metode formal untuk mengukur kinerja manajemen risiko? <i>Processes</i> : teknik pengukuran, audit. 5. Bagaimana informasi hasil pengukuran risiko disampaikan ke pimpinan? <i>Information Flows</i> : laporan kinerja. 6. Apakah organisasi menggunakan sistem/ <i>tools</i> untuk mengumpulkan data metrik risiko? <i>Services & Infrastructure</i> : aplikasi monitoring. 7. Bagaimana pimpinan menilai apakah indikator risiko sesuai dengan tujuan strategis? <i>Culture & Behavior</i> : kesadaran pimpinan. 8. Apakah hasil <i>monitoring</i> indikator risiko terdokumentasi secara rutin? <i>Information Items</i> : laporan bulanan, tahunan. 9. Apakah metrik risiko pernah direvisi karena dianggap			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			tidak relevan? <i>Processes</i> : siklus perbaikan metrik.			
EDM03.03 Monitor risk management (Memantau manajemen risiko).						
13	<i>Report any risk management issues to the board or executive committee.</i>	Melaporkan setiap permasalahan terkait manajemen risiko kepada Dewan Komisaris atau komite eksekutif.	1. Apakah organisasi memiliki mekanisme resmi untuk melaporkan masalah manajemen risiko ke pimpinan/komite eksekutif? <i>Policies</i> : aturan pelaporan risiko. 2. Siapa yang bertanggung jawab menyusun laporan masalah manajemen risiko ke pimpinan? <i>Organizational Structures (RACI)</i> : Bidang Telematika, Kepala Dinas. 3. Bagaimana laporan masalah manajemen risiko biasanya disampaikan? (tertulis, presentasi, rapat) <i>Information Flows</i> : media komunikasi. 4. Apakah laporan masalah manajemen risiko terdokumentasi secara formal? <i>Information Items</i> : notulen, laporan resmi. 5. Bagaimana sikap pimpinan saat menerima laporan masalah manajemen risiko?	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Culture & Behavior</i> : keseriusan pimpinan menindaklanjuti.			
14	<i>Monitor the extent to which the risk profile is managed within the enterprise's risk appetite and tolerance thresholds.</i>	Memantau sejauh mana profil risiko dikelola dalam selera risiko dan ambang batas toleransi perusahaan.	1. Apakah organisasi memantau apakah profil risiko I&T sesuai dengan <i>risk appetite</i> dan <i>tolerance</i> yang telah ditetapkan? <i>Processes</i>: mekanisme monitoring. 2. Siapa yang memantau kesesuaian profil risiko terhadap <i>risk appetite</i>? <i>Organizational Structures (RACI)</i>: pejabat <i>risk owner</i>. 3. Apakah ada sistem/tools yang digunakan untuk memantau profil risiko? <i>Services & Infrastructure</i>: aplikasi <i>monitoring</i>. 4. Bagaimana hasil pemantauan disampaikan ke pimpinan? <i>Information Flows</i>: laporan periodik. 5. Apakah profil risiko pernah melebihi batas <i>appetite</i> atau <i>tolerance</i>? <i>Information Items</i>: bukti laporan pelanggaran. 6. Bagaimana budaya organisasi ketika terjadi	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			pelanggaran <i>risk appetite/tolerance</i>? <i>Culture & Behavior</i>: reaksi staf/pimpinan. 7. Apakah hasil monitoring digunakan untuk memperbarui strategi risiko I&T? <i>Processes</i>: siklus perbaikan.			
15	<i>Monitor key goals and metrics of risk governance and management processes against targets, analyze the cause of any deviations, and initiate remedial actions to address the underlying causes.</i>	Memantau tujuan dan metrik utama tata kelola risiko dan proses manajemen terhadap target, menganalisis penyebab penyimpangan, dan mengambil tindakan perbaikan untuk mengatasi penyebab yang mendasarinya.	1. Apakah organisasi memiliki target jelas untuk tujuan dan metrik tata kelola risiko I&T? <i>Policies</i>: dokumen KPI risiko. 2. Bagaimana kinerja tata kelola risiko I&T dipantau dan dibandingkan terhadap target? <i>Processes</i>: metode <i>monitoring</i>. 3. Siapa yang melakukan analisis jika ada penyimpangan dari target? <i>Organizational Structures (RACI)</i>: unit analisis, pimpinan. 4. Apakah hasil monitoring metrik risiko terdokumentasi? <i>Information Items</i>: laporan kinerja risiko. 5. Apakah penyebab penyimpangan risiko biasanya	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			dicatat dan dianalisis? <i>Processes: root cause analysis.</i> 6. Bagaimana budaya pimpinan saat membahas penyimpangan risiko? Apakah mencari solusi atau menyalahkan? <i>Culture & Behavior: sikap pimpinan.</i> 7. Apakah organisasi memiliki prosedur untuk tindakan korektif bila metrik risiko menyimpang jauh dari target? <i>Policies: pedoman tindakan korektif.</i> 8. Apakah remedial action pernah berhasil mengembalikan kinerja risiko ke target? <i>Processes: contoh nyata corrective action.</i>			
16	<i>Enable key stakeholders' review of the enterprise's progress toward identified goals.</i>	Memungkinkan peninjauan oleh pemangku kepentingan utama atas kemajuan perusahaan terhadap tujuan yang telah ditetapkan.	1. Apakah pemangku kepentingan (internal maupun eksternal) dilibatkan dalam peninjauan kemajuan pencapaian tujuan risiko I&T? <i>Organizational Structures (RACI):</i> pemangku kepentingan utama. 2. Apakah ada forum khusus untuk melakukan peninjauan bersama pemangku kepentingan?	✓		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Processes:</i> rapat evaluasi, forum koordinasi. 3. Bagaimana hasil peninjauan pemangku kepentingan didokumentasikan? <i>Information Items:</i> notulen, laporan hasil peninjauan 4. Apakah masukan pemangku kepentingan digunakan untuk memperbaiki manajemen risiko I&T? <i>Processes:</i> siklus perbaikan. 5. Bagaimana budaya organisasi dalam menerima masukan dari pemangku kepentingan? <i>Culture & Behavior:</i> keterbukaan terhadap kritik. 6. Apakah organisasi menggunakan laporan khusus untuk menunjukkan progres kepada pemangku kepentingan? <i>Information Flows:</i> laporan publik, <i>dashboard</i>.			

Tujuan	
<i>Integrate the management of I&T-related enterprise risk with overall enterprise risk management (ERM) and balance the costs and benefits of managing I&T-related enterprise risk.</i>	Mengintegrasikan pengelolaan risiko perusahaan terkait I&T dengan manajemen risiko perusahaan (ERM) secara keseluruhan dan seimbangkan biaya dan manfaat pengelolaan risiko perusahaan terkait I&T.

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
APO12.01 Collect data (Mengumpulkan data).						
1	Establish and maintain a method for the collection, classification and analysis of I&T risk-related data.	Membangun dan memelihara metode untuk pengumpulan, klasifikasi, dan analisis data terkait risiko I&T.	1. Apakah organisasi memiliki metode resmi untuk mengumpulkan dan menganalisis data risiko I&T ? <i>Policies:</i> SOP atau pedoman resmi pengumpulan risiko 2. Apakah klasifikasi data risiko sudah ditetapkan (misalnya insiden keamanan, <i>downtime</i> , kesalahan manusia)? <i>Processes:</i> mekanisme klasifikasi risiko 3. Bagaimana prosedur memastikan data yang dikumpulkan valid dan konsisten? <i>Processes:</i> verifikasi data risiko 4. Apakah metode ini didokumentasikan dalam bentuk SOP atau pedoman resmi? <i>Information Items:</i> dokumen SOP, pedoman risiko	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
2	<i>Record relevant and significant I&T risk-related data on the enterprise's internal and external operating environment.</i>	Mencatat data risiko I&T yang relevan dan signifikan pada lingkungan operasi internal dan eksternal perusahaan.	1. Jenis data risiko I&T apa saja yang biasanya dicatat (internal vs eksternal)? <i>Information Items:</i> risk log, laporan eksternal 2. Apakah ada format baku untuk pencatatan data risiko? <i>Policies:</i> format standar pencatatan risiko 3. Siapa yang biasanya mencatat data risiko I&T? <i>Organizational Structures:</i> staf Bidang Telematika / manajemen risiko 4. Bagaimana data eksternal (misalnya regulasi pemerintah, tren industri) ikut didokumentasikan? <i>Processes:</i> integrasi data eksternal ke pencatatan			
3	<i>Adopt or define a risk taxonomy for consistent definitions of risk scenarios and impact and likelihood categories.</i>	Mengadopsi atau menetapkan taksonomi risiko untuk definisi skenario risiko dan kategori dampak serta kemungkinan yang konsisten.	1. Apakah organisasi memiliki taksonomi risiko I&T (misalnya kategori dampak: finansial, reputasi, layanan publik)? <i>Policies:</i> dokumen taksonomi risiko 2. Apakah kategori risiko dan probabilitasnya konsisten dipakai semua bidang? <i>Processes:</i> penerapan klasifikasi risiko 3. Bagaimana taksonomi risiko ini dikomunikasikan	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			kepada staf yang terlibat? <i>Information Flows</i> : sosialisasi taksonomi risiko 4. Apakah pernah ada revisi/penyesuaian taksonomi risiko? <i>Culture & Behavior</i> : kesadaran untuk memperbarui taksonomi			
4	<i>Record data on risk events that have caused or may cause business impacts as per the impact categories defined in the risk taxonomy. Capture relevant data from related issues, incidents, problems and investigations.</i>	Mencatat data tentang peristiwa risiko yang telah menyebabkan atau mungkin menyebabkan dampak bisnis sesuai kategori dampak yang ditetapkan dalam taksonomi risiko. Menangkap data yang relevan dari isu, insiden, masalah, dan investigasi terkait.	1. Apakah insiden risiko I&T (<i>downtime</i> , serangan siber) selalu dicatat sesuai kategori dampak? <i>Processes</i> : pencatatan insiden sesuai kategori risiko 2. Apakah ada integrasi data dari laporan insiden, problem, atau investigasi? <i>Information Items</i> : laporan insiden, investigasi 3. Siapa yang bertanggung jawab memastikan pencatatan insiden sesuai kategori risiko? <i>Organizational Structures</i> : tim TI / manajemen risiko 4. Apakah catatan insiden digunakan untuk perbaikan layanan? <i>Processes</i> : <i>feedback loop</i> ke perbaikan layanan	✓		
5	<i>Survey and analyze the</i>	Melakukan survei dan	1. Apakah organisasi menganalisis data risiko historis	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>historical I&T risk data and loss experience from externally available data and trends, industry peers through industry-based event logs, databases, and industry agreements for common event disclosure.</i>	analisis data risiko I&T historis dan pengalaman kerugian dari data dan tren yang tersedia secara eksternal, rekan industri melalui log peristiwa berbasis industri, basis data, dan perjanjian industri untuk pengungkapan peristiwa umum.	internal? <i>Processes:</i> analisis data historis 2. Apakah data eksternal (tren industri, data asosiasi pemerintah/kominfo) juga digunakan? <i>Information Items:</i> laporan tren eksternal 3. Bagaimana data eksternal dibandingkan dengan kondisi internal organisasi? <i>Processes:</i> benchmarking internal-eksternal 4. Apakah ada contoh perbaikan kebijakan/teknis yang diambil dari analisis tren eksternal? <i>Culture & Behavior:</i> keterbukaan untuk belajar dari eksternal			
6	<i>For similar classes of events, organize the collected data and highlight contributing factors. Determine common contributing factors across multiple</i>	Untuk kelas kejadian yang serupa, menyusun data yang terkumpul dan soroti faktor-faktor yang berkontribusi. Tentukan faktor-faktor yang berkontribusi secara	1. Apakah organisasi mengelompokkan insiden serupa (misalnya serangan <i>malware</i> berulang)? <i>Processes:</i> klasifikasi insiden serupa 2. Faktor penyebab umum apa saja yang biasanya diidentifikasi? <i>Information Items:</i> catatan faktor penyebab 3. Apakah hasil analisis faktor penyebab digunakan	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>events.</i>	umum pada beberapa kejadian.	untuk mencegah kejadian serupa? <i>Culture & Behavior</i> : kesadaran mencegah insiden berulang			
7	<i>Determine the specific conditions that existed or were absent when risk events occurred and the way the conditions affected event frequency and loss magnitude.</i>	Menentukan kondisi spesifik yang ada atau tidak ada saat peristiwa risiko terjadi dan cara kondisi tersebut memengaruhi frekuensi peristiwa dan besarnya kerugian.	1. Apakah kondisi tertentu (misalnya kurang staf, beban server tinggi) selalu dicatat saat insiden terjadi? <i>Processes</i> : pencatatan kondisi insiden 2. Bagaimana kondisi tersebut memengaruhi frekuensi kejadian/tingkat kerugian? <i>Information Items</i> : laporan analisis insiden 3. Apakah organisasi melakukan analisis <i>root cause</i> berbasis kondisi lingkungan/operasional? <i>Processes</i> : <i>root cause analysis</i> Root cause = penyebab paling mendasar suatu masalah/insiden, bukan sekadar gejala permukaan.	✓		
8	<i>Perform periodic event and risk factor analysis to identify new or emerging risk issues and to gain an</i>	Melakukan analisis kejadian dan faktor risiko secara berkala untuk mengidentifikasi masalah risiko baru atau	1. Seberapa sering dilakukan analisis risiko I&T berkala? <i>Policies</i> : kebijakan <i>review</i> berkala 2. Siapa yang terlibat dalam analisis berkala ini? <i>Organizational Structures</i> : tim Manajemen Risiko,	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>understanding of the associated internal and external risk factors.</i>	yang muncul dan untuk memperoleh pemahaman tentang faktor risiko internal dan eksternal terkait.	Bidang Telematika 3. Apakah hasil analisis digunakan untuk memperbarui daftar risiko organisasi? <i>Processes:</i> pembaruan daftar risiko 4. Apakah ada contoh risiko baru yang teridentifikasi dari analisis periodik (misalnya tren <i>ransomware</i>)? <i>Information Items:</i> laporan analisis risiko			
APO12.02 Analyze risk (Menganalisis risiko).						
9	<i>Define the appropriate scope of risk analysis efforts, considering all risk factors and/or the business criticality of assets.</i>	Menentukan cakupan upaya analisis risiko yang tepat, dengan mempertimbangkan semua faktor risiko dan/atau kekritisian aset dalam bisnis.	1. Bagaimana organisasi menentukan lingkup analisis risiko I&T (misalnya hanya pada aplikasi tertentu atau seluruh layanan publik)? <i>Processes:</i> prosedur penetapan lingkup analisis. 2. Siapa yang memutuskan ruang lingkup analisis risiko? <i>Organizational Structures (RACI):</i> Kepala Dinas, Bidang Telematika, Tim Manajemen Risiko. 3. Apakah ada kriteria formal untuk memilih aset mana yang dianggap kritis dalam analisis risiko? <i>Policies:</i> pedoman kritikalitas aset. 4. Bagaimana hasil penentuan lingkup analisis risiko	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			didokumentasikan? <i>Information Items: risk analysis scope document.</i>			
10	<i>Build and regularly update I&T risk scenarios; I&T-related loss exposures; and scenarios regarding reputational risk, including compound scenarios of cascading and/or coincidental threat types and events. Develop expectations for specific control activities and capabilities to detect.</i>	Menyusun dan memperbarui skenario risiko I&T secara berkala; paparan kerugian terkait I&T; dan skenario terkait risiko reputasi, termasuk skenario gabungan dari jenis dan peristiwa ancaman yang berjenjang dan/atau bersamaan. Mengembangkan ekspektasi untuk aktivitas dan kemampuan kontrol tertentu untuk	1. Apakah organisasi memiliki daftar atau katalog skenario risiko I&T yang terdokumentasi? <i>Policies: dokumen risk scenario register.</i> Risk scenario = gambaran terstruktur tentang kemungkinan kejadian risiko, dampak, dan penyebabnya. 2. Seberapa sering skenario risiko diperbarui (tahunan, per proyek besar, setelah insiden)? <i>Processes: siklus update skenario.</i> 3. Apakah organisasi pernah menyusun skenario gabungan (contoh: serangan siber + kegagalan infrastruktur jaringan terjadi bersamaan)? <i>Processes: penyusunan skenario multi-event.</i> 4. Siapa yang terlibat dalam penyusunan dan pembaruan skenario risiko I&T? <i>Organizational Structures (RACI): Bidang Telematika, Kepala Dinas, tim keamanan informasi.</i>	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
		mendeteksi.	5. Apakah ada metode standar dalam memperkirakan dampak reputasi dari sebuah skenario risiko I&T? <i>Policies:</i> panduan analisis reputasi. 6. Bagaimana informasi dari insiden nyata sebelumnya dipakai untuk memperkaya skenario risiko baru? <i>Information Items:</i> catatan insiden, laporan audit. 7. Bagaimana organisasi menentukan kontrol apa saja yang harus tersedia untuk setiap skenario risiko? <i>Processes:</i> mapping skenario ke kontrol. Control = mekanisme/prosedur untuk mengurangi atau mendeteksi risiko. 8. Apakah pimpinan atau <i>stakeholder</i> pernah dilibatkan dalam validasi skenario risiko sebelum dipakai dalam analisis formal? <i>Culture & Behavior:</i> keterlibatan pimpinan, tingkat keseriusan validasi.			
11	<i>Estimate the frequency (or likelihood) and magnitude of loss or</i>	Memperkirakan frekuensi (atau kemungkinan) dan	1. Bagaimana organisasi memperkirakan seberapa sering risiko I&T bisa terjadi? <i>Processes:</i> metode estimasi frekuensi.	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>gain associated with I&T risk scenarios. Take into account all applicable risk factors and evaluate known operational controls.</i>	besarnya kerugian atau keuntungan yang terkait dengan skenario risiko I&T. Mempertimbangkan semua faktor risiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.	2. Bagaimana memperkirakan besarnya kerugian (atau keuntungan) bila risiko terjadi? <i>Information Items:</i> data historis, perhitungan biaya. 3. Apakah faktor-faktor risiko eksternal (misalnya regulasi, tren siber) ikut dipertimbangkan? <i>Policies:</i> pedoman analisis risiko. 4. Bagaimana pengendalian yang ada dievaluasi saat memperkirakan dampak risiko? <i>Processes:</i> evaluasi kontrol.			
12	<i>Compare current risk (I&T-related loss exposure) to risk appetite and acceptable risk tolerance. Identify unacceptable or elevated risk.</i>	Membandingkan risiko saat ini (paparan kerugian terkait I&T) dengan selera risiko dan toleransi risiko yang dapat diterima. Mengidentifikasi risiko yang tidak dapat	1. Apakah organisasi pernah membandingkan profil risiko saat ini dengan <i>risk appetite</i> yang sudah ditetapkan? <i>Processes:</i> <i>risk profile vs appetite.</i> 2. Siapa yang berwenang menyatakan risiko melebihi batas <i>appetite/tolerance</i> ? <i>Organizational Structures (RACI):</i> pimpinan, komite risiko.	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
		diterima atau tinggi.	3. Apakah ada format laporan resmi untuk menyampaikan risiko yang tidak dapat diterima? <i>Information Items:</i> laporan eksposur risiko. 4. Bagaimana pimpinan menindaklanjuti risiko yang melebihi toleransi? <i>Culture & Behavior:</i> reaksi pimpinan terhadap pelanggaran batas.			
13	<i>Propose risk responses for risk exceeding risk appetite and tolerance levels.</i>	Mengusulkan respons risiko untuk risiko yang melampaui selera risiko dan tingkat toleransi.	1. Bagaimana organisasi menentukan opsi respons (menghindari, mengurangi, transfer, menerima)? <i>Processes:</i> risk response planning. 2. Siapa yang berwenang mengusulkan atau memilih opsi respons risiko? <i>Organizational Structures (RACI):</i> pimpinan, tim manajemen risiko. 3. Apakah ada dokumen yang mencatat usulan respons risiko? <i>Information Items:</i> risk response proposal. 4. Bagaimana respons risiko disesuaikan dengan	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			kebijakan organisasi? <i>Policies</i> : pedoman respons risiko.			
14	<i>Specify high-level requirements for projects or programs that will implement the selected risk responses. Identify requirements and expectations for appropriate key controls for risk mitigation responses.</i>	Menetapkan persyaratan tingkat tinggi untuk proyek atau program yang akan menerapkan respons risiko yang dipilih. Identifikasi persyaratan dan harapan untuk kontrol utama yang sesuai untuk respons mitigasi risiko.	1. Bagaimana organisasi menentukan proyek/program untuk mengurangi risiko I&T? <i>Processes</i> : perencanaan proyek mitigasi. 2. Apakah ada dokumen resmi yang menjelaskan kebutuhan & harapan kontrol utama? <i>Information Items</i> : <i>project charter</i> , TOR, <i>Business Case</i> <i>Project Charter</i> = dokumen awal proyek yang memuat tujuan, scope, risiko, dan high-level requirement. <i>TOR (Terms of Reference)</i> = dokumen yang menjelaskan detail kebutuhan, ruang lingkup, dan harapan dari suatu program/proyek. <i>Dokumen Business Case</i> = justifikasi proyek, sering kali berisi requirement kontrol risiko. 3. Siapa yang menyetujui requirement mitigasi risiko I&T? <i>Organizational Structures (RACI)</i> : pimpinan proyek, Kepala Dinas.	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			4. Bagaimana requirement tersebut dikomunikasikan ke tim pelaksana? <i>Information Flows</i> : rapat, dokumen tertulis.			
15	<i>Validate the risk analysis and business impact analysis (BIA) results before using them in decision making. Confirm that the analysis aligns with enterprise requirements and verify that estimations were properly calibrated and scrutinized for bias.</i>	Memvalidasi hasil analisis risiko dan analisis dampak bisnis (BIA) sebelum menggunakannya dalam pengambilan keputusan. Pastikan analisis tersebut sesuai dengan persyaratan perusahaan dan verifikasi bahwa estimasi telah dikalibrasi dengan benar dan diteliti untuk mengetahui biasnya.	1. Apakah hasil analisis risiko/BIA pernah diverifikasi ulang sebelum dipakai untuk keputusan? <i>Processes</i>: validasi analisis. BIA = analisis dampak bisnis, menilai seberapa parah dampak jika layanan terganggu. 2. Siapa yang melakukan validasi hasil analisis risiko? <i>Organizational Structures (RACI)</i>: tim independen, pimpinan. 3. Bagaimana memastikan hasil analisis bebas bias? <i>Policies</i>: prinsip validasi objektif. 4. Apakah ada bukti dokumentasi validasi (notulen, laporan)? <i>Information Items</i>: dokumen validasi.	✓		
16	<i>Analyze cost/benefit of</i>	Menganalisis	1. Apakah organisasi memiliki prosedur formal dalam	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>potential risk response options such as avoid, reduce/mitigate, transfer/share, and accept and exploit/seize. Confirm the optimal risk response.</i>	biaya/manfaat dari opsi respons risiko potensial seperti menghindari, mengurangi/meringankan, mentransfer/membagi, dan menerima serta memanfaatkan/merebut. Mengonfirmasikan respons risiko yang optimal.	membandingkan biaya dan manfaat dari berbagai opsi respons risiko? <i>Policies:</i> pedoman analisis <i>cost and benefit</i>. 2. Bagaimana cara organisasi menilai manfaat dari suatu respons risiko (misalnya pengurangan <i>downtime</i>, peningkatan kepercayaan publik)? <i>Processes:</i> metode analisis manfaat. 3. Apakah ada standar atau indikator keuangan yang digunakan dalam menghitung biaya (contoh: ROI, <i>payback period</i>)? <i>Information Items:</i> laporan keuangan, proyeksi biaya. 4. Siapa yang biasanya memutuskan opsi respons risiko yang dipilih (misalnya Kepala Dinas, komite risiko, atau bagian keuangan)? <i>Organizational Structures (RACI):</i> pengambil keputusan. 5. Bagaimana organisasi memastikan bahwa opsi respons risiko yang dipilih sesuai dengan <i>risk appetite</i> dan <i>tolerance</i> yang berlaku?			

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Processes: alignment</i> dengan <i>risk appetite</i>. 6. Apakah organisasi pernah menggunakan pendekatan transfer risiko (misalnya asuransi, outsourcing) dan bagaimana analisis biayanya dibanding mitigasi internal? <i>Processes: evaluasi opsi transfer.</i> 7. Apakah budaya organisasi cenderung lebih memilih menghindari risiko (<i>risk averse</i>) atau berani mengambil risiko untuk peluang strategis (<i>risk seeking</i>)? <i>Culture & Behavior: sikap organisasi terhadap risiko.</i> 8. Apakah hasil analisis <i>cost/benefit</i> didokumentasikan dan dilaporkan secara formal untuk mendukung keputusan manajemen? <i>Information Flows: laporan analisis risiko ke pimpinan.</i>			
APO12.03 Maintain a risk profile (Memelihara profile risiko).						
17	<i>Inventory business processes and document their dependency on I&T</i>	Menginventarisasi proses bisnis dan dokumentasikan ketergantungannya pada	1. Apakah organisasi memiliki inventaris proses bisnis yang terdokumentasi? <i>Information Items: dokumen inventaris proses bisnis.</i> 2. Bagaimana ketergantungan proses bisnis pada sistem	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>service management processes and IT infrastructure resources. Identify supporting personnel, applications, infrastructure, facilities, critical manual records, vendors, suppliers and outsourcers.</i>	proses manajemen layanan I&T dan sumber daya infrastruktur I&T. Mengidentifikasi personel pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan pihak yang melakukan alih daya.	I&T dicatat? <i>Processes:</i> pemetaan <i>dependency</i> . 3. Apakah personel pendukung, aplikasi, infrastruktur, vendor juga dicatat dalam inventaris ini? <i>Policies:</i> aturan kelengkapan inventaris. 4. Siapa yang bertanggung jawab memelihara inventaris tersebut? <i>Organizational Structures (RACI):</i> Bidang Telematika, unit perencanaan.			
18	<i>Determine and agree on which I&T services and IT infrastructure resources are essential to sustain the operation of business processes. Analyze dependencies and</i>	Menentukan dan menyetujui layanan I&T dan sumber daya infrastruktur I&T mana yang penting untuk mempertahankan operasi proses bisnis. Menganalisis	1. Bagaimana organisasi menentukan layanan I&T mana yang sangat kritis untuk layanan publik? <i>Processes:</i> analisis layanan esensial. 2. Apakah ada dokumen resmi yang menyatakan layanan/infrastruktur esensial? <i>Information Items:</i> daftar layanan kritis, BCP. 3. Siapa yang menyetujui daftar layanan/infrastruktur esensial?	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>identify weak links.</i>	ketergantungan dan mengidentifikasi titik lemah.	<i>Organizational Structures (RACI):</i> pimpinan, manajemen risiko. 4. Bagaimana titik lemah dalam ketergantungan layanan dianalisis? <i>Processes:</i> weak link analysis.			
19	<i>Aggregate current risk scenarios by category, business line and functional area.</i>	Mengumpulkan skenario risiko saat ini berdasarkan kategori, lini bisnis, dan area fungsional.	1. Apakah skenario risiko I&T pernah dikategorikan (contoh: operasional, keamanan data, layanan publik)? <i>Processes:</i> risk categorization. 2. Bagaimana skenario risiko dikonsolidasikan lintas unit? <i>Information Flows:</i> laporan konsolidasi. 3. Siapa yang menyetujui agregasi risiko lintas fungsi? <i>Organizational Structures (RACI):</i> komite risiko, pimpinan.	✓		
20	<i>Regularly capture all risk profile information and consolidate it into an aggregated risk profile.</i>	Secara berkala menangkap semua informasi profil risiko dan menggabungkannya menjadi profil risiko	1. Bagaimana organisasi menyatukan seluruh informasi risiko ke dalam profil risiko terkini? <i>Processes:</i> konsolidasi profil risiko. 2. Apakah ada sistem/ <i>tools</i> yang digunakan untuk mengelola profil risiko?	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
		agregat.	<i>Services & Infrastructure:</i> aplikasi GRC, spreadsheet, dsb. 3. Bagaimana hasil konsolidasi dibagikan ke stakeholder? <i>Information Flows:</i> laporan risk profile.			
21	<i>Capture information on the status of the risk action plan for inclusion in the I&T risk profile of the enterprise.</i>	Menangkap informasi tentang status rencana tindakan risiko untuk dimasukkan dalam profil risiko I&T perusahaan.	1. Apakah setiap tindakan mitigasi risiko memiliki action plan resmi? <i>Policies:</i> pedoman penyusunan action plan. 2. Bagaimana status pelaksanaan action plan dipantau? <i>Processes:</i> monitoring rencana aksi. 3. Siapa yang bertanggung jawab melaporkan progres action plan? <i>Organizational Structures (RACI):</i> pemilik risiko, pimpinan unit.	✓		
22	<i>Based on all risk profile data, define a set of risk indicators that allow the quick identification and</i>	Berdasarkan semua data profil risiko, tentukan serangkaian indikator risiko yang memungkinkan	1. Apakah organisasi memiliki indikator risiko utama (KRI) untuk memantau tren risiko? <i>Policies:</i> definisi KRI. 2. Bagaimana KRI ditentukan dari data profil risiko? <i>Processes:</i> metode penetapan indikator.	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>monitoring of current risk and risk trends.</i>	identifikasi dan pemantauan cepat risiko terkini dan tren risiko.	3. Apakah indikator risiko digunakan secara rutin dalam rapat pimpinan? <i>Information Items:</i> laporan KRI. 4. Siapa yang menyetujui indikator risiko sebelum digunakan? <i>Organizational Structures (RACI):</i> pimpinan, komite risiko. KRI (Key Risk Indicator) = indikator pengukuran kuantitatif atau kualitatif yang digunakan organisasi			
23	<i>Capture information on I&T risk events that have materialized for inclusion in the IT risk profile of the enterprise.</i>	Menangkap informasi tentang peristiwa risiko I&T yang telah terwujud untuk dimasukkan dalam profil risiko I&T perusahaan.	1. Apakah organisasi memiliki catatan formal untuk insiden atau peristiwa risiko I&T? <i>Information Items:</i> log insiden, laporan keamanan. 2. Bagaimana data insiden dikumpulkan (manual, sistem otomatis)? <i>Processes:</i> mekanisme pencatatan insiden. 3. Siapa yang bertanggung jawab melaporkan insiden risiko I&T? <i>Organizational Structures (RACI):</i> unit operasional, helpdesk TI.	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
APO12.04 Articulate risk (Mengartikulasikan Risiko).						
24	Report the results of risk analysis to all affected stakeholders in terms and formats useful to support enterprise decisions. Whenever possible, include probabilities and ranges of loss or gain along with confidence levels, to enable management to balance risk-return.	Melaporkan hasil analisis risiko kepada semua pemangku kepentingan yang terpengaruh dalam bentuk dan format yang berguna untuk mendukung keputusan perusahaan. Jika memungkinkan, sertakan probabilitas dan rentang kerugian atau keuntungan beserta tingkat keyakinan, untuk memungkinkan manajemen menyeimbangkan risiko-imbal hasil.	1. Bagaimana hasil analisis risiko disampaikan ke stakeholder? <i>Information Flows</i> : laporan, dashboard. 2. Apakah laporan analisis risiko mencantumkan probabilitas dan range kerugian? <i>Information Items</i> : format laporan risiko. 3. Siapa yang meninjau laporan analisis risiko sebelum didistribusikan? <i>Organizational Structures (RACI)</i> : pimpinan, tim analisis.	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
25	<i>Provide decision makers with an understanding of worst-case and most-probable scenarios, I&T-related loss exposures and significant reputation, legal and regulatory considerations, or any other impact category as per the risk taxonomy.</i>	Memberikan para pengambil keputusan pemahaman tentang skenario terburuk dan paling mungkin, paparan kerugian terkait I&T, serta reputasi signifikan, pertimbangan hukum dan peraturan, atau kategori dampak lainnya sesuai taksonomi risiko.	1. Bagaimana pengambil keputusan mendapat gambaran skenario terburuk/terbaik dari risiko I&T? <i>Processes: briefing</i> risiko. 2. Apakah aspek reputasi, hukum, dan regulasi juga disampaikan dalam laporan risiko? <i>Policies: pedoman</i> laporan risiko. 3. Bagaimana kejelasan laporan disesuaikan dengan kebutuhan pimpinan? <i>Culture & Behavior: komunikasi</i> yang dipahami non-teknis.	✓		
26	<i>Report the current risk profile to all stakeholders. Include information on the effectiveness of the risk management process,</i>	Melaporkan profil risiko terkini kepada semua pemangku kepentingan. Sertakan informasi tentang efektivitas proses manajemen	1. Apakah organisasi secara rutin melaporkan profil risiko terkini ke <i>stakeholder</i> ? <i>Processes: siklus</i> pelaporan risiko. 2. Apa saja informasi yang disertakan (efektivitas kontrol, kesenjangan, status remediasi)? <i>Information Items: laporan</i> profil risiko.	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>control effectiveness, gaps, inconsistencies, redundancies, remediation status and their impacts on the risk profile.</i>	risiko, efektivitas pengendalian, kesenjangan, inkonsistensi, redundansi, status perbaikan, dan dampaknya terhadap profil risiko.	3. Siapa yang menerima laporan profil risiko? <i>Organizational Structures (RACI):</i> pimpinan, auditor, regulator.			
27	<i>On a periodic basis, for areas with relative risk and risk capacity parity, identify I&T-related opportunities that would allow the acceptance of greater risk and enhanced growth and return.</i>	Secara berkala, untuk area dengan risiko relatif dan paritas kapasitas risiko, mengidentifikasi peluang terkait I&T yang akan memungkinkan penerimaan risiko lebih besar dan peningkatan pertumbuhan dan laba.	1. Apakah organisasi pernah mengidentifikasi peluang I&T saat risiko relatif rendah? <i>Processes:</i> analisis peluang risiko. 2. Bagaimana peluang tersebut dievaluasi terhadap kapasitas risiko organisasi? <i>Policies:</i> pedoman evaluasi peluang. 3. Apakah ada contoh peluang I&T yang dimanfaatkan untuk pertumbuhan? <i>Information Items:</i> studi kasus peluang.	✓		
28	<i>Review the results of</i>	Meninjau hasil penilaian	1. Apakah hasil audit eksternal/asesmen pihak ketiga	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>objective third-party assessments and internal audit and quality assurance reviews. Include them in the risk profile. Review identified gaps and I&T-related loss exposures to determine the need for additional risk analysis.</i>	pihak ketiga yang objektif dan tinjauan audit internal serta jaminan kualitas. Sertakan hasil tersebut dalam profil risiko. Tinjau kesenjangan yang teridentifikasi dan paparan kerugian terkait I&T untuk menentukan perlunya analisis risiko tambahan.	dimasukkan ke dalam profil risiko? <i>Processes: integrasi hasil audit.</i> 2. Bagaimana kesenjangan yang ditemukan ditindaklanjuti? <i>Processes: corrective action.</i> 3. Siapa yang meninjau hasil asesmen tersebut? <i>Organizational Structures (RACI): pimpinan, auditor internal.</i>			
APO12.05 Define a risk management action portfolio (Menentukan portofolio tindakan manajemen risiko).						
29	<i>Maintain an inventory of control activities that are in place to mitigate risk and that enable risk to be taken in line with the risk</i>	Memelihara inventaris aktivitas pengendalian yang ada untuk mengurangi risiko dan yang memungkinkan risiko ditangani sesuai	1. Apakah organisasi memiliki daftar resmi kontrol mitigasi risiko? <i>Information Items: control inventory.</i> 2. Bagaimana kontrol diklasifikasikan dan dipetakan ke skenario risiko? <i>Processes: kontrol mapping.</i>	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>appetite and tolerance. Classify control activities and map them to specific I&T risk scenarios and aggregations of I&T risk scenarios.</i>	dengan selera dan toleransi risiko. Mengklasifikasikan aktivitas pengendalian dan memetakannya ke skenario risiko I&T tertentu dan agregasi skenario risiko I&T.	3. Siapa yang bertanggung jawab memperbarui inventaris kontrol? <i>Organizational Structures (RACI):</i> tim pengendalian internal, Bidang Telematika.			
30	<i>Determine whether each organizational entity monitors risk and accepts accountability for operating within its individual and portfolio tolerance levels.</i>	Menentukan apakah setiap entitas organisasi memantau risiko dan menerima akuntabilitas untuk beroperasi dalam tingkat toleransi individu dan portofolionya.	1. Apakah tiap unit organisasi diminta memantau risiko sendiri? <i>Policies:</i> aturan akuntabilitas risiko. 2. Bagaimana akuntabilitas risiko dibuktikan? <i>Information Items:</i> laporan risiko unit. 3. Siapa yang menilai apakah unit sudah sesuai toleransi? <i>Organizational Structures (RACI):</i> manajemen risiko, pimpinan.	✓		
31	<i>Define a balanced set</i>	Menentukan	4. Bagaimana organisasi menilai proyek mitigasi risiko			

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>of project proposals designed to reduce risk and/or projects that enable strategic enterprise opportunities, considering costs, benefits, effect on current risk profile and regulations.</i>	serangkaian proposal proyek yang seimbang yang dirancang untuk mengurangi risiko dan/atau proyek yang memungkinkan peluang perusahaan strategis, dengan mempertimbangkan biaya, manfaat, dampak pada profil risiko dan peraturan saat ini.	vs proyek peluang? <i>Processes:</i> penilaian biaya-manfaat proyek. 5. Apakah biaya, manfaat, dan regulasi dijadikan pertimbangan formal? <i>Policies:</i> pedoman seleksi proyek. 6. Siapa yang memutuskan proposal proyek mana yang dijalankan? <i>Organizational Structures (RACI):</i> pimpinan, tim perencanaan.			
APO12.06 Respond to risk (Menanggapi risiko).						
32	<i>Prepare, maintain and test plans that document the specific steps to take when a risk event may cause a significant operational</i>	Menyiapkan, memelihara, dan menguji rencana yang mendokumentasikan langkah-langkah spesifik yang harus	1. Apakah organisasi memiliki dokumen rencana penanganan insiden risiko I&T yang formal? <i>Policies:</i> <i>disaster recovery plan</i> (DRP), <i>business continuity plan</i> (BCP). 2. Bagaimana rencana penanganan insiden tersebut disusun? Apakah ada prosedur baku?	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>or development incident with serious business impact. Ensure that plans include pathways of escalation across the enterprise.</i>	diambil ketika suatu peristiwa risiko dapat menyebabkan insiden operasional atau pengembangan yang signifikan dengan dampak bisnis yang serius. Pastikan bahwa rencana tersebut mencakup jalur eskalasi di seluruh perusahaan.	<i>Processes:</i> mekanisme penyusunan rencana. 3. Siapa yang terlibat dalam penyusunan dan pemeliharaan rencana ini? <i>Organizational Structures (RACI):</i> tim TI, pimpinan, manajemen risiko, pihak eksternal. 4. Apakah rencana ini secara berkala diuji melalui simulasi/drill? Jika ya, seberapa sering? <i>Processes:</i> uji coba dan review periodik. 5. Apakah tersedia jalur eskalasi resmi bila insiden signifikan terjadi (contoh: siapa yang dihubungi pertama, siapa yang memberi keputusan)? <i>Information Flows:</i> diagram eskalasi, SOP eskalasi. 6. Apakah ada sarana/infrastruktur khusus untuk mendukung eksekusi rencana (misalnya backup site, hotline darurat)? <i>Services & Infrastructure:</i> fasilitas pendukung. 7. Bagaimana budaya staf dan pimpinan dalam mengikuti simulasi atau uji coba rencana (serius, formalitas, atau kurang antusias)?			

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Culture & Behavior</i> : keterlibatan dalam simulasi. 8. Apakah hasil uji coba rencana (misalnya drill bencana I&T) selalu didokumentasikan dan dipakai untuk perbaikan rencana berikutnya? <i>Information Items</i> : laporan hasil <i>drill</i> , <i>corrective action</i> .			
33	<i>Apply the appropriate response plan to minimize the impact when risk incidents occur.</i>	Menerapkan rencana respons yang tepat untuk meminimalkan dampak saat insiden risiko terjadi.	1. Apakah organisasi pernah benar-benar menerapkan rencana respons risiko I&T saat terjadi insiden besar (misalnya server <i>down</i> , kebocoran data)? <i>Information Items</i> : laporan insiden, catatan tindak lanjut. 2. Siapa yang biasanya mengambil keputusan utama ketika insiden risiko terjadi? <i>Organizational Structures (RACI)</i> : Kepala Dinas, Bidang Telematika, tim tanggap darurat. 3. Bagaimana proses koordinasi antar-unit dilakukan saat rencana respons dijalankan? <i>Processes</i> : mekanisme koordinasi lintas unit. 4. Apakah tersedia sarana pendukung untuk memfasilitasi eksekusi respons (contoh: sistem monitoring <i>real-time</i> , ruang kendali)?	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Services & Infrastructure:</i> tools dan fasilitas darurat. 5. Bagaimana budaya staf saat menghadapi insiden – apakah tenang dan mengikuti prosedur, atau panik dan improvisasi? <i>Culture & Behavior:</i> reaksi nyata staf/pimpinan. 6. Apakah hasil penerapan rencana respons dievaluasi untuk memperbaiki SOP atau prosedur yang ada? <i>Processes:</i> siklus pembelajaran pasca-insiden.			
34	<i>Categorize incidents and compare I&T-related loss exposures against risk tolerance thresholds.</i> <i>Communicate business impacts to decision makers as part of reporting and update the risk profile.</i>	Mengategorikan insiden dan bandingkan paparan kerugian terkait I&T terhadap ambang batas toleransi risiko. Komunikasikan dampak bisnis kepada para pengambil keputusan sebagai bagian dari pelaporan dan perbarui profil risiko.	1. Apakah insiden I&T (misalnya <i>downtime</i> aplikasi, serangan siber, kebocoran data) dikategorikan secara resmi menurut tingkat keparahan? <i>Policies:</i> SOP kategorisasi insiden. 2. Bagaimana organisasi menentukan apakah suatu insiden sudah melewati ambang batas toleransi risiko? <i>Processes:</i> mekanisme penilaian toleransi. 3. Siapa yang berwenang melakukan validasi kategori insiden dan memutuskan langkah eskalasi? <i>Organizational Structures (RACI):</i> pejabat <i>risk owner</i>, Kepala Dinas, tim TI.	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			4. Apakah hasil perbandingan insiden dengan toleransi risiko terdokumentasi dan masuk ke profil risiko organisasi? <i>Information Items:</i> risk register, laporan insiden. 5. Bagaimana dampak bisnis dari insiden I&T dikomunikasikan kepada pengambil keputusan? <i>Information Flows:</i> laporan resmi, rapat pimpinan, dashboard. 6. Bagaimana budaya organisasi dalam menyikapi insiden yang melewati toleransi risiko, apakah terbuka membahasnya atau cenderung menutupinya? <i>Culture & Behavior:</i> keterbukaan pimpinan/staf.			
35	<i>Examine past adverse events/losses and missed opportunities and determine root causes.</i>	Memeriksa kejadian/kerugian buruk di masa lalu dan kesempatan yang hilang, serta menentukan akar penyebabnya.	1. Apakah organisasi memiliki catatan resmi terkait insiden atau kerugian I&T di masa lalu (misalnya downtime panjang, kebocoran data, proyek I&T gagal)? <i>Information Items:</i> laporan insiden, audit, lessons learned. 2. Bagaimana organisasi menganalisis akar penyebab (root cause) dari insiden atau kerugian tersebut?	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Processes</i>: metode <i>root cause analysis</i> (misalnya <i>fishbone</i>, <i>5-why</i>). 3. Siapa saja yang biasanya dilibatkan dalam proses investigasi akar penyebab insiden I&T? <i>Organizational Structures (RACI)</i>: tim TI, manajemen risiko, pimpinan. 4. Apakah ada prosedur formal untuk melakukan evaluasi pasca-insiden (<i>post-mortem review</i>)? <i>Policies</i>: SOP evaluasi insiden. 5. Apakah faktor eksternal (regulasi, vendor, cuaca, tren industri) juga dipertimbangkan dalam analisis kerugian masa lalu? <i>Processes</i>: analisis faktor eksternal. 6. Bagaimana budaya organisasi dalam menyikapi insiden masa lalu, apakah terbuka mencari solusi atau cenderung menyalahkan pihak tertentu? <i>Culture & Behavior</i>: sikap staf/pimpinan. 7. Apakah hasil analisis insiden masa lalu digunakan sebagai bahan pembelajaran untuk memperbaiki			

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			kebijakan atau SOP? <i>Processes</i> : siklus perbaikan berkelanjutan.			
36	<i>Communicate root cause, additional risk response requirements and process improvements to appropriate decision makers. Ensure that the cause, response requirements and process improvement are included in risk governance processes.</i>	Mengomunikasikan akar permasalahan, persyaratan respons risiko tambahan, dan perbaikan proses kepada para pengambil keputusan yang tepat. Pastikan bahwa penyebab, persyaratan respons, dan perbaikan proses disertakan dalam proses tata kelola risiko.	1. Apakah hasil analisis akar penyebab (<i>root cause</i>) insiden I&T secara rutin disampaikan ke pimpinan atau pengambil keputusan? <i>Information Flows</i>: laporan resmi, rapat evaluasi. 2. Bagaimana organisasi memastikan bahwa kebutuhan respons tambahan (misalnya kontrol baru, peningkatan keamanan) disampaikan dengan jelas kepada pengambil keputusan? <i>Processes</i>: mekanisme eskalasi kebutuhan respons. 3. Siapa yang bertanggung jawab mengomunikasikan hasil analisis akar penyebab dan rekomendasi perbaikan? <i>Organizational Structures (RACI)</i>: manajemen risiko, Kepala Bidang Telematika, tim investigasi. 4. Apakah ada kebijakan formal yang mewajibkan penyampaian hasil analisis akar penyebab kepada level manajemen tertentu?	✓		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Policies:</i> aturan eskalasi hasil investigasi. 5. Bagaimana budaya organisasi dalam menerima rekomendasi perbaikan, apakah proaktif untuk memperbaiki atau cenderung menunda? <i>Culture & Behavior:</i> sikap pimpinan dan staf. 6. Apakah hasil rekomendasi perbaikan biasanya diintegrasikan ke dalam kebijakan atau prosedur manajemen risiko? <i>Processes:</i> pembaruan SOP, kebijakan risiko. 7. Apakah organisasi pernah mengevaluasi efektivitas perbaikan proses setelah implementasi rekomendasi? <i>Information Items:</i> laporan evaluasi, hasil audit tindak lanjut.			

Keterangan:

R: Relevan

TR: Tidak Relevan

Hasil Validasi Uji Instrumen FGD Oleh Ahli
Dalam Rangka Penelitian Skripsi Pengukuran Kapabilitas Manajemen Risiko
Informasi dan Teknologi (I&T) pada Dinas Komunikasi dan Informatika Kabupaten
Klungkung Menggunakan *Framework* COBIT 2019

Data Penguji Ahli

Nama	: Ir. I Nyoman Sujana Saputra, S.T., M.TI., IPU.
Instansi	: PT. Tigatra Infokom
Jabatan	: Ahli COBIT 2019 – Sr. Manager Digital Transformation and I&T Solution
NIK	: 36201911089

Hasil Instrumen FGD

1. –



Semarang, 18 Oktober 2025

Penguji Ahli,

Peneliti,

Ir. I Nyoman Sujana Saputra, S.T., M.TI., IPU.

Ketut Ananda Dharmawati

NIK. 36201911089

NIM 2215091035

Lampiran 5. Hasil Uji Instrumen FGD dengan Validator Kedua

Form Uji Validasi Oleh Ahli Dalam Rangka Penelitian Skripsi

Nama Mahasiswa	: Ketut Ananda Dharmawati
NIM	: 2215091035
Judul Skripsi:	: Pengukuran Kapabilitas Manajemen Risiko Informasi dan Teknologi (I&T) pada Dinas Komunikasi dan Informatika Kabupaten Klungkung Menggunakan <i>Framework</i> COBIT 2019.
Tujuan Uji	: Untuk memastikan bahwa butir-butir pertanyaan dalam instrumen FGD: 1. Sudah sesuai dan mewakili indikator aktivitas dalam domain EDM03 dan APO12 pada <i>framework</i> COBIT 2019. 2. Memiliki relevansi dan kejelasan makna sesuai konteks penelitian di lingkungan instansi pemerintah, khususnya Diskominfo Klungkung. 3. Dapat mengukur kemampuan manajemen risiko I&T secara konsisten dan objektif, tanpa menimbulkan tafsir ganda bagi informan maupun peneliti. 4. Layak digunakan sebagai alat pengumpulan data melalui FGD, setelah dilakukan telaah oleh ahli di bidang tata kelola I&T (COBIT 2019).

INSTRUMEN FGD

Keterangan:

R: Relevan

TR: Tidak Relevan

Tujuan						
<i>Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.</i>			Memastikan bahwa risiko perusahaan yang terkait dengan I&T tidak melebihi selera risiko dan toleransi risiko perusahaan, dampak risiko I&T terhadap nilai perusahaan diidentifikasi dan dikelola, dan potensi kegagalan kepatuhan diminimalkan.			
EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
EDM03.01 Evaluate risk management (Mengevaluasi manajemen risiko).						
1	<i>Understand the organization and its context related to I&T risk.</i>	Memahami organisasi dan konteksnya terkait dengan risiko I&T.	1. Apakah organisasi memiliki dokumen yang menggambarkan risiko I&T dalam konteks pelayanan publik (misalnya Renstra Diskominfo atau <i>Masterplan</i> I&T)? <i>Policies</i> : aturan tertulis, rencana strategis. 2. Bagaimana pimpinan mengidentifikasi faktor	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			eksternal (peraturan pemerintah, ancaman siber nasional) yang dapat memengaruhi risiko I&T? <i>Processes</i>: prosedur evaluasi eksternal. 3. Apakah ada forum khusus untuk membahas faktor internal yang menambah risiko I&T (misalnya keterbatasan SDM, anggaran, atau infrastruktur)? <i>Organizational Structures</i>: siapa yang ikut forum (Kepala Dinas, Bidang Telematika). 4. Bagaimana risiko I&T dipetakan terhadap layanan publik yang dikelola Diskominfo (contoh: <i>e-government</i>, data kependudukan)? <i>Processes</i>: cara organisasi memetakan risiko. 5. Apakah hasil identifikasi konteks risiko I&T biasanya didokumentasikan? <i>Information Items</i>: notulen rapat, <i>risk register</i>. 6. Bagaimana budaya pimpinan/staf dalam membicarakan (membahas) risiko I&T, terbuka, formal, atau memiliki kecenderungan menutupi masalah? <i>Culture & Behavior</i>: kebiasaan staf/pimpinan.			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
2	<i>Determine the risk appetite of the organization, i.e., the level of I&T-related risk that the enterprise is willing to take in its pursuit of enterprise objectives.</i>	Menentukan selera risiko organisasi, yaitu tingkat risiko terkait I&T yang bersedia diambil perusahaan dalam mengejar tujuan perusahaan.	1. Apakah organisasi memiliki pernyataan formal tentang tingkat risiko I&T yang masih bisa ditoleransi? <i>Policies</i>: dokumen risk appetite statement, SK, kebijakan risiko. 2. Siapa yang berwenang menentukan risk appetite organisasi? <i>Organizational Structures (RACI)</i>: Kepala Dinas, Sekda, atau komite. 3. Apakah risk appetite berbeda untuk tiap bidang (contoh: keamanan data vs layanan jaringan)? <i>Processes</i>: cara organisasi menetapkan risk appetite berbeda. 4. Bagaimana risk appetite dikaitkan dengan tujuan strategis Diskominfo (misalnya digitalisasi layanan publik)? <i>Information Items</i>: strategi TI, KPI organisasi. 5. Apakah risk appetite pernah direvisi/ditinjau ulang secara berkala? <i>Processes</i>: siklus review.			Risk appetite: Dokumen tingkat risiko

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			6. Bagaimana pimpinan menyampaikan <i>risk appetite</i> kepada staf teknis? <i>Information Flows</i>: rapat, edaran, sosialisasi. 7. Apakah ada contoh nyata risiko yang dianggap “masih bisa diterima”? <i>Culture & Behavior</i>: contoh sikap pimpinan/staf.			
3	<i>Determine risk tolerance levels against the risk appetite, i.e., temporarily acceptable deviations from the risk appetite.</i>	Menentukan tingkat toleransi risiko terhadap selera risiko, yaitu penyimpangan yang dapat diterima sementara dari selera risiko.	1. Apakah organisasi memiliki standar formal terkait toleransi risiko (misalnya <i>downtime server</i> maksimal 30 menit)? <i>Policies</i>: SLA, SOP. 2. Bagaimana proses penetapan batas toleransi risiko dilakukan? <i>Processes</i>: prosedur penetapan toleransi. 3. Apakah toleransi berbeda antara sistem kritis (contoh: data kependudukan) dan sistem pendukung (contoh: website informasi)? <i>Information Items</i>: dokumen SLA/kontrak. 4. Siapa yang memutuskan kapan suatu risiko sudah melampaui toleransi dan harus diekskalasi?	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Organizational Structures (RACI)</i>: pejabat yang berwenang. 5. Bagaimana toleransi risiko dikomunikasikan ke staf operasional? <i>Information Flows</i>: SOP, pelatihan, <i>briefing</i>. 6. Apakah pernah terjadi pelanggaran batas toleransi risiko? Bagaimana tindak lanjutnya? <i>Processes</i>: tindakan korektif. 7. Apakah toleransi risiko dipengaruhi oleh regulasi eksternal (misalnya standar keamanan nasional)? <i>Culture & Behavior</i>: kesadaran staf terhadap aturan luar. 8. Bagaimana organisasi membedakan toleransi jangka pendek (sementara) dengan <i>risk appetite</i> jangka panjang? <i>Processes</i>: mekanisme pembedaan.			
4	<i>Determine the extent of alignment of the I&T risk strategy to the enterprise risk strategy</i>	Menentukan tingkat keselarasan strategi risiko I&T dengan strategi risiko	1. Apakah strategi risiko I&T pernah dibandingkan atau diselaraskan dengan strategi risiko organisasi secara keseluruhan? <i>Processes</i>: mekanisme evaluasi strategi.	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>and ensure the risk appetite is below the organization's risk capacity.</i>	perusahaan dan memastikan selera risiko berada di bawah kapasitas risiko organisasi.	2. Siapa yang bertanggung jawab memastikan keselarasan ini? <i>Organizational Structures (RACI):</i> Kepala Dinas, Komite Risiko (divisi / tim ad-hoc). 3. Apakah ada dokumen yang menunjukkan integrasi antara strategi risiko I&T dan strategi risiko organisasi? <i>Information Items: risk strategy document, Renstra, laporan risiko.</i> 4. Bagaimana pimpinan memastikan bahwa <i>risk appetite</i> I&T tidak melebihi kapasitas risiko organisasi? <i>Policies:</i> prinsip atau batas resmi dalam dokumen. 5. Apakah ada forum lintas unit (I&T dan non-I&T) untuk meninjau keselarasan strategi risiko? <i>Organizational Structures:</i> kolaborasi antar-unit. 6. Apakah ada contoh keputusan strategis yang memperlihatkan keterkaitan langsung antara risiko I&T dan strategi organisasi? <i>Culture & Behavior:</i> kesadaran pimpinan.			
5	<i>Proactively evaluate</i>	Mengevaluasi faktor	1. Apakah organisasi selalu menilai risiko I&T sebelum	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>I&T risk factors in advance of pending strategic enterprise decisions and ensure that risk considerations are part of the strategic enterprise decision process.</i>	risiko I&T secara proaktif sebelum mengambil keputusan strategis perusahaan dan memastikan bahwa pertimbangan risiko menjadi bagian dari proses pengambilan keputusan strategis perusahaan.	mengambil keputusan strategis (misalnya terkait digitalisasi layanan)? <i>Processes: risk assessment</i> pra-keputusan. 2. Siapa yang wajib memberikan masukan risiko I&T dalam rapat pengambilan keputusan strategis? <i>Organizational Structures (RACI):</i> Kepala Dinas, Bidang Telematika. 3. Apakah ada prosedur baku yang mengatur penyampaian risiko I&T sebelum keputusan dibuat? <i>Policies: SOP, aturan rapat.</i> 4. Bagaimana informasi risiko I&T disampaikan ke pimpinan sebelum keputusan? <i>Information Flows: notulen, laporan, presentasi.</i> 5. Apakah faktor risiko I&T selalu menjadi agenda dalam rapat pimpinan strategis? <i>Policies: tata tertib rapat.</i> 6. Bagaimana pimpinan merespons masukan risiko I&T dalam rapat? <i>Culture & Behavior: sikap pimpinan terhadap masukan</i>			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			risiko. 7. Apakah ada kasus nyata di mana keputusan strategis berubah karena pertimbangan risiko I&T? <i>Processes:</i> bukti integrasi risiko ke pengambilan keputusan. 8. Apakah hasil evaluasi risiko I&T terdokumentasi sebagai bahan pembelajaran untuk keputusan berikutnya? <i>Information Items:</i> laporan evaluasi, lessons learned.			
6	<i>Evaluate risk management activities to ensure alignment with the enterprise's capacity for I&T-related loss and leadership's tolerance of it.</i>	Mengevaluasi aktivitas manajemen risiko untuk memastikan keselarasan dengan kapasitas perusahaan terhadap kerugian terkait I&T dan toleransi pimpinan terhadap kerugian tersebut.	1. Apakah ada evaluasi formal terhadap kegiatan manajemen risiko I&T? <i>Processes:</i> audit internal, <i>review</i> tahunan. 2. Bagaimana organisasi memastikan kegiatan manajemen risiko sesuai kapasitas keuangan atau sumber daya? <i>Policies:</i> batas anggaran, pedoman alokasi SDM. 3. Apakah pimpinan menetapkan batas toleransi kerugian terkait I&T (misalnya <i>downtime</i> maksimal, batas kehilangan data)?	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Organizational Structures (RACI)</i>: pimpinan, dewan. 4. Bagaimana hasil evaluasi manajemen risiko I&T dilaporkan? <i>Information Items</i>: laporan risiko, hasil audit. 5. Apakah kegiatan manajemen risiko I&T pernah dikoreksi karena dianggap melampaui kapasitas organisasi? <i>Processes: corrective actions.</i> 6. Bagaimana sikap pimpinan terhadap hasil evaluasi yang menunjukkan potensi kerugian besar? <i>Culture & Behavior</i>: penerimaan pimpinan atas risiko. 7. Apakah ada mekanisme eskalasi jika aktivitas manajemen risiko I&T dinilai tidak sesuai kapasitas organisasi? <i>Information Flows</i>: jalur eskalasi resmi.			
7	<i>Attract and maintain necessary skills and personnel for I&T Risk Management.</i>	Merekrut dan mempertahankan keterampilan dan personel yang	1. Apakah organisasi memiliki staf khusus yang menangani manajemen risiko I&T? <i>Organizational Structures (RACI)</i>: posisi formal di struktur organisasi.	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
		diperlukan untuk Manajemen Risiko I&T.	2. Bagaimana organisasi mengidentifikasi kebutuhan keterampilan staf untuk manajemen risiko I&T? <i>Processes:</i> analisis kebutuhan SDM. 3. Apakah tersedia program pelatihan internal maupun eksternal atau sertifikasi khusus untuk staf terkait risiko I&T? <i>People, Skills & Competencies:</i> pelatihan, <i>workshop</i>. 4. Bagaimana organisasi memastikan staf baru memahami kebijakan manajemen risiko I&T? <i>Policies:</i> materi induksi/briefing. 5. Apakah ada program retensi untuk mempertahankan staf yang kompeten di bidang risiko I&T? <i>Culture & Behavior:</i> penghargaan, promosi. 6. Bagaimana organisasi mengatasi kekurangan staf berkompeten di bidang risiko I&T? <i>Processes:</i> strategi rekrutmen, outsourcing. 7. Apakah ada perencanaan jangka panjang untuk pengembangan kompetensi staf risiko I&T? <i>Policies:</i> dokumen HR, Renstra SDM.			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			8. Bagaimana organisasi memanfaatkan infrastruktur (contoh: <i>e-learning</i>, <i>platform</i> pelatihan <i>online</i>) untuk mendukung pengembangan staf? <i>Services & Infrastructure</i>: sistem pendukung pelatihan. 9. Apakah kompetensi staf di bidang risiko I&T pernah dievaluasi secara formal (misalnya melalui asesmen)? <i>People, Skills & Competencies</i>: uji kompetensi.			
EDM03.02 Direct risk management (Mengarahkan manajemen risiko).						
8	<i>Direct the translation and integration of the I&T risk strategy into risk management practices and operational activities.</i>	Mengarahkan penerjemahan dan integrasi strategi risiko I&T ke dalam praktik manajemen risiko dan aktivitas operasional.	1. Apakah strategi risiko I&T yang dimiliki organisasi sudah diterjemahkan menjadi praktik operasional sehari-hari? <i>Processes</i>: bukti implementasi dalam SOP atau <i>workflow</i>. 2. Siapa yang bertanggung jawab memastikan strategi risiko I&T diintegrasikan ke kegiatan operasional? <i>Organizational Structures (RACI)</i>: Kepala Dinas, Bidang Telematika, tim manajemen risiko. 3. Apakah ada dokumen yang menjelaskan bagaimana strategi risiko I&T diturunkan ke tingkat operasional?	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Information Items:</i> pedoman, manual kerja, SOP. 4. Bagaimana organisasi memastikan staf memahami strategi risiko I&T dalam pekerjaannya sehari-hari? <i>Culture & Behavior:</i> komunikasi & sosialisasi. 5. Apakah ada rapat rutin untuk meninjau sejauh mana strategi risiko I&T dijalankan di <i>level</i> operasional? <i>Information Flows:</i> laporan rapat, notulen. 6. Apakah terdapat contoh nyata kegiatan operasional yang sudah menyesuaikan strategi risiko I&T? <i>Processes:</i> contoh implementasi. 7. Bagaimana organisasi mengukur efektivitas integrasi strategi risiko I&T ke operasional? <i>Policies:</i> indikator kinerja, KPI. 8. Apakah strategi risiko I&T pernah gagal diterapkan di lapangan? Jika ya, apa penyebabnya? <i>Processes:</i> evaluasi kegagalan.			
9	<i>Direct the development of risk communication plans (covering all</i>	Mengarahkan pengembangan rencana komunikasi risiko	1. Apakah organisasi memiliki rencana komunikasi risiko yang formal dan tertulis? <i>Policies:</i> dokumen komunikasi risiko.	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>levels of the enterprise).</i>	(mencakup semua tingkatan perusahaan).	2. Siapa yang bertanggung jawab mengembangkan rencana komunikasi risiko? <i>Organizational Structures (RACI):</i> Bidang Telematika, Sekretariat, pimpinan. 3. Bagaimana informasi risiko disampaikan ke level pimpinan, staf teknis, dan pemangku kepentingan eksternal? <i>Information Flows:</i> jalur komunikasi resmi. 4. Apakah ada perbedaan cara komunikasi risiko untuk level manajemen dan staf operasional? <i>Processes:</i> metode komunikasi berbeda. 5. Bagaimana budaya organisasi memengaruhi keterbukaan dalam komunikasi risiko? <i>Culture & Behavior:</i> keterbukaan vs tertutup. 6. Apakah ada pelatihan atau sosialisasi mengenai komunikasi risiko? <i>People, Skills & Competencies:</i> program pelatihan. 7. Bagaimana efektivitas komunikasi risiko dievaluasi? <i>Processes:</i> feedback, survei kepuasan komunikasi.			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
10	<i>Direct implementation of the appropriate mechanisms to respond quickly to changing risk and report immediately to appropriate levels of management, supported by agreed principles of escalation (what to report, when, where and how).</i>	Mengarahkan penerapan mekanisme yang tepat untuk merespons perubahan risiko dengan cepat dan segera melaporkannya ke tingkat manajemen yang sesuai, didukung oleh prinsip-prinsip eskalasi yang disepakati (apa yang harus dilaporkan, kapan, di mana, dan bagaimana).	1. Apakah organisasi memiliki mekanisme resmi untuk merespons perubahan risiko I&T secara cepat? <i>Processes:</i> prosedur tanggap risiko. 2. Bagaimana staf melaporkan risiko baru atau perubahan risiko yang muncul? <i>Information Flows:</i> jalur pelaporan resmi. 3. Siapa yang bertugas menerima dan menindaklanjuti laporan risiko baru? <i>Organizational Structures (RACI):</i> pejabat pengelola risiko. 4. Apakah ada prinsip eskalasi / peningkatan yang jelas (apa yang dilaporkan, kapan, kepada siapa)? <i>Policies:</i> pedoman eskalasi. Dokumen rencana tindak lanjut 5. Bagaimana organisasi memastikan laporan risiko segera sampai ke pimpinan terkait? <i>Processes:</i> mekanisme komunikasi cepat. 6. Apakah tersedia media khusus untuk laporan risiko darurat (misalnya <i>hotline</i>, aplikasi <i>internal</i>)?	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Services & Infrastructure:</i> sistem pelaporan. 7. Apakah ada contoh kasus nyata di mana eskalasi risiko berhasil dilakukan dengan cepat? <i>Processes:</i> studi kasus. 8. Bagaimana pimpinan biasanya menanggapi laporan eskalasi risiko? <i>Culture & Behavior:</i> respons pimpinan. 9. Apakah efektivitas mekanisme eskalasi risiko pernah dievaluasi secara formal? <i>Information Items:</i> laporan evaluasi.			
11	<i>Direct that risk, opportunities, issues and concerns may be identified and reported by anyone to the appropriate party at any time. Risk should be managed in accordance with</i>	Mengarahkan agar risiko, peluang, isu, dan kekhawatiran dapat diidentifikasi dan dilaporkan oleh siapa pun kepada pihak yang tepat kapan saja. Risiko harus dikelola sesuai dengan kebijakan dan	1. Apakah ada kebijakan yang memperbolehkan semua pegawai melaporkan risiko atau isu tanpa batasan hierarki? <i>Policies:</i> aturan open reporting. (jelaskan dengan Bahasa di organisasi) 2. Bagaimana staf biasanya menyampaikan risiko, peluang, atau isu yang mereka temukan? <i>Information Flows:</i> jalur komunikasi resmi maupun informal.			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>published policies and procedures and escalated to the relevant decision makers.</i>	prosedur yang dipublikasikan dan dieskalasikan kepada para pengambil keputusan yang relevan.	3. Siapa yang menerima laporan risiko dari staf? <i>Organizational Structures (RACI)</i>: pejabat penerima laporan. 4. Apakah laporan risiko bisa dilakukan secara anonim untuk menghindari hambatan budaya? <i>Culture & Behavior</i>: keberanian/keterbukaan staf. 5. Apakah organisasi menyediakan media resmi untuk laporan terbuka (aplikasi, kotak saran, hotline)? <i>Services & Infrastructure</i>: sarana pelaporan. 6. Apakah ada prosedur bagaimana laporan staf ditindaklanjuti? <i>Processes</i>: alur tindak lanjut. 7. Apakah peluang yang dilaporkan staf juga dipertimbangkan sebagai masukan strategis? <i>Processes</i>: integrasi peluang ke strategi. 8. Apakah ada contoh nyata risiko/isu dari staf yang berhasil mencegah masalah besar di organisasi? <i>Information Items</i>: catatan kasus.			
12	<i>Identify key goals and</i>	Mengidentifikasi tujuan	1. Apakah organisasi memiliki tujuan utama yang jelas	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>metrics of the risk governance and management processes to be monitored, and approve the approaches, methods, techniques and processes for capturing and reporting the measurement information.</i>	dan metrik utama dari proses tata kelola dan manajemen risiko yang akan dipantau, dan menyetujui pendekatan, metode, teknik, dan proses untuk menangkap dan melaporkan informasi pengukuran.	untuk tata kelola risiko I&T? <i>Policies:</i> dokumen tujuan risiko. 2. Bagaimana indikator keberhasilan manajemen risiko I&T ditentukan? <i>Processes:</i> penetapan KPI. 3. Siapa yang menyetujui metrik dan indikator risiko yang digunakan? <i>Organizational Structures (RACI):</i> pimpinan, komite risiko. 4. Apakah ada metode formal untuk mengukur kinerja manajemen risiko? <i>Processes:</i> teknik pengukuran, audit. 5. Bagaimana informasi hasil pengukuran risiko disampaikan ke pimpinan? <i>Information Flows:</i> laporan kinerja. 6. Apakah organisasi menggunakan sistem/ <i>tools</i> untuk mengumpulkan data metrik risiko? <i>Services & Infrastructure:</i> aplikasi monitoring. 7. Bagaimana pimpinan menilai apakah indikator risiko			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			sesuai dengan tujuan strategis? <i>Culture & Behavior</i>: kesadaran pimpinan. 8. Apakah hasil <i>monitoring</i> indikator risiko terdokumentasi secara rutin? <i>Information Items</i>: laporan bulanan, tahunan. 9. Apakah metrik risiko pernah direvisi karena dianggap tidak relevan? <i>Processes</i>: siklus perbaikan metrik.			
EDM03.03 Monitor risk management (Memantau manajemen risiko).						
13	<i>Report any risk management issues to the board or executive committee.</i>	Melaporkan setiap permasalahan terkait manajemen risiko kepada Dewan Komisaris atau komite eksekutif.	1. Apakah organisasi memiliki mekanisme resmi untuk melaporkan masalah manajemen risiko ke pimpinan/komite eksekutif? <i>Policies</i>: aturan pelaporan risiko. 2. Siapa yang bertanggung jawab menyusun laporan masalah manajemen risiko ke pimpinan? <i>Organizational Structures (RACI)</i>: Bidang Telematika, Kepala Dinas. 3. Bagaimana laporan masalah manajemen risiko biasanya disampaikan? (tertulis, presentasi, rapat)	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Information Flows</i> : media komunikasi. 4. Apakah laporan masalah manajemen risiko terdokumentasi secara formal? <i>Information Items</i> : notulen, laporan resmi. 5. Bagaimana sikap pimpinan saat menerima laporan masalah manajemen risiko? <i>Culture & Behavior</i> : keseriusan pimpinan menindaklanjuti.			
14	<i>Monitor the extent to which the risk profile is managed within the enterprise's risk appetite and tolerance thresholds.</i>	Memantau sejauh mana profil risiko dikelola dalam selera risiko dan ambang batas toleransi perusahaan.	1. Apakah organisasi memantau apakah profil risiko I&T sesuai dengan <i>risk appetite</i> dan <i>tolerance</i> yang telah ditetapkan? <i>Processes</i> : mekanisme monitoring. 2. Siapa yang memantau kesesuaian profil risiko terhadap <i>risk appetite</i> ? <i>Organizational Structures (RACI)</i> : pejabat <i>risk owner</i> . 3. Apakah ada sistem/ <i>tools</i> yang digunakan untuk memantau profil risiko? <i>Services & Infrastructure</i> : aplikasi <i>monitoring</i> . 4. Bagaimana hasil pemantauan disampaikan ke	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			pimpinan? <i>Information Flows</i>: laporan periodik. 5. Apakah profil risiko pernah melebihi batas appetite atau tolerance? <i>Information Items</i>: bukti laporan pelanggaran. 6. Bagaimana budaya organisasi ketika terjadi pelanggaran <i>risk appetite/tolerance</i>? <i>Culture & Behavior</i>: reaksi staf/pimpinan. 7. Apakah hasil monitoring digunakan untuk memperbarui strategi risiko I&T? <i>Processes</i>: siklus perbaikan.			
15	<i>Monitor key goals and metrics of risk governance and management processes against targets, analyze the cause of any deviations, and initiate remedial</i>	Memantau tujuan dan metrik utama tata kelola risiko dan proses manajemen terhadap target, menganalisis penyebab penyimpangan, dan mengambil tindakan	1. Apakah organisasi memiliki target jelas untuk tujuan dan metrik tata kelola risiko I&T? <i>Policies</i>: dokumen KPI risiko. 2. Bagaimana kinerja tata kelola risiko I&T dipantau dan dibandingkan terhadap terhadap target? <i>Processes</i>: metode <i>monitoring</i>. 3. Siapa yang melakukan analisis jika ada penyimpangan dari target?	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>actions to address the underlying causes.</i>	perbaikan untuk mengatasi penyebab yang mendasarinya.	<i>Organizational Structures (RACI):</i> unit analisis, pimpinan. 4. Apakah hasil monitoring metrik risiko terdokumentasi? <i>Information Items:</i> laporan kinerja risiko. 5. Apakah penyebab penyimpangan risiko biasanya dicatat dan dianalisis? <i>Processes: root cause analysis.</i> 6. Bagaimana budaya pimpinan saat membahas penyimpangan risiko? Apakah mencari solusi atau menyalahkan? <i>Culture & Behavior:</i> sikap pimpinan. 7. Apakah organisasi memiliki prosedur untuk tindakan korektif bila metrik risiko menyimpang jauh dari target? <i>Policies:</i> pedoman tindakan korektif. 8. Apakah remedial action pernah berhasil mengembalikan kinerja risiko ke target? <i>Processes:</i> contoh nyata <i>corrective action</i>.			
16	<i>Enable key</i>	Memungkinkan	1. Apakah pemangku kepentingan (internal maupun	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>stakeholders' review of the enterprise's progress toward identified goals.</i>	peninjauan oleh pemangku kepentingan utama atas kemajuan perusahaan terhadap tujuan yang telah ditetapkan.	eksternal) dilibatkan dalam peninjauan kemajuan pencapaian tujuan risiko I&T? <i>Organizational Structures (RACI):</i> pemangku kepentingan utama. 2. Apakah ada forum khusus untuk melakukan peninjauan bersama pemangku kepentingan? <i>Processes:</i> rapat evaluasi, forum koordinasi. 3. Bagaimana hasil peninjauan pemangku kepentingan didokumentasikan? <i>Information Items:</i> notulen, laporan hasil peninjauan 4. Apakah masukan pemangku kepentingan digunakan untuk memperbaiki manajemen risiko I&T? <i>Processes:</i> siklus perbaikan. 5. Bagaimana budaya organisasi dalam menerima masukan dari pemangku kepentingan? <i>Culture & Behavior:</i> keterbukaan terhadap kritik. 6. Apakah organisasi menggunakan laporan khusus untuk menunjukkan progres kepada pemangku kepentingan?			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Information Flows: laporan publik, dashboard.</i>			

Tujuan						
<i>Integrate the management of I&T-related enterprise risk with overall enterprise risk management (ERM) and balance the costs and benefits of managing I&T-related enterprise risk.</i>			Mengintegrasikan pengelolaan risiko perusahaan terkait I&T dengan manajemen risiko perusahaan (ERM) secara keseluruhan dan seimbangkan biaya dan manfaat pengelolaan risiko perusahaan terkait I&T.			

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
APO12.01 Collect data (Mengumpulkan data).						
1	Establish and maintain a method for the collection, classification and analysis of I&T risk-related data.	Membangun dan memelihara metode untuk pengumpulan, klasifikasi, dan analisis data terkait risiko I&T.	1. Apakah organisasi memiliki metode resmi untuk mengumpulkan dan menganalisis data risiko I&T ? Policies: SOP atau pedoman resmi pengumpulan risiko 2. Apakah klasifikasi data risiko sudah ditetapkan (misalnya insiden keamanan, downtime, kesalahan manusia)? Processes: mekanisme klasifikasi risiko	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			3. Bagaimana prosedur memastikan data yang dikumpulkan valid dan konsisten? <i>Processes:</i> verifikasi data risiko 4. Apakah metode ini didokumentasikan dalam bentuk SOP atau pedoman resmi? <i>Information Items:</i> dokumen SOP, pedoman risiko			
2	<i>Record relevant and significant I&T risk-related data on the enterprise's internal and external operating environment.</i>	Mencatat data risiko I&T yang relevan dan signifikan pada lingkungan operasi internal dan eksternal perusahaan.	1. Jenis data risiko I&T apa saja yang biasanya dicatat (internal vs eksternal)? <i>Information Items:</i> risk log, laporan eksternal 2. Apakah ada format baku untuk pencatatan data risiko? <i>Policies:</i> format standar pencatatan risiko 3. Siapa yang biasanya mencatat data risiko I&T? <i>Organizational Structures:</i> staf Bidang Telematika / manajemen risiko 4. Bagaimana data eksternal (misalnya regulasi pemerintah, tren industri) ikut didokumentasikan? <i>Processes:</i> integrasi data eksternal ke pencatatan	R		
3	<i>Adopt or define a risk taxonomy for</i>	Mengadopsi atau menetapkan taksonomi	1. Apakah organisasi memiliki taksonomi risiko I&T (misalnya kategori dampak: finansial, reputasi, layanan	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>consistent definitions of risk scenarios and impact and likelihood categories.</i>	risiko untuk definisi skenario risiko dan kategori dampak serta kemungkinan yang konsisten.	publik)? <i>Policies</i>: dokumen taksonomi risiko 2. Apakah kategori risiko dan probabilitasnya konsisten dipakai semua bidang? <i>Processes</i>: penerapan klasifikasi risiko 3. Bagaimana taksonomi risiko ini dikomunikasikan kepada staf yang terlibat? <i>Information Flows</i>: sosialisasi taksonomi risiko 4. Apakah pernah ada revisi/penyesuaian taksonomi risiko? <i>Culture & Behavior</i>: kesadaran untuk memperbarui taksonomi			
4	<i>Record data on risk events that have caused or may cause business impacts as per the impact categories defined in the risk taxonomy.</i>	Mencatat data tentang peristiwa risiko yang telah menyebabkan atau mungkin menyebabkan dampak bisnis sesuai kategori dampak yang ditetapkan dalam	1. Apakah insiden risiko I&T (<i>downtime</i>, serangan siber) selalu dicatat sesuai kategori dampak? <i>Processes</i>: pencatatan insiden sesuai kategori risiko 2. Apakah ada integrasi data dari laporan insiden, problem, atau investigasi? <i>Information Items</i>: laporan insiden, investigasi 3. Siapa yang bertanggung jawab memastikan	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>Capture relevant data from related issues, incidents, problems and investigations.</i>	taksonomi risiko. Menangkap data yang relevan dari isu, insiden, masalah, dan investigasi terkait.	pencatatan insiden sesuai kategori risiko? <i>Organizational Structures:</i> tim TI / manajemen risiko 4. Apakah catatan insiden digunakan untuk perbaikan layanan? <i>Processes:</i> <i>feedback loop</i> ke perbaikan layanan			
5	<i>Survey and analyze the historical I&T risk data and loss experience from externally available data and trends, industry peers through industry-based event logs, databases, and industry agreements for common event disclosure.</i>	Melakukan survei dan analisis data risiko I&T historis dan pengalaman kerugian dari data dan tren yang tersedia secara eksternal, rekan industri melalui log peristiwa berbasis industri, basis data, dan perjanjian industri untuk pengungkapan peristiwa umum.	1. Apakah organisasi menganalisis data risiko historis internal? <i>Processes:</i> analisis data historis 2. Apakah data eksternal (tren industri, data asosiasi pemerintah/kominfo) juga digunakan? <i>Information Items:</i> laporan tren eksternal 3. Bagaimana data eksternal dibandingkan dengan kondisi internal organisasi? <i>Processes:</i> benchmarking internal-eksternal 4. Apakah ada contoh perbaikan kebijakan/teknis yang diambil dari analisis tren eksternal? <i>Culture & Behavior:</i> keterbukaan untuk belajar dari eksternal	R		
6	<i>For similar classes of</i>	Untuk kelas kejadian	1. Apakah organisasi mengelompokkan insiden serupa	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>events, organize the collected data and highlight contributing factors. Determine common contributing factors across multiple events.</i>	yang serupa, menyusun data yang terkumpul dan soroti faktor-faktor yang berkontribusi. Tentukan faktor-faktor yang berkontribusi secara umum pada beberapa kejadian.	(misalnya serangan <i>malware</i> berulang)? <i>Processes</i> : klasifikasi insiden serupa 2. Faktor penyebab umum apa saja yang biasanya diidentifikasi? <i>Information Items</i> : catatan faktor penyebab 3. Apakah hasil analisis faktor penyebab digunakan untuk mencegah kejadian serupa? <i>Culture & Behavior</i> : kesadaran mencegah insiden berulang			
7	<i>Determine the specific conditions that existed or were absent when risk events occurred and the way the conditions affected event frequency and loss magnitude.</i>	Menentukan kondisi spesifik yang ada atau tidak ada saat peristiwa risiko terjadi dan cara kondisi tersebut memengaruhi frekuensi peristiwa dan besarnya kerugian.	1. Apakah kondisi tertentu (misalnya kurang staf, beban server tinggi) selalu dicatat saat insiden terjadi? <i>Processes</i> : pencatatan kondisi insiden 2. Bagaimana kondisi tersebut memengaruhi frekuensi kejadian/tingkat kerugian? <i>Information Items</i> : laporan analisis insiden 3. Apakah organisasi melakukan analisis <i>root cause</i> berbasis kondisi lingkungan/operasional? <i>Processes</i> : <i>root cause analysis</i> <i>Root cause</i> = penyebab paling mendasar suatu	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			masalah/insiden, bukan sekadar gejala permukaan.			
8	<i>Perform periodic event and risk factor analysis to identify new or emerging risk issues and to gain an understanding of the associated internal and external risk factors.</i>	Melakukan analisis kejadian dan faktor risiko secara berkala untuk mengidentifikasi masalah risiko baru atau yang muncul dan untuk memperoleh pemahaman tentang faktor risiko internal dan eksternal terkait.	1. Seberapa sering dilakukan analisis risiko I&T berkala? <i>Policies:</i> kebijakan <i>review</i> berkala 2. Siapa yang terlibat dalam analisis berkala ini? <i>Organizational Structures:</i> tim Manajemen Risiko, Bidang Telematika 3. Apakah hasil analisis digunakan untuk memperbarui daftar risiko organisasi? <i>Processes:</i> pembaruan daftar risiko 4. Apakah ada contoh risiko baru yang teridentifikasi dari analisis periodik (misalnya tren <i>ransomware</i>)? <i>Information Items:</i> laporan analisis risiko	R		
APO12.02 Analyze risk (Menganalisis risiko).						
9	<i>Define the appropriate scope of risk analysis efforts, considering all risk factors and/or the business criticality of</i>	Menentukan cakupan upaya analisis risiko yang tepat, dengan mempertimbangkan semua faktor risiko	1. Bagaimana organisasi menentukan lingkup analisis risiko I&T (misalnya hanya pada aplikasi tertentu atau seluruh layanan publik)? <i>Processes:</i> prosedur penetapan lingkup analisis. 2. Siapa yang memutuskan ruang lingkup analisis risiko?	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>assets.</i>	dan/atau kekritisitas aset dalam bisnis.	<i>Organizational Structures (RACI):</i> Kepala Dinas, Bidang Telematika, Tim Manajemen Risiko. 3. Apakah ada kriteria formal untuk memilih aset mana yang dianggap kritis dalam analisis risiko? <i>Policies:</i> pedoman kritikalitas aset. 4. Bagaimana hasil penentuan lingkup analisis risiko didokumentasikan? <i>Information Items:</i> risk analysis scope document.			
10	<i>Build and regularly update I&T risk scenarios; I&T-related loss exposures; and scenarios regarding reputational risk, including compound scenarios of cascading and/or coincidental threat types and events. Develop</i>	Menyusun dan memperbarui skenario risiko I&T secara berkala; paparan kerugian terkait I&T; dan skenario terkait risiko reputasi, termasuk skenario gabungan dari jenis dan peristiwa ancaman yang berjenjang dan/atau	1. Apakah organisasi memiliki daftar atau katalog skenario risiko I&T yang terdokumentasi? <i>Policies:</i> dokumen <i>risk scenario register</i>. Risk scenario = gambaran terstruktur tentang kemungkinan kejadian risiko, dampak, dan penyebabnya. 2. Seberapa sering skenario risiko diperbarui (tahunan, per proyek besar, setelah insiden)? <i>Processes:</i> siklus update skenario. 3. Apakah organisasi pernah menyusun skenario gabungan (contoh: serangan siber + kegagalan	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>expectations for specific control activities and capabilities to detect.</i>	bersamaan. Mengembangkan ekspektasi untuk aktivitas dan kemampuan kontrol tertentu untuk mendeteksi.	infrastruktur jaringan terjadi bersamaan)? <i>Processes</i> : penyusunan skenario multi-event. 4. Siapa yang terlibat dalam penyusunan dan pembaruan skenario risiko I&T? <i>Organizational Structures (RACI)</i> : Bidang Telematika, Kepala Dinas, tim keamanan informasi. 5. Apakah ada metode standar dalam memperkirakan dampak reputasi dari sebuah skenario risiko I&T? <i>Policies</i> : panduan analisis reputasi. 6. Bagaimana informasi dari insiden nyata sebelumnya dipakai untuk memperkaya skenario risiko baru? (sederhanakan bahasanya) <i>Information Items</i> : catatan insiden, laporan audit. 7. Bagaimana organisasi menentukan kontrol apa saja yang harus tersedia untuk setiap skenario risiko? <i>Processes</i> : <i>mapping</i> skenario ke kontrol. <i>Control</i> = mekanisme/prosedur untuk mengurangi atau mendeteksi risiko. 8. Apakah pimpinan atau <i>stakeholder</i> pernah dilibatkan			

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			dalam validasi skenario risiko sebelum dipakai dalam analisis formal? <i>Culture & Behavior</i> : keterlibatan pimpinan, tingkat keseriusan validasi.			
11	<i>Estimate the frequency (or likelihood) and magnitude of loss or gain associated with I&T risk scenarios. Take into account all applicable risk factors and evaluate known operational controls.</i>	Memperkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario risiko I&T. Mempertimbangkan semua faktor risiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.	1. Bagaimana organisasi memperkirakan seberapa sering risiko I&T bisa terjadi? <i>Processes</i> : metode estimasi frekuensi. 2. Bagaimana memperkirakan besarnya kerugian (atau keuntungan) bila risiko terjadi? <i>Information Items</i> : data historis, perhitungan biaya. 3. Apakah faktor-faktor risiko eksternal (misalnya regulasi, tren siber) ikut dipertimbangkan? <i>Policies</i> : pedoman analisis risiko. 4. Bagaimana pengendalian yang ada dievaluasi saat memperkirakan dampak risiko? <i>Processes</i> : evaluasi kontrol.	R		
12	<i>Compare current risk</i>	Membandingkan risiko	1. Apakah organisasi pernah membandingkan profil	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>(I&T-related loss exposure) to risk appetite and acceptable risk tolerance. Identify unacceptable or elevated risk.</i>	saat ini (paparan kerugian terkait I&T) dengan selera risiko dan toleransi risiko yang dapat diterima. Mengidentifikasi risiko yang tidak dapat diterima atau tinggi.	risiko saat ini dengan risk appetite yang sudah ditetapkan? <i>Processes: risk profile vs appetite.</i> 2. Siapa yang berwenang menyatakan risiko melebihi batas <i>appetite/tolerance</i>? <i>Organizational Structures (RACI):</i> pimpinan, komite risiko. 3. Apakah ada format laporan resmi untuk menyampaikan risiko yang tidak dapat diterima? <i>Information Items:</i> laporan eksposur risiko. 4. Bagaimana pimpinan menindaklanjuti risiko yang melebihi toleransi? <i>Culture & Behavior:</i> reaksi pimpinan terhadap pelanggaran batas.			
13	<i>Propose risk responses for risk exceeding risk appetite and tolerance levels.</i>	Mengusulkan respons risiko untuk risiko yang melampaui selera risiko dan tingkat toleransi.	1. Bagaimana organisasi menentukan opsi respons (menghindari, mengurangi, transfer, menerima)? <i>Processes: risk response planning.</i> 2. Siapa yang berwenang mengusulkan atau memilih	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			opsi respons risiko? <i>Organizational Structures (RACI):</i> pimpinan, tim manajemen risiko. 3. Apakah ada dokumen yang mencatat usulan respons risiko? <i>Information Items: risk response proposal.</i> 4. Bagaimana respons risiko disesuaikan dengan kebijakan organisasi? <i>Policies: pedoman respons risiko.</i>			
14	<i>Specify high-level requirements for projects or programs that will implement the selected risk responses. Identify requirements and expectations for appropriate key controls for risk</i>	Menetapkan persyaratan tingkat tinggi untuk proyek atau program yang akan menerapkan respons risiko yang dipilih. Identifikasi persyaratan dan harapan untuk kontrol utama yang sesuai untuk respons mitigasi risiko.	1. Bagaimana organisasi menentukan proyek/program untuk mengurangi risiko I&T? <i>Processes: perencanaan proyek mitigasi.</i> 2. Apakah ada dokumen resmi yang menjelaskan kebutuhan & harapan kontrol utama? <i>Information Items: project charter, TOR, Business Case</i> Project Charter = dokumen awal proyek yang memuat tujuan, scope, risiko, dan high-level requirement. TOR (Terms of Reference) = dokumen yang menjelaskan detail kebutuhan, ruang lingkup, dan harapan dari suatu	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>mitigation responses.</i>		program/proyek. Dokumen <i>Business Case</i> = justifikasi proyek, sering kali berisi requirement kontrol risiko. 3. Siapa yang menyetujui requirement mitigasi risiko I&T? <i>Organizational Structures (RACI)</i>: pimpinan proyek, Kepala Dinas. 4. Bagaimana requirement tersebut dikomunikasikan ke tim pelaksana? <i>Information Flows</i>: rapat, dokumen tertulis.			
15	<i>Validate the risk analysis and business impact analysis (BIA) results before using them in decision making. Confirm that the analysis aligns with enterprise</i>	Memvalidasi hasil analisis risiko dan analisis dampak bisnis (BIA) sebelum menggunakannya dalam pengambilan keputusan. Pastikan analisis tersebut sesuai dengan	1. Apakah hasil analisis risiko/BIA pernah diverifikasi ulang sebelum dipakai untuk keputusan? <i>Processes</i>: validasi analisis. BIA = analisis dampak bisnis, menilai seberapa parah dampak jika layanan terganggu. 2. Siapa yang melakukan validasi hasil analisis risiko? <i>Organizational Structures (RACI)</i>: tim independen, pimpinan.	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>requirements and verify that estimations were properly calibrated and scrutinized for bias.</i>	persyaratan perusahaan dan verifikasi bahwa estimasi telah dikalibrasi dengan benar dan diteliti untuk mengetahui biasnya.	3. Bagaimana memastikan hasil analisis bebas bias? <i>Policies:</i> prinsip validasi objektif. 4. Apakah ada bukti dokumentasi validasi (notulen, laporan)? <i>Information Items:</i> dokumen validasi.			
16	<i>Analyze cost/benefit of potential risk response options such as avoid, reduce/mitigate, transfer/share, and accept and exploit/seize. Confirm the optimal risk response.</i>	Menganalisis biaya/manfaat dari opsi respons risiko potensial seperti menghindari, mengurangi/meringankan, mentransfer/membagi, dan menerima serta memanfaatkan/merebut. Mengonfirmasikan respons risiko yang optimal.	1. Apakah organisasi memiliki prosedur formal dalam membandingkan biaya dan manfaat dari berbagai opsi respons risiko? <i>Policies:</i> pedoman analisis <i>cost and benefit</i> . 2. Bagaimana cara organisasi menilai manfaat dari suatu respons risiko (misalnya pengurangan <i>downtime</i> , peningkatan kepercayaan publik)? <i>Processes:</i> metode analisis manfaat. 3. Apakah ada standar atau indikator keuangan yang digunakan dalam menghitung biaya (contoh: ROI, <i>payback period</i>)? <i>Information Items:</i> laporan keuangan, proyeksi biaya. 4. Siapa yang biasanya memutuskan opsi respons risiko	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			yang dipilih (misalnya Kepala Dinas, komite risiko, atau bagian keuangan)? <i>Organizational Structures (RACI):</i> pengambil keputusan. 5. Bagaimana organisasi memastikan bahwa opsi respons risiko yang dipilih sesuai dengan <i>risk appetite</i> dan <i>tolerance</i> yang berlaku? <i>Processes: alignment</i> dengan <i>risk appetite</i>. 6. Apakah organisasi pernah menggunakan pendekatan transfer risiko (misalnya asuransi, outsourcing) dan bagaimana analisis biayanya dibanding mitigasi internal? <i>Processes:</i> evaluasi opsi transfer. 7. Apakah budaya organisasi cenderung lebih memilih menghindari risiko (<i>risk averse</i>) atau berani mengambil risiko untuk peluang strategis (<i>risk seeking</i>)? <i>Culture & Behavior:</i> sikap organisasi terhadap risiko. 8. Apakah hasil analisis <i>cost/benefit</i> didokumentasikan dan dilaporkan secara formal untuk mendukung			

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			keputusan manajemen? <i>Information Flows</i> : laporan analisis risiko ke pimpinan.			
APO12.03 Maintain a risk profile (Memelihara profile risiko).						
17	<i>Inventory business processes and document their dependency on I&T service management processes and IT infrastructure resources. Identify supporting personnel, applications, infrastructure, facilities, critical manual records, vendors, suppliers and outsourcers.</i>	Menginventarisasi proses bisnis dan dokumentasikan ketergantungannya pada proses manajemen layanan I&T dan sumber daya infrastruktur I&T. Mengidentifikasi personel pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan pihak yang melakukan alih daya.	1. Apakah organisasi memiliki inventaris proses bisnis yang terdokumentasi? <i>Information Items</i> : dokumen inventaris proses bisnis. 2. Bagaimana ketergantungan proses bisnis pada sistem I&T dicatat? <i>Processes</i> : pemetaan <i>dependency</i> . 3. Apakah personel pendukung, aplikasi, infrastruktur, vendor juga dicatat dalam inventaris ini? <i>Policies</i> : aturan kelengkapan inventaris. 4. Siapa yang bertanggung jawab memelihara inventaris tersebut? <i>Organizational Structures (RACI)</i> : Bidang Telematika, unit perencanaan.			
18	<i>Determine and agree</i>	Menentukan dan	1. Bagaimana organisasi menentukan layanan I&T mana	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>on which I&T services and IT infrastructure resources are essential to sustain the operation of business processes. Analyze dependencies and identify weak links.</i>	menyetujui layanan I&T dan sumber daya infrastruktur I&T mana yang penting untuk mempertahankan operasi proses bisnis. Menganalisis ketergantungan dan mengidentifikasi titik lemah.	yang sangat kritis untuk layanan publik? <i>Processes:</i> analisis layanan esensial. 2. Apakah ada dokumen resmi yang menyatakan layanan/infrastruktur esensial? <i>Information Items:</i> daftar layanan kritis, BCP. 3. Siapa yang menyetujui daftar layanan/infrastruktur esensial? <i>Organizational Structures (RACI):</i> pimpinan, manajemen risiko. 4. Bagaimana titik lemah dalam ketergantungan layanan dianalisis? <i>Processes:</i> weak link analysis.			
19	<i>Aggregate current risk scenarios by category, business line and functional area.</i>	Mengumpulkan skenario risiko saat ini berdasarkan kategori, lini bisnis, dan area fungsional.	1. Apakah skenario risiko I&T pernah dikategorikan (contoh: operasional, keamanan data, layanan publik)? <i>Processes:</i> risk categorization. 2. Bagaimana skenario risiko dikonsolidasikan lintas unit? <i>Information Flows:</i> laporan konsolidasi. 3. Siapa yang menyetujui agregasi risiko lintas fungsi?	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Organizational Structures (RACI):</i> komite risiko, pimpinan.			
20	<i>Regularly capture all risk profile information and consolidate it into an aggregated risk profile.</i>	Secara berkala menangkap semua informasi profil risiko dan menggabungkannya menjadi profil risiko agregat.	1. Bagaimana organisasi menyatukan seluruh informasi risiko ke dalam profil risiko terkini? <i>Processes:</i> konsolidasi profil risiko. 2. Apakah ada sistem/ <i>tools</i> yang digunakan untuk mengelola profil risiko? <i>Services & Infrastructure:</i> aplikasi GRC, <i>spreadsheet</i> , dsb. 3. Bagaimana hasil konsolidasi dibagikan ke <i>stakeholder</i> ? <i>Information Flows:</i> laporan <i>risk profile</i> .	R		
21	<i>Capture information on the status of the risk action plan for inclusion in the I&T risk profile of the enterprise.</i>	Menangkap informasi tentang status rencana tindakan risiko untuk dimasukkan dalam profil risiko I&T perusahaan.	1. Apakah setiap tindakan mitigasi risiko memiliki <i>action plan</i> resmi? <i>Policies:</i> pedoman penyusunan <i>action plan</i> . 2. Bagaimana status pelaksanaan <i>action plan</i> dipantau? <i>Processes:</i> monitoring rencana aksi. 3. Siapa yang bertanggung jawab melaporkan progres <i>action plan</i> ?	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			Organizational Structures (RACI): pemilik risiko, pimpinan unit.			
22	Based on all risk profile data, define a set of risk indicators that allow the quick identification and monitoring of current risk and risk trends.	Berdasarkan semua data profil risiko, tentukan serangkaian indikator risiko yang memungkinkan identifikasi dan pemantauan cepat risiko terkini dan tren risiko.	1. Apakah organisasi memiliki indikator risiko utama (KRI) untuk memantau tren risiko? <i>Policies:</i> definisi KRI. 2. Bagaimana KRI ditentukan dari data profil risiko? <i>Processes:</i> metode penetapan indikator. 3. Apakah indikator risiko digunakan secara rutin dalam rapat pimpinan? <i>Information Items:</i> laporan KRI. 4. Siapa yang menyetujui indikator risiko sebelum digunakan? <i>Organizational Structures (RACI):</i> pimpinan, komite risiko. KRI (Key Risk Indicator) = indikator pengukuran kuantitatif atau kualitatif yang digunakan organisasi	R		
23	Capture information on I&T risk events that have materialized for	Menangkap informasi tentang peristiwa risiko I&T yang telah terwujud	1. Apakah organisasi memiliki catatan formal untuk insiden atau peristiwa risiko I&T? <i>Information Items:</i> log insiden, laporan keamanan.	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>inclusion in the IT risk profile of the enterprise.</i>	untuk dimasukkan dalam profil risiko I&T perusahaan.	2. Bagaimana data insiden dikumpulkan (manual, sistem otomatis)? <i>Processes:</i> mekanisme pencatatan insiden. 3. Siapa yang bertanggung jawab melaporkan insiden risiko I&T? <i>Organizational Structures (RACI):</i> unit operasional, helpdesk TI.			
APO12.04 Articulate risk (Mengartikulasikan Risiko).						
24	<i>Report the results of risk analysis to all affected stakeholders in terms and formats useful to support enterprise decisions. Whenever possible, include probabilities and ranges of loss or gain along with confidence levels, to</i>	Melaporkan hasil analisis risiko kepada semua pemangku kepentingan yang terpengaruh dalam bentuk dan format yang berguna untuk mendukung keputusan perusahaan. Jika memungkinkan, sertakan probabilitas	1. Bagaimana hasil analisis risiko disampaikan ke <i>stakeholder</i> ? <i>Information Flows:</i> laporan, <i>dashboard</i> . 2. Apakah laporan analisis risiko mencantumkan probabilitas dan range kerugian? <i>Information Items:</i> format laporan risiko. 3. Siapa yang meninjau laporan analisis risiko sebelum didistribusikan? <i>Organizational Structures (RACI):</i> pimpinan, tim analisis.	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>enable management to balance risk-return.</i>	dan rentang kerugian atau keuntungan beserta tingkat keyakinan, untuk memungkinkan manajemen menyeimbangkan risiko-imbal hasil.				
25	<i>Provide decision makers with an understanding of worst-case and most-probable scenarios, I&T-related loss exposures and significant reputation, legal and regulatory considerations, or any other impact category as per the risk</i>	Memberikan para pengambil keputusan pemahaman tentang skenario terburuk dan paling mungkin, paparan kerugian terkait I&T, serta reputasi signifikan, pertimbangan hukum dan peraturan, atau kategori dampak lainnya sesuai taksonomi risiko.	1. Bagaimana pengambil keputusan mendapat gambaran skenario terburuk/terbaik dari risiko I&T? <i>Processes: briefing risiko.</i> 2. Apakah aspek reputasi, hukum, dan regulasi juga disampaikan dalam laporan risiko? <i>Policies: pedoman laporan risiko.</i> 3. Bagaimana kejelasan laporan disesuaikan dengan kebutuhan pimpinan? <i>Culture & Behavior: komunikasi yang dipahami non-teknis.</i>	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>taxonomy.</i>					
26	<i>Report the current risk profile to all stakeholders. Include information on the effectiveness of the risk management process, control effectiveness, gaps, inconsistencies, redundancies, remediation status and their impacts on the risk profile.</i>	Melaporkan profil risiko terkini kepada semua pemangku kepentingan. Sertakan informasi tentang efektivitas proses manajemen risiko, efektivitas pengendalian, kesenjangan, inkonsistensi, redundansi, status perbaikan, dan dampaknya terhadap profil risiko.	1. Apakah organisasi secara rutin melaporkan profil risiko terkini ke <i>stakeholder</i> ? <i>Processes</i> : siklus pelaporan risiko. 2. Apa saja informasi yang disertakan (efektivitas kontrol, kesenjangan, status remediasi)? <i>Information Items</i> : laporan profil risiko. 3. Siapa yang menerima laporan profil risiko? <i>Organizational Structures (RACI)</i> : pimpinan, <i>auditor</i> , <i>regulator</i> .	R		
27	<i>On a periodic basis, for areas with relative risk and risk capacity parity, identify I&T-</i>	Secara berkala, untuk area dengan risiko relatif dan paritas kapasitas risiko, mengidentifikasi	1. Apakah organisasi pernah mengidentifikasi peluang I&T saat risiko relatif rendah? <i>Processes</i> : analisis peluang risiko. 2. Bagaimana peluang tersebut dievaluasi terhadap	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>related opportunities that would allow the acceptance of greater risk and enhanced growth and return.</i>	peluang terkait I&T yang akan memungkinkan penerimaan risiko lebih besar dan peningkatan pertumbuhan dan laba.	kapasitas risiko organisasi? <i>Policies:</i> pedoman evaluasi peluang. 3. Apakah ada contoh peluang I&T yang dimanfaatkan untuk pertumbuhan? <i>Information Items:</i> studi kasus peluang.			
28	<i>Review the results of objective third-party assessments and internal audit and quality assurance reviews. Include them in the risk profile. Review identified gaps and I&T-related loss exposures to determine the need for additional risk analysis.</i>	Meninjau hasil penilaian pihak ketiga yang objektif dan tinjauan audit internal serta jaminan kualitas. Sertakan hasil tersebut dalam profil risiko. Tinjau kesenjangan yang teridentifikasi dan paparan kerugian terkait I&T untuk menentukan perlunya analisis risiko tambahan.	1. Apakah hasil audit eksternal/asesmen pihak ketiga dimasukkan ke dalam profil risiko? <i>Processes:</i> integrasi hasil audit. 2. Bagaimana kesenjangan yang ditemukan ditindaklanjuti? <i>Processes:</i> corrective action. 3. Siapa yang meninjau hasil asesmen tersebut? <i>Organizational Structures (RACI):</i> pimpinan, auditor internal.	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
APO12.05 Define a risk management action portfolio (Menentukan portofolio tindakan manajemen risiko).						
29	<i>Maintain an inventory of control activities that are in place to mitigate risk and that enable risk to be taken in line with the risk appetite and tolerance. Classify control activities and map them to specific I&T risk scenarios and aggregations of I&T risk scenarios.</i>	Memelihara inventaris aktivitas pengendalian yang ada untuk mengurangi risiko dan yang memungkinkan risiko ditangani sesuai dengan selera dan toleransi risiko. Mengklasifikasikan aktivitas pengendalian dan memetakannya ke skenario risiko I&T tertentu dan agregasi skenario risiko I&T.	1. Apakah organisasi memiliki daftar resmi kontrol mitigasi risiko? <i>Information Items: control inventory.</i> 2. Bagaimana kontrol diklasifikasikan dan dipetakan ke skenario risiko? <i>Processes: kontrol mapping.</i> 3. Siapa yang bertanggung jawab memperbarui inventaris kontrol? <i>Organizational Structures (RACI): tim pengendalian internal, Bidang Telematika.</i>	R		
30	<i>Determine whether each organizational entity monitors risk and accepts</i>	Menentukan apakah setiap entitas organisasi memantau risiko dan menerima akuntabilitas	1. Apakah tiap unit organisasi diminta memantau risiko sendiri? <i>Policies: aturan akuntabilitas risiko.</i> 2. Bagaimana akuntabilitas risiko dibuktikan?	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>accountability for operating within its individual and portfolio tolerance levels.</i>	untuk beroperasi dalam tingkat toleransi individu dan portofolionya.	<i>Information Items:</i> laporan risiko unit. 3. Siapa yang menilai apakah unit sudah sesuai toleransi? <i>Organizational Structures (RACI):</i> manajemen risiko, pimpinan.			
31	<i>Define a balanced set of project proposals designed to reduce risk and/or projects that enable strategic enterprise opportunities, considering costs, benefits, effect on current risk profile and regulations.</i>	Menentukan serangkaian proposal proyek yang seimbang yang dirancang untuk mengurangi risiko dan/atau proyek yang memungkinkan peluang perusahaan strategis, dengan mempertimbangkan biaya, manfaat, dampak pada profil risiko dan peraturan saat ini.	4. Bagaimana organisasi menilai proyek mitigasi risiko vs proyek peluang? <i>Processes:</i> penilaian biaya-manfaat proyek. 5. Apakah biaya, manfaat, dan regulasi dijadikan pertimbangan formal? <i>Policies:</i> pedoman seleksi proyek. 6. Siapa yang memutuskan proposal proyek mana yang dijalankan? <i>Organizational Structures (RACI):</i> pimpinan, tim perencanaan.	R		

APO12 Managed Risk					
No. Akt	Aspek yang Diuji			Butir Penilaian	
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR
APO12.06 Respond to risk (Menanggapi risiko).					
32	<i>Prepare, maintain and test plans that document the specific steps to take when a risk event may cause a significant operational or development incident with serious business impact. Ensure that plans include pathways of escalation across the enterprise.</i>	Menyiapkan, memelihara, dan menguji rencana yang mendokumentasikan langkah-langkah spesifik yang harus diambil ketika suatu peristiwa risiko dapat menyebabkan insiden operasional atau pengembangan yang signifikan dengan dampak bisnis yang serius. Pastikan bahwa rencana tersebut mencakup jalur eskalasi di seluruh perusahaan.	1. Apakah organisasi memiliki dokumen rencana penanganan insiden risiko I&T yang formal? <i>Policies: disaster recovery plan (DRP), business continuity plan (BCP).</i> 2. Bagaimana rencana penanganan insiden tersebut disusun? Apakah ada prosedur baku? <i>Processes: mekanisme penyusunan rencana.</i> 3. Siapa yang terlibat dalam penyusunan dan pemeliharaan rencana ini? <i>Organizational Structures (RACI):</i> tim TI, pimpinan, manajemen risiko, pihak eksternal. 4. Apakah rencana ini secara berkala diuji melalui simulasi/drill? Jika ya, seberapa sering? <i>Processes: uji coba dan review periodik.</i> 5. Apakah tersedia jalur eskalasi resmi bila insiden signifikan terjadi (contoh: siapa yang dihubungi pertama, siapa yang memberi keputusan)? <i>Information Flows: diagram eskalasi, SOP eskalasi.</i>	R	

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			6. Apakah ada sarana/infrastruktur khusus untuk mendukung eksekusi rencana (misalnya backup site, hotline darurat)? <i>Services & Infrastructure:</i> fasilitas pendukung. 7. Bagaimana budaya staf dan pimpinan dalam mengikuti simulasi atau uji coba rencana (serius, formalitas, atau kurang antusias)? <i>Culture & Behavior:</i> keterlibatan dalam simulasi. 8. Apakah hasil uji coba rencana (misalnya drill bencana I&T) selalu didokumentasikan dan dipakai untuk perbaikan rencana berikutnya? <i>Information Items:</i> laporan hasil <i>drill</i>, <i>corrective action</i>.			
33	<i>Apply the appropriate response plan to minimize the impact when risk incidents occur.</i>	Menerapkan rencana respons yang tepat untuk meminimalkan dampak saat insiden risiko terjadi.	1. Apakah organisasi pernah benar-benar menerapkan rencana respons risiko I&T saat terjadi insiden besar (misalnya server <i>down</i>, kebocoran data)? <i>Information Items:</i> laporan insiden, catatan tindak lanjut. 2. Siapa yang biasanya mengambil keputusan utama ketika insiden risiko terjadi? <i>Organizational Structures (RACI):</i> Kepala Dinas,	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			Bidang Telematika, tim tanggap darurat. 3. Bagaimana proses koordinasi antar-unit dilakukan saat rencana respons dijalankan? <i>Processes:</i> mekanisme koordinasi lintas unit. 4. Apakah tersedia sarana pendukung untuk memfasilitasi eksekusi respons (contoh: sistem monitoring <i>real-time</i>, ruang kendali)? <i>Services & Infrastructure:</i> tools dan fasilitas darurat. 5. Bagaimana budaya staf saat menghadapi insiden – apakah tenang dan mengikuti prosedur, atau panik dan improvisasi? <i>Culture & Behavior:</i> reaksi nyata staf/pimpinan. 6. Apakah hasil penerapan rencana respons dievaluasi untuk memperbaiki SOP atau prosedur yang ada? <i>Processes:</i> siklus pembelajaran pasca-insiden.			
34	<i>Categorize incidents and compare I&T-related loss exposures against risk tolerance</i>	Mengategorikan insiden dan bandingkan paparan kerugian terkait I&T terhadap ambang batas	1. Apakah insiden I&T (misalnya <i>downtime</i> aplikasi, serangan siber, kebocoran data) dikategorikan secara resmi menurut tingkat keparahan? <i>Policies:</i> SOP kategorisasi insiden.	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>thresholds. Communicate business impacts to decision makers as part of reporting and update the risk profile.</i>	toleransi risiko. Komunikasikan dampak bisnis kepada para pengambil keputusan sebagai bagian dari pelaporan dan perbarui profil risiko.	2. Bagaimana organisasi menentukan apakah suatu insiden sudah melewati ambang batas toleransi risiko? <i>Processes:</i> mekanisme penilaian toleransi. 3. Siapa yang berwenang melakukan validasi kategori insiden dan memutuskan langkah eskalasi? <i>Organizational Structures (RACI):</i> pejabat <i>risk owner</i> , Kepala Dinas, tim TI. 4. Apakah hasil perbandingan insiden dengan toleransi risiko terdokumentasi dan masuk ke profil risiko organisasi? <i>Information Items:</i> <i>risk register</i> , laporan insiden. 5. Bagaimana dampak bisnis dari insiden I&T dikomunikasikan kepada pengambil keputusan? <i>Information Flows:</i> laporan resmi, rapat pimpinan, <i>dashboard</i> . 6. Bagaimana budaya organisasi dalam menyikapi insiden yang melewati toleransi risiko, apakah terbuka membahasnya atau cenderung menutupinya? <i>Culture & Behavior:</i> keterbukaan pimpinan/staf.			

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
35	<i>Examine past adverse events/losses and missed opportunities and determine root causes.</i>	Memeriksa kejadian/kerugian buruk di masa lalu dan kesempatan yang hilang, serta menentukan akar penyebabnya.	1. Apakah organisasi memiliki catatan resmi terkait insiden atau kerugian I&T di masa lalu (misalnya <i>downtime</i> panjang, kebocoran data, proyek I&T gagal)? <i>Information Items</i>: laporan insiden, audit, <i>lessons learned</i>. 2. Bagaimana organisasi menganalisis akar penyebab (<i>root cause</i>) dari insiden atau kerugian tersebut? <i>Processes</i>: metode <i>root cause analysis</i> (misalnya <i>fishbone</i>, <i>5-why</i>). 3. Siapa saja yang biasanya dilibatkan dalam proses investigasi akar penyebab insiden I&T? <i>Organizational Structures (RACI)</i>: tim TI, manajemen risiko, pimpinan. 4. Apakah ada prosedur formal untuk melakukan evaluasi pasca-insiden (<i>post-mortem review</i>)? <i>Policies</i>: SOP evaluasi insiden. 5. Apakah faktor eksternal (regulasi, vendor, cuaca, tren industri) juga dipertimbangkan dalam analisis kerugian masa lalu?	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Processes:</i> analisis faktor eksternal. 6. Bagaimana budaya organisasi dalam menyikapi insiden masa lalu, apakah terbuka mencari solusi atau cenderung menyalahkan pihak tertentu? <i>Culture & Behavior:</i> sikap staf/pimpinan. 7. Apakah hasil analisis insiden masa lalu digunakan sebagai bahan pembelajaran untuk memperbaiki kebijakan atau SOP? <i>Processes:</i> siklus perbaikan berkelanjutan.			
36	<i>Communicate root cause, additional risk response requirements and process improvements to appropriate decision makers. Ensure that the cause, response requirements and process improvement</i>	Mengomunikasikan akar permasalahan, persyaratan respons risiko tambahan, dan perbaikan proses kepada para pengambil keputusan yang tepat. Pastikan bahwa penyebab, persyaratan respons, dan perbaikan	1. Apakah hasil analisis akar penyebab (<i>root cause</i>) insiden I&T secara rutin disampaikan ke pimpinan atau pengambil keputusan? <i>Information Flows:</i> laporan resmi, rapat evaluasi. 2. Bagaimana organisasi memastikan bahwa kebutuhan respons tambahan (misalnya kontrol baru, peningkatan keamanan) disampaikan dengan jelas kepada pengambil keputusan? <i>Processes:</i> mekanisme eskalasi kebutuhan respons. 3. Siapa yang bertanggung jawab mengomunikasikan	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>are included in risk governance processes.</i>	proses disertakan dalam proses tata kelola risiko.	hasil analisis akar penyebab dan rekomendasi perbaikan? <i>Organizational Structures (RACI):</i> manajemen risiko, Kepala Bidang Telematika, tim investigasi. 4. Apakah ada kebijakan formal yang mewajibkan penyampaian hasil analisis akar penyebab kepada level manajemen tertentu? <i>Policies:</i> aturan eskalasi hasil investigasi. 5. Bagaimana budaya organisasi dalam menerima rekomendasi perbaikan, apakah proaktif untuk memperbaiki atau cenderung menunda? <i>Culture & Behavior:</i> sikap pimpinan dan staf. 6. Apakah hasil rekomendasi perbaikan biasanya diintegrasikan ke dalam kebijakan atau prosedur manajemen risiko? <i>Processes:</i> pembaruan SOP, kebijakan risiko. 7. Apakah organisasi pernah mengevaluasi efektivitas perbaikan proses setelah implementasi rekomendasi? <i>Information Items:</i> laporan evaluasi, hasil audit tindak			

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			lanjut.			



Hasil Validasi Uji Instrumen FGD Oleh Ahli
Dalam Rangka Penelitian Skripsi Pengukuran Kapabilitas Manajemen Risiko
Informasi dan Teknologi (I&T) pada Dinas Komunikasi dan Informatika Kabupaten
Klungkung Menggunakan *Framework* COBIT 2019

Data Penguji Ahli

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

Hasil Instrumen FGD

1. Pada EDM03 Aktivitas No. 2 RELEVAN DENGAN REVISI istilah *risk appetite* disarankan diganti dengan “dokumen tingkat risiko” agar lebih sesuai dengan terminologi dan konteks organisasi pemerintah daerah.
2. EDM03 Aktivitas No. 11 RELEVAN DENGAN PENYESUAIAN pertanyaan nomor 1 disarankan open reporting dijelaskan menggunakan bahasa yang lazim digunakan di organisasi, agar lebih mudah dipahami oleh informan.
3. APO12.02 Aktivitas No. 10 RELEVAN DENGAN PENYESUAIAN Pertanyaan nomor 6 disarankan disederhanakan bahasanya, khususnya pada bagian “*insiden nyata sebelumnya*” dan “*memperkaya skenario risiko baru*”.
4. Validator telah melakukan penyesuaian langsung (dengan *highlight* kuning) terhadap beberapa istilah agar lebih sesuai dengan konteks instansi pemerintah.

Penguji Ahli,



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

Semarang, 07 November 2025
Peneliti,



Ketut Ananda Dharmawati
NIM 2215091035

Form Uji Validasi Oleh Ahli

Dalam Rangka Penelitian Skripsi

Nama Mahasiswa	: Ketut Ananda Dharmawati
NIM	: 2215091035
Judul Skripsi:	: Pengukuran Kapabilitas Manajemen Risiko Informasi dan Teknologi (I&T) pada Dinas Komunikasi dan Informatika Kabupaten Klungkung Menggunakan <i>Framework</i> COBIT 2019.
Tujuan Uji	: Untuk memastikan bahwa butir-butir pertanyaan dalam instrumen FGD: 1. Sudah sesuai dan mewakili indikator aktivitas dalam domain EDM03 dan APO12 pada <i>framework</i> COBIT 2019. 2. Memiliki relevansi dan kejelasan makna sesuai konteks penelitian di lingkungan instansi pemerintah, khususnya Diskominfo Klungkung. 3. Dapat mengukur kemampuan manajemen risiko I&T secara konsisten dan objektif, tanpa menimbulkan tafsir ganda bagi informan maupun peneliti. 4. Layak digunakan sebagai alat pengumpulan data melalui FGD, setelah dilakukan telaah oleh ahli di bidang tata kelola I&T (COBIT 2019).

INSTRUMEN FGD

Keterangan:

R: Relevan

TR: Tidak Relevan

Tujuan						
<i>Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.</i>			Memastikan bahwa risiko perusahaan yang terkait dengan I&T tidak melebihi selera risiko dan toleransi risiko perusahaan, dampak risiko I&T terhadap nilai perusahaan diidentifikasi dan dikelola, dan potensi kegagalan kepatuhan diminimalkan.			
EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
EDM03.01 Evaluate risk management (Mengevaluasi manajemen risiko).						
1	<i>Understand the organization and its context related to I&T risk.</i>	Memahami organisasi dan konteksnya terkait dengan risiko I&T.	1. Apakah organisasi memiliki dokumen yang menggambarkan risiko I&T dalam konteks pelayanan publik (misalnya Renstra Diskominfo atau <i>Masterplan</i> I&T)? <i>Policies</i> : aturan tertulis, rencana strategis. 2. Bagaimana pimpinan mengidentifikasi faktor	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			eksternal (peraturan pemerintah, ancaman siber nasional) yang dapat memengaruhi risiko I&T? <i>Processes</i> : prosedur evaluasi eksternal. 3. Apakah ada forum khusus untuk membahas faktor internal yang menambah risiko I&T (misalnya keterbatasan SDM, anggaran, atau infrastruktur)? <i>Organizational Structures</i> : siapa yang ikut forum (Kepala Dinas, Bidang Telematika). 4. Bagaimana risiko I&T dipetakan terhadap layanan publik yang dikelola Diskominfo (contoh: <i>e-government</i> , data kependudukan)? <i>Processes</i> : cara organisasi memetakan risiko. 5. Apakah hasil identifikasi konteks risiko I&T biasanya didokumentasikan? <i>Information Items</i> : notulen rapat, <i>risk register</i> . 6. Bagaimana budaya pimpinan/staf dalam membahas risiko I&T, terbuka, formal, atau memiliki kecenderungan menutupi masalah? <i>Culture & Behavior</i> : kebiasaan staf/pimpinan.			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
2	<i>Determine the risk appetite of the organization, i.e., the level of I&T-related risk that the enterprise is willing to take in its pursuit of enterprise objectives.</i>	Menentukan selera risiko organisasi, yaitu tingkat risiko terkait I&T yang bersedia diambil perusahaan dalam mengejar tujuan perusahaan.	1. Apakah organisasi memiliki pernyataan formal tentang tingkat risiko I&T yang masih bisa ditoleransi? <i>Policies</i>: dokumen tingkat risiko SK, kebijakan risiko. 2. Siapa yang berwenang menentukan dokumen tingkat risiko organisasi? <i>Organizational Structures (RACI)</i>: Kepala Dinas, Sekda, atau komite. 3. Apakah dokumen tingkat risiko berbeda untuk tiap bidang (contoh: keamanan data vs layanan jaringan)? <i>Processes</i>: cara organisasi menetapkan dokumen tingkat risiko berbeda. 4. Bagaimana dokumen tingkat risiko dikaitkan dengan tujuan strategis Diskominfo (misalnya digitalisasi layanan publik)? <i>Information Items</i>: strategi TI, KPI organisasi. 5. Apakah dokumen tingkat risiko pernah direvisi/ditinjau ulang secara berkala? <i>Processes</i>: siklus <i>review</i>. 6. Bagaimana pimpinan menyampaikan dokumen	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			tingkat risiko kepada staf teknis? <i>Information Flows:</i> rapat, edaran, sosialisasi. 7. Apakah ada contoh nyata risiko yang dianggap “masih bisa diterima”? <i>Culture & Behavior:</i> contoh sikap pimpinan/staf.			
3	<i>Determine risk tolerance levels against the risk appetite, i.e., temporarily acceptable deviations from the risk appetite.</i>	Menentukan tingkat toleransi risiko terhadap selera risiko, yaitu penyimpangan yang dapat diterima sementara dari selera risiko.	1. Apakah organisasi memiliki standar formal terkait toleransi risiko (misalnya <i>downtime server</i> maksimal 30 menit)? <i>Policies:</i> SLA, SOP. 2. Bagaimana proses penetapan batas toleransi risiko dilakukan? <i>Processes:</i> prosedur penetapan toleransi. 3. Apakah toleransi berbeda antara sistem kritis (contoh: data kependudukan) dan sistem pendukung (contoh: website informasi)? <i>Information Items:</i> dokumen SLA/kontrak. 4. Siapa yang memutuskan kapan suatu risiko sudah melampaui toleransi dan harus diekskalasi? <i>Organizational Structures (RACI):</i> pejabat yang	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			berwenang. 5. Bagaimana toleransi risiko dikomunikasikan ke staf operasional? <i>Information Flows:</i> SOP, pelatihan, <i>briefing</i>. 6. Apakah pernah terjadi pelanggaran batas toleransi risiko? Bagaimana tindak lanjutnya? <i>Processes:</i> tindakan korektif. 7. Apakah toleransi risiko dipengaruhi oleh regulasi eksternal (misalnya standar keamanan nasional)? <i>Culture & Behavior:</i> kesadaran staf terhadap aturan luar. 8. Bagaimana organisasi membedakan toleransi jangka pendek (sementara) dengan <i>risk appetite</i> jangka panjang? <i>Processes:</i> mekanisme perbedaan.			
4	<i>Determine the extent of alignment of the I&T risk strategy to the enterprise risk strategy and ensure the risk</i>	Menentukan tingkat keselarasan strategi risiko I&T dengan strategi risiko perusahaan dan	1. Apakah strategi risiko I&T pernah dibandingkan atau diselaraskan dengan strategi risiko organisasi secara keseluruhan? <i>Processes:</i> mekanisme evaluasi strategi. 2. Siapa yang bertanggung jawab memastikan	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>appetite is below the organization's risk capacity.</i>	memastikan selera risiko berada di bawah kapasitas risiko organisasi.	keselarasan ini? <i>Organizational Structures (RACI)</i>: Kepala Dinas, Komite Risiko (divisi / tim ad-hoc). 3. Apakah ada dokumen yang menunjukkan integrasi antara strategi risiko I&T dan strategi risiko organisasi? <i>Information Items</i>: risk strategy document, Renstra, laporan risiko. 4. Bagaimana pimpinan memastikan bahwa <i>risk appetite</i> I&T tidak melebihi kapasitas risiko organisasi? <i>Policies</i>: prinsip atau batas resmi dalam dokumen. 5. Apakah ada forum lintas unit (I&T dan non-I&T) untuk meninjau keselarasan strategi risiko? <i>Organizational Structures</i>: kolaborasi antar-unit. 6. Apakah ada contoh keputusan strategis yang memperlihatkan keterkaitan langsung antara risiko I&T dan strategi organisasi? <i>Culture & Behavior</i>: kesadaran pimpinan.			
5	<i>Proactively evaluate I&T risk factors in</i>	Mengevaluasi faktor risiko I&T secara	1. Apakah organisasi selalu menilai risiko I&T sebelum mengambil keputusan strategis (misalnya terkait	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>advance of pending strategic enterprise decisions and ensure that risk considerations are part of the strategic enterprise decision process.</i>	proaktif sebelum mengambil keputusan strategis perusahaan dan memastikan bahwa pertimbangan risiko menjadi bagian dari proses pengambilan keputusan strategis perusahaan.	digitalisasi layanan)? <i>Processes: risk assessment</i> pra-keputusan. 2. Siapa yang wajib memberikan masukan risiko I&T dalam rapat pengambilan keputusan strategis? <i>Organizational Structures (RACI):</i> Kepala Dinas, Bidang Telematika. 3. Apakah ada prosedur baku yang mengatur penyampaian risiko I&T sebelum keputusan dibuat? <i>Policies:</i> SOP, aturan rapat. 4. Bagaimana informasi risiko I&T disampaikan ke pimpinan sebelum keputusan? <i>Information Flows:</i> notulen, laporan, presentasi. 5. Apakah faktor risiko I&T selalu menjadi agenda dalam rapat pimpinan strategis? <i>Policies:</i> tata tertib rapat. 6. Bagaimana pimpinan merespons masukan risiko I&T dalam rapat? <i>Culture & Behavior:</i> sikap pimpinan terhadap masukan risiko.			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			7. Apakah ada kasus nyata di mana keputusan strategis berubah karena pertimbangan risiko I&T? <i>Processes:</i> bukti integrasi risiko ke pengambilan keputusan. 8. Apakah hasil evaluasi risiko I&T terdokumentasi sebagai bahan pembelajaran untuk keputusan berikutnya? <i>Information Items:</i> laporan evaluasi, lessons learned.			
6	<i>Evaluate risk management activities to ensure alignment with the enterprise's capacity for I&T-related loss and leadership's tolerance of it.</i>	Mengevaluasi aktivitas manajemen risiko untuk memastikan keselarasan dengan kapasitas perusahaan terhadap kerugian terkait I&T dan toleransi pimpinan terhadap kerugian tersebut.	1. Apakah ada evaluasi formal terhadap kegiatan manajemen risiko I&T? <i>Processes:</i> audit internal, <i>review</i> tahunan. 2. Bagaimana organisasi memastikan kegiatan manajemen risiko sesuai kapasitas keuangan atau sumber daya? <i>Policies:</i> batas anggaran, pedoman alokasi SDM. 3. Apakah pimpinan menetapkan batas toleransi kerugian terkait I&T (misalnya <i>downtime</i> maksimal, batas kehilangan data)? <i>Organizational Structures (RACI):</i> pimpinan, dewan.	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			4. Bagaimana hasil evaluasi manajemen risiko I&T dilaporkan? <i>Information Items:</i> laporan risiko, hasil audit. 5. Apakah kegiatan manajemen risiko I&T pernah dikoreksi karena dianggap melampaui kapasitas organisasi? <i>Processes:</i> corrective actions. 6. Bagaimana sikap pimpinan terhadap hasil evaluasi yang menunjukkan potensi kerugian besar? <i>Culture & Behavior:</i> penerimaan pimpinan atas risiko. 7. Apakah ada mekanisme eskalasi jika aktivitas manajemen risiko I&T dinilai tidak sesuai kapasitas organisasi? <i>Information Flows:</i> jalur eskalasi resmi.			
7	<i>Attract and maintain necessary skills and personnel for I&T Risk Management.</i>	Merekrut dan mempertahankan keterampilan dan personel yang diperlukan untuk	1. Apakah organisasi memiliki staf khusus yang menangani manajemen risiko I&T? <i>Organizational Structures (RACI):</i> posisi formal di struktur organisasi. 2. Bagaimana organisasi mengidentifikasi kebutuhan	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
		Manajemen Risiko I&T.	keterampilan staf untuk manajemen risiko I&T? <i>Processes:</i> analisis kebutuhan SDM. 3. Apakah tersedia program pelatihan internal maupun eksternal atau sertifikasi khusus untuk staf terkait risiko I&T? <i>People, Skills & Competencies:</i> pelatihan, <i>workshop</i>. 4. Bagaimana organisasi memastikan staf baru memahami kebijakan manajemen risiko I&T? <i>Policies:</i> materi induksi/briefing. 5. Apakah ada program retensi untuk mempertahankan staf yang kompeten di bidang risiko I&T? <i>Culture & Behavior:</i> penghargaan, promosi. 6. Bagaimana organisasi mengatasi kekurangan staf berkompeten di bidang risiko I&T? <i>Processes:</i> strategi rekrutmen, outsourcing. 7. Apakah ada perencanaan jangka panjang untuk pengembangan kompetensi staf risiko I&T? <i>Policies:</i> dokumen HR, Renstra SDM. 8. Bagaimana organisasi memanfaatkan infrastruktur			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			(contoh: <i>e-learning, platform</i> pelatihan <i>online</i>) untuk mendukung pengembangan staf? <i>Services & Infrastructure</i> : sistem pendukung pelatihan. 9. Apakah kompetensi staf di bidang risiko I&T pernah dievaluasi secara formal (misalnya melalui asesmen)? <i>People, Skills & Competencies</i> : uji kompetensi.			
EDM03.02 Direct risk management (Mengarahkan manajemen risiko).						
8	<i>Direct the translation and integration of the I&T risk strategy into risk management practices and operational activities.</i>	Mengarahkan penerjemahan dan integrasi strategi risiko I&T ke dalam praktik manajemen risiko dan aktivitas operasional.	1. Apakah strategi risiko I&T yang dimiliki organisasi sudah diterjemahkan menjadi praktik operasional sehari-hari? <i>Processes</i> : bukti implementasi dalam SOP atau <i>workflow</i> . 2. Siapa yang bertanggung jawab memastikan strategi risiko I&T diintegrasikan ke kegiatan operasional? <i>Organizational Structures (RACI)</i> : Kepala Dinas, Bidang Telematika, tim manajemen risiko. 3. Apakah ada dokumen yang menjelaskan bagaimana strategi risiko I&T diturunkan ke tingkat operasional? <i>Information Items</i> : pedoman, manual kerja, SOP.	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			4. Bagaimana organisasi memastikan staf memahami strategi risiko I&T dalam pekerjaannya sehari-hari? <i>Culture & Behavior</i>: komunikasi & sosialisasi. 5. Apakah ada rapat rutin untuk meninjau sejauh mana strategi risiko I&T dijalankan di <i>level</i> operasional? <i>Information Flows</i>: laporan rapat, notulen. 6. Apakah terdapat contoh nyata kegiatan operasional yang sudah menyesuaikan strategi risiko I&T? <i>Processes</i>: contoh implementasi. 7. Bagaimana organisasi mengukur efektivitas integrasi strategi risiko I&T ke operasional? <i>Policies</i>: indikator kinerja, KPI. 8. Apakah strategi risiko I&T pernah gagal diterapkan di lapangan? Jika ya, apa penyebabnya? <i>Processes</i>: evaluasi kegagalan.			
9	<i>Direct the development of risk communication plans (covering all levels of the</i>	Mengarahkan pengembangan rencana komunikasi risiko (mencakup semua	1. Apakah organisasi memiliki rencana komunikasi risiko yang formal dan tertulis? <i>Policies</i>: dokumen komunikasi risiko. 2. Siapa yang bertanggung jawab mengembangkan	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>enterprise).</i>	tingkatan perusahaan).	rencana komunikasi risiko? <i>Organizational Structures (RACI):</i> Bidang Telematika, Sekretariat, pimpinan. 3. Bagaimana informasi risiko disampaikan ke level pimpinan, staf teknis, dan pemangku kepentingan eksternal? <i>Information Flows:</i> jalur komunikasi resmi. 4. Apakah ada perbedaan cara komunikasi risiko untuk level manajemen dan staf operasional? <i>Processes:</i> metode komunikasi berbeda. 5. Bagaimana budaya organisasi memengaruhi keterbukaan dalam komunikasi risiko? <i>Culture & Behavior:</i> keterbukaan vs tertutup. 6. Apakah ada pelatihan atau sosialisasi mengenai komunikasi risiko? <i>People, Skills & Competencies:</i> program pelatihan. 7. Bagaimana efektivitas komunikasi risiko dievaluasi? <i>Processes:</i> feedback, survei kepuasan komunikasi.			
10	<i>Direct implementation</i>	Mengarahkan penerapan	1. Apakah organisasi memiliki mekanisme resmi untuk	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>of the appropriate mechanisms to respond quickly to changing risk and report immediately to appropriate levels of management, supported by agreed principles of escalation (what to report, when, where and how).</i>	mekanisme yang tepat untuk merespons perubahan risiko dengan cepat dan segera melaporkannya ke tingkat manajemen yang sesuai, didukung oleh prinsip-prinsip eskalasi yang disepakati (apa yang harus dilaporkan, kapan, di mana, dan bagaimana).	merespons perubahan risiko I&T secara cepat? <i>Processes:</i> prosedur tanggap risiko. 2. Bagaimana staf melaporkan risiko baru atau perubahan risiko yang muncul? <i>Information Flows:</i> jalur pelaporan resmi. 3. Siapa yang bertugas menerima dan menindaklanjuti laporan risiko baru? <i>Organizational Structures (RACI):</i> pejabat pengelola risiko. 4. Apakah ada peningkatan yang jelas (apa yang dilaporkan, kapan, kepada siapa)? <i>Policies:</i> dokumen rencana tindak lanjut 5. Bagaimana organisasi memastikan laporan risiko segera sampai ke pimpinan terkait? <i>Processes:</i> mekanisme komunikasi cepat. 6. Apakah tersedia media khusus untuk laporan risiko darurat (misalnya <i>hotline</i>, aplikasi <i>internal</i>)? <i>Services & Infrastructure:</i> sistem pelaporan. 7. Apakah ada contoh kasus nyata di mana eskalasi			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			risiko berhasil dilakukan dengan cepat? <i>Processes:</i> studi kasus. 8. Bagaimana pimpinan biasanya menanggapi laporan eskalasi risiko? <i>Culture & Behavior:</i> respons pimpinan. 9. Apakah efektivitas mekanisme eskalasi risiko pernah dievaluasi secara formal? <i>Information Items:</i> laporan evaluasi.			
11	<i>Direct that risk, opportunities, issues and concerns may be identified and reported by anyone to the appropriate party at any time. Risk should be managed in accordance with published policies and procedures and</i>	Mengarahkan agar risiko, peluang, isu, dan kekhawatiran dapat diidentifikasi dan dilaporkan oleh siapa pun kepada pihak yang tepat kapan saja. Risiko harus dikelola sesuai dengan kebijakan dan prosedur yang dipublikasikan dan	1. Apakah ada kebijakan yang memperbolehkan semua pegawai melaporkan risiko atau isu tanpa batasan hierarki? <i>Policies:</i> kebijakan pelaporan terbuka 2. Bagaimana staf biasanya menyampaikan risiko, peluang, atau isu yang mereka temukan? <i>Information Flows:</i> jalur komunikasi resmi maupun informal. 3. Siapa yang menerima laporan risiko dari staf? <i>Organizational Structures (RACI):</i> pejabat penerima laporan.	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>escalated to the relevant decision makers.</i>	dieskalasikan kepada para pengambil keputusan yang relevan.	4. Apakah laporan risiko bisa dilakukan secara anonim untuk menghindari hambatan budaya? <i>Culture & Behavior</i>: keberanian/keterbukaan staf. 5. Apakah organisasi menyediakan media resmi untuk laporan terbuka (aplikasi, kotak saran, hotline)? <i>Services & Infrastructure</i>: sarana pelaporan. 6. Apakah ada prosedur bagaimana laporan staf ditindaklanjuti? <i>Processes</i>: alur tindak lanjut. 7. Apakah peluang yang dilaporkan staf juga dipertimbangkan sebagai masukan strategis? <i>Processes</i>: integrasi peluang ke strategi. 8. Apakah ada contoh nyata risiko/isu dari staf yang berhasil mencegah masalah besar di organisasi? <i>Information Items</i>: catatan kasus.			
12	<i>Identify key goals and metrics of the risk governance and management processes</i>	Mengidentifikasi tujuan dan metrik utama dari proses tata kelola dan manajemen risiko yang	1. Apakah organisasi memiliki tujuan utama yang jelas untuk tata kelola risiko I&T? <i>Policies</i>: dokumen tujuan risiko. 2. Bagaimana indikator keberhasilan manajemen risiko	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>to be monitored, and approve the approaches, methods, techniques and processes for capturing and reporting the measurement information.</i>	akan dipantau, dan menyetujui pendekatan, metode, teknik, dan proses untuk menangkap dan melaporkan informasi pengukuran.	I&T ditentukan? <i>Processes:</i> penetapan KPI. 3. Siapa yang menyetujui metrik dan indikator risiko yang digunakan? <i>Organizational Structures (RACI):</i> pimpinan, komite risiko. 4. Apakah ada metode formal untuk mengukur kinerja manajemen risiko? <i>Processes:</i> teknik pengukuran, audit. 5. Bagaimana informasi hasil pengukuran risiko disampaikan ke pimpinan? <i>Information Flows:</i> laporan kinerja. 6. Apakah organisasi menggunakan sistem/ <i>tools</i> untuk mengumpulkan data metrik risiko? <i>Services & Infrastructure:</i> aplikasi monitoring. 7. Bagaimana pimpinan menilai apakah indikator risiko sesuai dengan tujuan strategis? <i>Culture & Behavior:</i> kesadaran pimpinan. 8. Apakah hasil <i>monitoring</i> indikator risiko			

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			terdokumentasi secara rutin? <i>Information Items:</i> laporan bulanan, tahunan. 9. Apakah metrik risiko pernah direvisi karena dianggap tidak relevan? <i>Processes:</i> siklus perbaikan metrik.			
EDM03.03 Monitor risk management (Memantau manajemen risiko).						
13	<i>Report any risk management issues to the board or executive committee.</i>	Melaporkan setiap permasalahan terkait manajemen risiko kepada Dewan Komisaris atau komite eksekutif.	1. Apakah organisasi memiliki mekanisme resmi untuk melaporkan masalah manajemen risiko ke pimpinan/komite eksekutif? <i>Policies:</i> aturan pelaporan risiko. 2. Siapa yang bertanggung jawab menyusun laporan masalah manajemen risiko ke pimpinan? <i>Organizational Structures (RACI):</i> Bidang Telematika, Kepala Dinas. 3. Bagaimana laporan masalah manajemen risiko biasanya disampaikan? (tertulis, presentasi, rapat) <i>Information Flows:</i> media komunikasi. 4. Apakah laporan masalah manajemen risiko terdokumentasi secara formal?	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Information Items:</i> notulen, laporan resmi. 5. Bagaimana sikap pimpinan saat menerima laporan masalah manajemen risiko? <i>Culture & Behavior:</i> keseriusan pimpinan menindaklanjuti.			
14	<i>Monitor the extent to which the risk profile is managed within the enterprise's risk appetite and tolerance thresholds.</i>	Memantau sejauh mana profil risiko dikelola dalam selera risiko dan ambang batas toleransi perusahaan.	1. Apakah organisasi memantau apakah profil risiko I&T sesuai dengan dokumen tingkat risiko dan <i>tolerance</i> yang telah ditetapkan? <i>Processes:</i> mekanisme monitoring. 2. Siapa yang memantau kesesuaian profil risiko terhadap dokumen tingkat risiko? <i>Organizational Structures (RACI):</i> pejabat <i>risk owner</i> . 3. Apakah ada sistem/ <i>tools</i> yang digunakan untuk memantau profil risiko? <i>Services & Infrastructure:</i> aplikasi <i>monitoring</i> . 4. Bagaimana hasil pemantauan disampaikan ke pimpinan? <i>Information Flows:</i> laporan periodik. 5. Apakah profil risiko pernah melebihi batas <i>tolerance</i> ?	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Information Items:</i> bukti laporan pelanggaran. 6. Bagaimana budaya organisasi ketika terjadi pelanggaran peningkat risiko/ <i>tolerance</i> ? <i>Culture & Behavior:</i> reaksi staf/pimpinan. 7. Apakah hasil monitoring digunakan untuk memperbarui strategi risiko I&T? <i>Processes:</i> siklus perbaikan.			
15	<i>Monitor key goals and metrics of risk governance and management processes against targets, analyze the cause of any deviations, and initiate remedial actions to address the underlying causes.</i>	Memantau tujuan dan metrik utama tata kelola risiko dan proses manajemen terhadap target, menganalisis penyebab penyimpangan, dan mengambil tindakan perbaikan untuk mengatasi penyebab yang mendasarinya.	1. Apakah organisasi memiliki target jelas untuk tujuan dan metrik tata kelola risiko I&T? <i>Policies:</i> dokumen KPI risiko. 2. Bagaimana kinerja tata kelola risiko I&T dipantau dan dibandingkan terhadap terhadap target? <i>Processes:</i> metode <i>monitoring</i> . 3. Siapa yang melakukan analisis jika ada penyimpangan dari target? <i>Organizational Structures (RACI):</i> unit analisis, pimpinan. 4. Apakah hasil monitoring metrik risiko terdokumentasi?	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			<i>Information Items:</i> laporan kinerja risiko. 5. Apakah penyebab penyimpangan risiko biasanya dicatat dan dianalisis? <i>Processes:</i> root cause analysis. 6. Bagaimana budaya pimpinan saat membahas penyimpangan risiko? Apakah mencari solusi atau menyalahkan? <i>Culture & Behavior:</i> sikap pimpinan. 7. Apakah organisasi memiliki prosedur untuk tindakan korektif bila metrik risiko menyimpang jauh dari target? <i>Policies:</i> pedoman tindakan korektif. 8. Apakah remedial action pernah berhasil mengembalikan kinerja risiko ke target? <i>Processes:</i> contoh nyata corrective action.			
16	<i>Enable key stakeholders' review of the enterprise's progress toward identified goals.</i>	Memungkinkan peninjauan oleh pemangku kepentingan utama atas kemajuan perusahaan terhadap	1. Apakah pemangku kepentingan (internal maupun eksternal) dilibatkan dalam peninjauan kemajuan pencapaian tujuan risiko I&T? <i>Organizational Structures (RACI):</i> pemangku kepentingan utama.	R		

EDM03 Ensure Risk Optimization						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
		tujuan yang telah ditetapkan.	2. Apakah ada forum khusus untuk melakukan peninjauan bersama pemangku kepentingan? <i>Processes</i>: rapat evaluasi, forum koordinasi. 3. Bagaimana hasil peninjauan pemangku kepentingan didokumentasikan? <i>Information Items</i>: notulen, laporan hasil peninjauan 4. Apakah masukan pemangku kepentingan digunakan untuk memperbaiki manajemen risiko I&T? <i>Processes</i>: siklus perbaikan. 5. Bagaimana budaya organisasi dalam menerima masukan dari pemangku kepentingan? <i>Culture & Behavior</i>: keterbukaan terhadap kritik. 6. Apakah organisasi menggunakan laporan khusus untuk menunjukkan progres kepada pemangku kepentingan? <i>Information Flows</i>: laporan publik, <i>dashboard</i>.			

Tujuan	
<i>Integrate the management of I&T-related enterprise risk with overall enterprise risk management (ERM) and balance the costs and benefits of managing I&T-related enterprise risk.</i>	Mengintegrasikan pengelolaan risiko perusahaan terkait I&T dengan manajemen risiko perusahaan (ERM) secara keseluruhan dan seimbangkan biaya dan manfaat pengelolaan risiko perusahaan terkait I&T.

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
APO12.01 Collect data (Mengumpulkan data).						
1	Establish and maintain a method for the collection, classification and analysis of I&T risk-related data.	Membangun dan memelihara metode untuk pengumpulan, klasifikasi, dan analisis data terkait risiko I&T.	1. Apakah organisasi memiliki metode resmi untuk mengumpulkan dan menganalisis data risiko I&T ? <i>Policies:</i> SOP atau pedoman resmi pengumpulan risiko 2. Apakah klasifikasi data risiko sudah ditetapkan (misalnya insiden keamanan, <i>downtime</i> , kesalahan manusia)? <i>Processes:</i> mekanisme klasifikasi risiko 3. Bagaimana prosedur memastikan data yang dikumpulkan valid dan konsisten? <i>Processes:</i> verifikasi data risiko 4. Apakah metode ini didokumentasikan dalam bentuk SOP atau pedoman resmi? <i>Information Items:</i> dokumen SOP, pedoman risiko	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
2	<i>Record relevant and significant I&T risk-related data on the enterprise's internal and external operating environment.</i>	Mencatat data risiko I&T yang relevan dan signifikan pada lingkungan operasi internal dan eksternal perusahaan.	1. Jenis data risiko I&T apa saja yang biasanya dicatat (internal vs eksternal)? <i>Information Items:</i> risk log, laporan eksternal 2. Apakah ada format baku untuk pencatatan data risiko? <i>Policies:</i> format standar pencatatan risiko 3. Siapa yang biasanya mencatat data risiko I&T? <i>Organizational Structures:</i> staf Bidang Telematika / manajemen risiko 4. Bagaimana data eksternal (misalnya regulasi pemerintah, tren industri) ikut didokumentasikan? <i>Processes:</i> integrasi data eksternal ke pencatatan	R		
3	<i>Adopt or define a risk taxonomy for consistent definitions of risk scenarios and impact and likelihood categories.</i>	Mengadopsi atau menetapkan taksonomi risiko untuk definisi skenario risiko dan kategori dampak serta kemungkinan yang konsisten.	1. Apakah organisasi memiliki taksonomi risiko I&T (misalnya kategori dampak: finansial, reputasi, layanan publik)? <i>Policies:</i> dokumen taksonomi risiko 2. Apakah kategori risiko dan probabilitasnya konsisten dipakai semua bidang? <i>Processes:</i> penerapan klasifikasi risiko 3. Bagaimana taksonomi risiko ini dikomunikasikan	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			kepada staf yang terlibat? <i>Information Flows</i>: sosialisasi taksonomi risiko 4. Apakah pernah ada revisi/penyesuaian taksonomi risiko? <i>Culture & Behavior</i>: kesadaran untuk memperbarui taksonomi			
4	<i>Record data on risk events that have caused or may cause business impacts as per the impact categories defined in the risk taxonomy.</i> <i>Capture relevant data from related issues, incidents, problems and investigations.</i>	Mencatat data tentang peristiwa risiko yang telah menyebabkan atau mungkin menyebabkan dampak bisnis sesuai kategori dampak yang ditetapkan dalam taksonomi risiko. Menangkap data yang relevan dari isu, insiden, masalah, dan investigasi terkait.	1. Apakah insiden risiko I&T (<i>downtime</i>, serangan siber) selalu dicatat sesuai kategori dampak? <i>Processes</i>: pencatatan insiden sesuai kategori risiko 2. Apakah ada integrasi data dari laporan insiden, problem, atau investigasi? <i>Information Items</i>: laporan insiden, investigasi 3. Siapa yang bertanggung jawab memastikan pencatatan insiden sesuai kategori risiko? <i>Organizational Structures</i>: tim TI / manajemen risiko 4. Apakah catatan insiden digunakan untuk perbaikan layanan? <i>Processes</i>: <i>feedback loop</i> ke perbaikan layanan	R		
5	<i>Survey and analyze the</i>	Melakukan survei dan	1. Apakah organisasi menganalisis data risiko historis	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>historical I&T risk data and loss experience from externally available data and trends, industry peers through industry-based event logs, databases, and industry agreements for common event disclosure.</i>	analisis data risiko I&T historis dan pengalaman kerugian dari data dan tren yang tersedia secara eksternal, rekan industri melalui log peristiwa berbasis industri, basis data, dan perjanjian industri untuk pengungkapan peristiwa umum.	internal? <i>Processes:</i> analisis data historis 2. Apakah data eksternal (tren industri, data asosiasi pemerintah/kominfo) juga digunakan? <i>Information Items:</i> laporan tren eksternal 3. Bagaimana data eksternal dibandingkan dengan kondisi internal organisasi? <i>Processes:</i> benchmarking internal-eksternal 4. Apakah ada contoh perbaikan kebijakan/teknis yang diambil dari analisis tren eksternal? <i>Culture & Behavior:</i> keterbukaan untuk belajar dari eksternal			
6	<i>For similar classes of events, organize the collected data and highlight contributing factors. Determine common contributing factors across multiple</i>	Untuk kelas kejadian yang serupa, menyusun data yang terkumpul dan soroti faktor-faktor yang berkontribusi. Tentukan faktor-faktor yang berkontribusi secara	1. Apakah organisasi mengelompokkan insiden serupa (misalnya serangan <i>malware</i> berulang)? <i>Processes:</i> klasifikasi insiden serupa 2. Faktor penyebab umum apa saja yang biasanya diidentifikasi? <i>Information Items:</i> catatan faktor penyebab 3. Apakah hasil analisis faktor penyebab digunakan	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>events.</i>	umum pada beberapa kejadian.	untuk mencegah kejadian serupa? <i>Culture & Behavior</i> : kesadaran mencegah insiden berulang			
7	<i>Determine the specific conditions that existed or were absent when risk events occurred and the way the conditions affected event frequency and loss magnitude.</i>	Menentukan kondisi spesifik yang ada atau tidak ada saat peristiwa risiko terjadi dan cara kondisi tersebut memengaruhi frekuensi peristiwa dan besarnya kerugian.	1. Apakah kondisi tertentu (misalnya kurang staf, beban server tinggi) selalu dicatat saat insiden terjadi? <i>Processes</i> : pencatatan kondisi insiden 2. Bagaimana kondisi tersebut memengaruhi frekuensi kejadian/tingkat kerugian? <i>Information Items</i> : laporan analisis insiden 3. Apakah organisasi melakukan analisis <i>root cause</i> berbasis kondisi lingkungan/operasional? <i>Processes</i> : <i>root cause analysis</i> <i>Root cause</i> = penyebab paling mendasar suatu masalah/insiden, bukan sekadar gejala permukaan.	R		
8	<i>Perform periodic event and risk factor analysis to identify new or emerging risk issues and to gain an</i>	Melakukan analisis kejadian dan faktor risiko secara berkala untuk mengidentifikasi masalah risiko baru atau	1. Seberapa sering dilakukan analisis risiko I&T berkala? <i>Policies</i> : kebijakan <i>review</i> berkala 2. Siapa yang terlibat dalam analisis berkala ini? <i>Organizational Structures</i> : tim Manajemen Risiko,	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>understanding of the associated internal and external risk factors.</i>	yang muncul dan untuk memperoleh pemahaman tentang faktor risiko internal dan eksternal terkait.	Bidang Telematika 3. Apakah hasil analisis digunakan untuk memperbarui daftar risiko organisasi? <i>Processes:</i> pembaruan daftar risiko 4. Apakah ada contoh risiko baru yang teridentifikasi dari analisis periodik (misalnya tren <i>ransomware</i>)? <i>Information Items:</i> laporan analisis risiko			
APO12.02 Analyze risk (Menganalisis risiko).						
9	<i>Define the appropriate scope of risk analysis efforts, considering all risk factors and/or the business criticality of assets.</i>	Menentukan cakupan upaya analisis risiko yang tepat, dengan mempertimbangkan semua faktor risiko dan/atau kekritisitas aset dalam bisnis.	1. Bagaimana organisasi menentukan lingkup analisis risiko I&T (misalnya hanya pada aplikasi tertentu atau seluruh layanan publik)? <i>Processes:</i> prosedur penetapan lingkup analisis. 2. Siapa yang memutuskan ruang lingkup analisis risiko? <i>Organizational Structures (RACI):</i> Kepala Dinas, Bidang Telematika, Tim Manajemen Risiko. 3. Apakah ada kriteria formal untuk memilih aset mana yang dianggap kritis dalam analisis risiko? <i>Policies:</i> pedoman kritikalitas aset. 4. Bagaimana hasil penentuan lingkup analisis risiko	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			didokumentasikan? <i>Information Items: risk analysis scope document.</i>			
10	<i>Build and regularly update I&T risk scenarios; I&T-related loss exposures; and scenarios regarding reputational risk, including compound scenarios of cascading and/or coincidental threat types and events. Develop expectations for specific control activities and capabilities to detect.</i>	Menyusun dan memperbarui skenario risiko I&T secara berkala; paparan kerugian terkait I&T; dan skenario terkait risiko reputasi, termasuk skenario gabungan dari jenis dan peristiwa ancaman yang berjenjang dan/atau bersamaan. Mengembangkan ekspektasi untuk aktivitas dan kemampuan kontrol tertentu untuk	1. Apakah organisasi memiliki daftar atau katalog skenario risiko I&T yang terdokumentasi? <i>Policies: dokumen risk scenario register.</i> <i>Risk scenario</i> = gambaran terstruktur tentang kemungkinan kejadian risiko, dampak, dan penyebabnya. 2. Seberapa sering skenario risiko diperbarui (tahunan, per proyek besar, setelah insiden)? <i>Processes: siklus update skenario.</i> 3. Apakah organisasi pernah menyusun skenario gabungan (contoh: serangan siber + kegagalan infrastruktur jaringan terjadi bersamaan)? <i>Processes: penyusunan skenario multi-event.</i> 4. Siapa yang terlibat dalam penyusunan dan pembaruan skenario risiko I&T? <i>Organizational Structures (RACI):</i> Bidang Telematika, Kepala Dinas, tim keamanan informasi.	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
		mendeteksi.	5. Apakah ada metode standar dalam memperkirakan dampak reputasi dari sebuah skenario risiko I&T? <i>Policies:</i> panduan analisis reputasi. 6. Bagaimana pengalaman dari insiden sebelumnya digunakan untuk memperbaiki atau menambah skenario risiko baru? <i>Information Items:</i> catatan insiden, laporan audit. 7. Bagaimana organisasi menentukan kontrol apa saja yang harus tersedia untuk setiap skenario risiko? <i>Processes:</i> mapping skenario ke kontrol. <i>Control</i> = mekanisme/prosedur untuk mengurangi atau mendeteksi risiko. 8. Apakah pimpinan atau <i>stakeholder</i> pernah dilibatkan dalam validasi skenario risiko sebelum dipakai dalam analisis formal? <i>Culture & Behavior:</i> keterlibatan pimpinan, tingkat keseriusan validasi.			
11	Estimate the frequency (or likelihood) and	Memperkirakan frekuensi (atau	1. Bagaimana organisasi memperkirakan seberapa sering risiko I&T bisa terjadi?	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>magnitude of loss or gain associated with I&T risk scenarios. Take into account all applicable risk factors and evaluate known operational controls.</i>	kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario risiko I&T. Mempertimbangkan semua faktor risiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.	<i>Processes:</i> metode estimasi frekuensi. 2. Bagaimana memperkirakan besarnya kerugian (atau keuntungan) bila risiko terjadi? <i>Information Items:</i> data historis, perhitungan biaya. 3. Apakah faktor-faktor risiko eksternal (misalnya regulasi, tren siber) ikut dipertimbangkan? <i>Policies:</i> pedoman analisis risiko. 4. Bagaimana pengendalian yang ada dievaluasi saat memperkirakan dampak risiko? <i>Processes:</i> evaluasi kontrol.			
12	<i>Compare current risk (I&T-related loss exposure) to risk appetite and acceptable risk tolerance. Identify unacceptable or</i>	Membandingkan risiko saat ini (paparan kerugian terkait I&T) dengan selera risiko dan toleransi risiko yang dapat diterima. Mengidentifikasi risiko	1. Apakah organisasi pernah membandingkan profil risiko saat ini dengan dokumen tingkat risiko yang sudah ditetapkan? <i>Processes:</i> risk profile vs appetite. 2. Siapa yang berwenang menyatakan risiko melebihi batas appetite/tolerance? <i>Organizational Structures (RACI):</i> pimpinan, komite	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>elevated risk.</i>	yang tidak dapat diterima atau tinggi.	risiko. 3. Apakah ada format laporan resmi untuk menyampaikan risiko yang tidak dapat diterima? <i>Information Items:</i> laporan eksposur risiko. 4. Bagaimana pimpinan menindaklanjuti risiko yang melebihi toleransi? <i>Culture & Behavior:</i> reaksi pimpinan terhadap pelanggaran batas.			
13	<i>Propose risk responses for risk exceeding risk appetite and tolerance levels.</i>	Mengusulkan respons risiko untuk risiko yang melampaui selera risiko dan tingkat toleransi.	1. Bagaimana organisasi menentukan opsi respons (menghindari, mengurangi, transfer, menerima)? <i>Processes:</i> <i>risk response planning.</i> 2. Siapa yang berwenang mengusulkan atau memilih opsi respons risiko? <i>Organizational Structures (RACI):</i> pimpinan, tim manajemen risiko. 3. Apakah ada dokumen yang mencatat usulan respons risiko? <i>Information Items:</i> <i>risk response proposal.</i>	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			4. Bagaimana respons risiko disesuaikan dengan kebijakan organisasi? <i>Policies: pedoman respons risiko.</i>			
14	<i>Specify high-level requirements for projects or programs that will implement the selected risk responses. Identify requirements and expectations for appropriate key controls for risk mitigation responses.</i>	Menetapkan persyaratan tingkat tinggi untuk proyek atau program yang akan menerapkan respons risiko yang dipilih. Identifikasi persyaratan dan harapan untuk kontrol utama yang sesuai untuk respons mitigasi risiko.	1. Bagaimana organisasi menentukan proyek/program untuk mengurangi risiko I&T? <i>Processes: perencanaan proyek mitigasi.</i> 2. Apakah ada dokumen resmi yang menjelaskan kebutuhan & harapan kontrol utama? <i>Information Items: project charter, TOR, Business Case</i> <i>Project Charter</i> = dokumen awal proyek yang memuat tujuan, scope, risiko, dan high-level requirement. <i>TOR (Terms of Reference)</i> = dokumen yang menjelaskan detail kebutuhan, ruang lingkup, dan harapan dari suatu program/proyek. Dokumen <i>Business Case</i> = justifikasi proyek, sering kali berisi requirement kontrol risiko. 3. Siapa yang menyetujui requirement mitigasi risiko I&T? <i>Organizational Structures (RACI):</i> pimpinan proyek,	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			Kepala Dinas. 4. Bagaimana requirement tersebut dikomunikasikan ke tim pelaksana? <i>Information Flows</i> : rapat, dokumen tertulis.			
15	<i>Validate the risk analysis and business impact analysis (BIA) results before using them in decision making. Confirm that the analysis aligns with enterprise requirements and verify that estimations were properly calibrated and scrutinized for bias.</i>	Memvalidasi hasil analisis risiko dan analisis dampak bisnis (BIA) sebelum menggunakannya dalam pengambilan keputusan. Pastikan analisis tersebut sesuai dengan persyaratan perusahaan dan verifikasi bahwa estimasi telah dikalibrasi dengan benar dan diteliti untuk mengetahui biasnya.	1. Apakah hasil analisis risiko/BIA pernah diverifikasi ulang sebelum dipakai untuk keputusan? <i>Processes</i> : validasi analisis. BIA = analisis dampak bisnis, menilai seberapa parah dampak jika layanan terganggu. 2. Siapa yang melakukan validasi hasil analisis risiko? <i>Organizational Structures (RACI)</i> : tim independen, pimpinan. 3. Bagaimana memastikan hasil analisis bebas bias? <i>Policies</i> : prinsip validasi objektif. 4. Apakah ada bukti dokumentasi validasi (notulen, laporan)? <i>Information Items</i> : dokumen validasi.	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
16	<i>Analyze cost/benefit of potential risk response options such as avoid, reduce/mitigate, transfer/share, and accept and exploit/seize. Confirm the optimal risk response.</i>	Menganalisis biaya/manfaat dari opsi respons risiko potensial seperti menghindari, mengurangi/meringankan, mentransfer/membagi, dan menerima serta memanfaatkan/merebut. Mengonfirmasikan respons risiko yang optimal.	1. Apakah organisasi memiliki prosedur formal dalam membandingkan biaya dan manfaat dari berbagai opsi respons risiko? <i>Policies: pedoman analisis cost and benefit.</i> 2. Bagaimana cara organisasi menilai manfaat dari suatu respons risiko (misalnya pengurangan <i>downtime</i>, peningkatan kepercayaan publik)? <i>Processes: metode analisis manfaat.</i> 3. Apakah ada standar atau indikator keuangan yang digunakan dalam menghitung biaya (contoh: ROI, <i>payback period</i>)? <i>Information Items: laporan keuangan, proyeksi biaya.</i> 4. Siapa yang biasanya memutuskan opsi respons risiko yang dipilih (misalnya Kepala Dinas, komite risiko, atau bagian keuangan)? <i>Organizational Structures (RACI):</i> pengambil keputusan. 5. Bagaimana organisasi memastikan bahwa opsi respons risiko yang dipilih sesuai dengan <i>risk appetite</i>	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			dan <i>tolerance</i> yang berlaku? <i>Processes: alignment</i> dengan <i>risk appetite</i>. 6. Apakah organisasi pernah menggunakan pendekatan transfer risiko (misalnya asuransi, outsourcing) dan bagaimana analisis biayanya dibanding mitigasi internal? <i>Processes: evaluasi opsi transfer.</i> 7. Apakah budaya organisasi cenderung lebih memilih menghindari risiko (<i>risk averse</i>) atau berani mengambil risiko untuk peluang strategis (<i>risk seeking</i>)? <i>Culture & Behavior: sikap organisasi terhadap risiko.</i> 8. Apakah hasil analisis <i>cost/benefit</i> didokumentasikan dan dilaporkan secara formal untuk mendukung keputusan manajemen? <i>Information Flows: laporan analisis risiko ke pimpinan.</i>			
APO12.03 Maintain a risk profile (Memelihara profile risiko).						
17	Inventory business processes and document their	Menginventarisasi proses bisnis dan dokumentasikan	1. Apakah organisasi memiliki inventaris proses bisnis yang terdokumentasi? <i>Information Items: dokumen inventaris proses bisnis.</i>	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>dependency on I&T service management processes and IT infrastructure resources. Identify supporting personnel, applications, infrastructure, facilities, critical manual records, vendors, suppliers and outsourcers.</i>	ketergantungannya pada proses manajemen layanan I&T dan sumber daya infrastruktur I&T. Mengidentifikasi personel pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan pihak yang melakukan alih daya.	2. Bagaimana ketergantungan proses bisnis pada sistem I&T dicatat? <i>Processes: pemetaan dependency.</i> 3. Apakah personel pendukung, aplikasi, infrastruktur, vendor juga dicatat dalam inventaris ini? <i>Policies: aturan kelengkapan inventaris.</i> 4. Siapa yang bertanggung jawab memelihara inventaris tersebut? <i>Organizational Structures (RACI):</i> Bidang Telematika, unit perencana.			
18	<i>Determine and agree on which I&T services and IT infrastructure resources are essential to sustain the operation of business processes. Analyze</i>	Menentukan dan menyetujui layanan I&T dan sumber daya infrastruktur I&T mana yang penting untuk mempertahankan operasi proses bisnis.	1. Bagaimana organisasi menentukan layanan I&T mana yang sangat kritis untuk layanan publik? <i>Processes: analisis layanan esensial.</i> 2. Apakah ada dokumen resmi yang menyatakan layanan/infrastruktur esensial? <i>Information Items: daftar layanan kritis, BCP.</i> 3. Siapa yang menyetujui daftar layanan/infrastruktur	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>dependencies and identify weak links.</i>	Menganalisis ketergantungan dan mengidentifikasi titik lemah.	esensial? <i>Organizational Structures (RACI):</i> pimpinan, manajemen risiko. 4. Bagaimana titik lemah dalam ketergantungan layanan dianalisis? <i>Processes:</i> weak link analysis.			
19	<i>Aggregate current risk scenarios by category, business line and functional area.</i>	Mengumpulkan skenario risiko saat ini berdasarkan kategori, lini bisnis, dan area fungsional.	1. Apakah skenario risiko I&T pernah dikategorikan (contoh: operasional, keamanan data, layanan publik)? <i>Processes:</i> risk categorization. 2. Bagaimana skenario risiko dikonsolidasikan lintas unit? <i>Information Flows:</i> laporan konsolidasi. 3. Siapa yang menyetujui agregasi risiko lintas fungsi? <i>Organizational Structures (RACI):</i> komite risiko, pimpinan.	R		
20	<i>Regularly capture all risk profile information and consolidate it into an aggregated risk</i>	Secara berkala menangkap semua informasi profil risiko dan menggabungkannya	1. Bagaimana organisasi menyatukan seluruh informasi risiko ke dalam profil risiko terkini? <i>Processes:</i> konsolidasi profil risiko. 2. Apakah ada sistem/ <i>tools</i> yang digunakan untuk	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>profile.</i>	menjadi profil risiko agregat.	mengelola profil risiko? <i>Services & Infrastructure:</i> aplikasi GRC, <i>spreadsheet</i> , dsb. 3. Bagaimana hasil konsolidasi dibagikan ke <i>stakeholder</i> ? <i>Information Flows:</i> laporan <i>risk profile</i> .			
21	<i>Capture information on the status of the risk action plan for inclusion in the I&T risk profile of the enterprise.</i>	Menangkap informasi tentang status rencana tindakan risiko untuk dimasukkan dalam profil risiko I&T perusahaan.	1. Apakah setiap tindakan mitigasi risiko memiliki <i>action plan</i> resmi? <i>Policies:</i> pedoman penyusunan <i>action plan</i> . 2. Bagaimana status pelaksanaan <i>action plan</i> dipantau? <i>Processes:</i> monitoring rencana aksi. 3. Siapa yang bertanggung jawab melaporkan progres <i>action plan</i> ? <i>Organizational Structures (RACI):</i> pemilik risiko, pimpinan unit.	R		
22	<i>Based on all risk profile data, define a set of risk indicators that allow the quick</i>	Berdasarkan semua data profil risiko, tentukan serangkaian indikator risiko yang	1. Apakah organisasi memiliki indikator risiko utama (KRI) untuk memantau tren risiko? <i>Policies:</i> definisi KRI. 2. Bagaimana KRI ditentukan dari data profil risiko?	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>identification and monitoring of current risk and risk trends.</i>	memungkinkan identifikasi dan pemantauan cepat risiko terkini dan tren risiko.	<i>Processes:</i> metode penetapan indikator. 3. Apakah indikator risiko digunakan secara rutin dalam rapat pimpinan? <i>Information Items:</i> laporan KRI. 4. Siapa yang menyetujui indikator risiko sebelum digunakan? <i>Organizational Structures (RACI):</i> pimpinan, komite risiko. KRI (<i>Key Risk Indicator</i>) = indikator pengukuran kuantitatif atau kualitatif yang digunakan organisasi			
23	<i>Capture information on I&T risk events that have materialized for inclusion in the IT risk profile of the enterprise.</i>	Menangkap informasi tentang peristiwa risiko I&T yang telah terwujud untuk dimasukkan dalam profil risiko I&T perusahaan.	1. Apakah organisasi memiliki catatan formal untuk insiden atau peristiwa risiko I&T? <i>Information Items:</i> log insiden, laporan keamanan. 2. Bagaimana data insiden dikumpulkan (manual, sistem otomatis)? <i>Processes:</i> mekanisme pencatatan insiden. 3. Siapa yang bertanggung jawab melaporkan insiden risiko I&T? <i>Organizational Structures (RACI):</i> unit operasional,	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			helpdesk TI.			
APO12.04 Articulate risk (Mengartikulasikan Risiko).						
24	Report the results of risk analysis to all affected stakeholders in terms and formats useful to support enterprise decisions. Whenever possible, include probabilities and ranges of loss or gain along with confidence levels, to enable management to balance risk-return.	Melaporkan hasil analisis risiko kepada semua pemangku kepentingan yang terpengaruh dalam bentuk dan format yang berguna untuk mendukung keputusan perusahaan. Jika memungkinkan, sertakan probabilitas dan rentang kerugian atau keuntungan beserta tingkat keyakinan, untuk memungkinkan manajemen menyeimbangkan risiko-	1. Bagaimana hasil analisis risiko disampaikan ke stakeholder? Information Flows: laporan, dashboard. 2. Apakah laporan analisis risiko mencantumkan probabilitas dan range kerugian? Information Items: format laporan risiko. 3. Siapa yang meninjau laporan analisis risiko sebelum didistribusikan? Organizational Structures (RACI): pimpinan, tim analisis.	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
		imbal hasil.				
25	<i>Provide decision makers with an understanding of worst-case and most-probable scenarios, I&T-related loss exposures and significant reputation, legal and regulatory considerations, or any other impact category as per the risk taxonomy.</i>	Memberikan para pengambil keputusan pemahaman tentang skenario terburuk dan paling mungkin, paparan kerugian terkait I&T, serta reputasi signifikan, pertimbangan hukum dan peraturan, atau kategori dampak lainnya sesuai taksonomi risiko.	1. Bagaimana pengambil keputusan mendapat gambaran skenario terburuk/terbaik dari risiko I&T? <i>Processes: briefing risiko.</i> 2. Apakah aspek reputasi, hukum, dan regulasi juga disampaikan dalam laporan risiko? <i>Policies: pedoman laporan risiko.</i> 3. Bagaimana kejelasan laporan disesuaikan dengan kebutuhan pimpinan? <i>Culture & Behavior: komunikasi yang dipahami non-teknis.</i>	R		
26	<i>Report the current risk profile to all stakeholders. Include information on the effectiveness of the risk</i>	Melaporkan profil risiko terkini kepada semua pemangku kepentingan. Sertakan informasi tentang efektivitas	1. Apakah organisasi secara rutin melaporkan profil risiko terkini ke <i>stakeholder</i> ? <i>Processes: siklus pelaporan risiko.</i> 2. Apa saja informasi yang disertakan (efektivitas kontrol, kesenjangan, status remediasi)?	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>management process, control effectiveness, gaps, inconsistencies, redundancies, remediation status and their impacts on the risk profile.</i>	proses manajemen risiko, efektivitas pengendalian, kesenjangan, inkonsistensi, redundansi, status perbaikan, dan dampaknya terhadap profil risiko.	<i>Information Items:</i> laporan profil risiko. 3. Siapa yang menerima laporan profil risiko? <i>Organizational Structures (RACI):</i> pimpinan, auditor, regulator.			
27	<i>On a periodic basis, for areas with relative risk and risk capacity parity, identify I&T-related opportunities that would allow the acceptance of greater risk and enhanced growth and return.</i>	Secara berkala, untuk area dengan risiko relatif dan paritas kapasitas risiko, mengidentifikasi peluang terkait I&T yang akan memungkinkan penerimaan risiko lebih besar dan peningkatan pertumbuhan dan laba.	1. Apakah organisasi pernah mengidentifikasi peluang I&T saat risiko relatif rendah? <i>Processes:</i> analisis peluang risiko. 2. Bagaimana peluang tersebut dievaluasi terhadap kapasitas risiko organisasi? <i>Policies:</i> pedoman evaluasi peluang. 3. Apakah ada contoh peluang I&T yang dimanfaatkan untuk pertumbuhan? <i>Information Items:</i> studi kasus peluang.	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
28	<i>Review the results of objective third-party assessments and internal audit and quality assurance reviews. Include them in the risk profile. Review identified gaps and I&T-related loss exposures to determine the need for additional risk analysis.</i>	Meninjau hasil penilaian pihak ketiga yang objektif dan tinjauan audit internal serta jaminan kualitas. Sertakan hasil tersebut dalam profil risiko. Tinjau kesenjangan yang teridentifikasi dan paparan kerugian terkait I&T untuk menentukan perlunya analisis risiko tambahan.	1. Apakah hasil audit eksternal/asesmen pihak ketiga dimasukkan ke dalam profil risiko? <i>Processes: integrasi hasil audit.</i> 2. Bagaimana kesenjangan yang ditemukan ditindaklanjuti? <i>Processes: corrective action.</i> 3. Siapa yang meninjau hasil asesmen tersebut? <i>Organizational Structures (RACI): pimpinan, auditor internal.</i>	R		
APO12.05 Define a risk management action portfolio (Menentukan portofolio tindakan manajemen risiko).						
29	<i>Maintain an inventory of control activities that are in place to mitigate risk and that enable risk to be taken</i>	Memelihara inventaris aktivitas pengendalian yang ada untuk mengurangi risiko dan yang memungkinkan	1. Apakah organisasi memiliki daftar resmi kontrol mitigasi risiko? <i>Information Items: control inventory.</i> 2. Bagaimana kontrol diklasifikasikan dan dipetakan ke skenario risiko?	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>in line with the risk appetite and tolerance. Classify control activities and map them to specific I&T risk scenarios and aggregations of I&T risk scenarios.</i>	risiko ditangani sesuai dengan selera dan toleransi risiko. Mengklasifikasikan aktivitas pengendalian dan memetakannya ke skenario risiko I&T tertentu dan agregasi skenario risiko I&T.	<i>Processes</i>: kontrol mapping. 3. Siapa yang bertanggung jawab memperbarui inventaris kontrol? <i>Organizational Structures (RACI)</i>: tim pengendalian internal, Bidang Telematika.			
30	<i>Determine whether each organizational entity monitors risk and accepts accountability for operating within its individual and portfolio tolerance levels.</i>	Menentukan apakah setiap entitas organisasi memantau risiko dan menerima akuntabilitas untuk beroperasi dalam tingkat toleransi individu dan portofolionya.	1. Apakah tiap unit organisasi diminta memantau risiko sendiri? <i>Policies</i>: aturan akuntabilitas risiko. 2. Bagaimana akuntabilitas risiko dibuktikan? <i>Information Items</i>: laporan risiko unit. 3. Siapa yang menilai apakah unit sudah sesuai toleransi? <i>Organizational Structures (RACI)</i>: manajemen risiko, pimpinan.	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
31	<i>Define a balanced set of project proposals designed to reduce risk and/or projects that enable strategic enterprise opportunities, considering costs, benefits, effect on current risk profile and regulations.</i>	Menentukan serangkaian proposal proyek yang seimbang yang dirancang untuk mengurangi risiko dan/atau proyek yang memungkinkan peluang perusahaan strategis, dengan mempertimbangkan biaya, manfaat, dampak pada profil risiko dan peraturan saat ini.	4. Bagaimana organisasi menilai proyek mitigasi risiko vs proyek peluang? <i>Processes:</i> penilaian biaya-manfaat proyek. 5. Apakah biaya, manfaat, dan regulasi dijadikan pertimbangan formal? <i>Policies:</i> pedoman seleksi proyek. 6. Siapa yang memutuskan proposal proyek mana yang dijalankan? <i>Organizational Structures (RACI):</i> pimpinan, tim perencanaan.	R		
APO12.06 Respond to risk (Menanggapi risiko).						
32	<i>Prepare, maintain and test plans that document the specific steps to take when a risk event may cause a</i>	Menyiapkan, memelihara, dan menguji rencana yang mendokumentasikan langkah-langkah	1. Apakah organisasi memiliki dokumen rencana penanganan insiden risiko I&T yang formal? <i>Policies:</i> <i>disaster recovery plan</i> (DRP), <i>business continuity plan</i> (BCP). 2. Bagaimana rencana penanganan insiden tersebut	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
	<i>significant operational or development incident with serious business impact. Ensure that plans include pathways of escalation across the enterprise.</i>	spesifik yang harus diambil ketika suatu peristiwa risiko dapat menyebabkan insiden operasional atau pengembangan yang signifikan dengan dampak bisnis yang serius. Pastikan bahwa rencana tersebut mencakup jalur eskalasi di seluruh perusahaan.	disusun? Apakah ada prosedur baku? <i>Processes:</i> mekanisme penyusunan rencana. 3. Siapa yang terlibat dalam penyusunan dan pemeliharaan rencana ini? <i>Organizational Structures (RACI):</i> tim TI, pimpinan, manajemen risiko, pihak eksternal. 4. Apakah rencana ini secara berkala diuji melalui simulasi/drill? Jika ya, seberapa sering? <i>Processes:</i> uji coba dan review periodik. 5. Apakah tersedia jalur eskalasi resmi bila insiden signifikan terjadi (contoh: siapa yang dihubungi pertama, siapa yang memberi keputusan)? <i>Information Flows:</i> diagram eskalasi, SOP eskalasi. 6. Apakah ada sarana/infrastruktur khusus untuk mendukung eksekusi rencana (misalnya backup site, hotline darurat)? <i>Services & Infrastructure:</i> fasilitas pendukung. 7. Bagaimana budaya staf dan pimpinan dalam mengikuti simulasi atau uji coba rencana (serius,			

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			formalitas, atau kurang antusias)? <i>Culture & Behavior</i>: keterlibatan dalam simulasi. 8. Apakah hasil uji coba rencana (misalnya drill bencana I&T) selalu didokumentasikan dan dipakai untuk perbaikan rencana berikutnya? <i>Information Items</i>: laporan hasil <i>drill</i>, <i>corrective action</i>.			
33	<i>Apply the appropriate response plan to minimize the impact when risk incidents occur.</i>	Menerapkan rencana respons yang tepat untuk meminimalkan dampak saat insiden risiko terjadi.	1. Apakah organisasi pernah benar-benar menerapkan rencana respons risiko I&T saat terjadi insiden besar (misalnya server <i>down</i>, kebocoran data)? <i>Information Items</i>: laporan insiden, catatan tindak lanjut. 2. Siapa yang biasanya mengambil keputusan utama ketika insiden risiko terjadi? <i>Organizational Structures (RACI)</i>: Kepala Dinas, Bidang Telematika, tim tanggap darurat. 3. Bagaimana proses koordinasi antar-unit dilakukan saat rencana respons dijalankan? <i>Processes</i>: mekanisme koordinasi lintas unit. 4. Apakah tersedia sarana pendukung untuk memfasilitasi eksekusi respons (contoh: sistem	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			monitoring <i>real-time</i>, ruang kendali)? <i>Services & Infrastructure</i>: tools dan fasilitas darurat. 5. Bagaimana budaya staf saat menghadapi insiden – apakah tenang dan mengikuti prosedur, atau panik dan improvisasi? <i>Culture & Behavior</i>: reaksi nyata staf/pimpinan. 6. Apakah hasil penerapan rencana respons dievaluasi untuk memperbaiki SOP atau prosedur yang ada? <i>Processes</i>: siklus pembelajaran pasca-insiden.			
34	<i>Categorize incidents and compare I&T-related loss exposures against risk tolerance thresholds.</i> <i>Communicate business impacts to decision makers as part of reporting and update the risk profile.</i>	Mengategorikan insiden dan bandingkan paparan kerugian terkait I&T terhadap ambang batas toleransi risiko. Komunikasikan dampak bisnis kepada para pengambil keputusan sebagai bagian dari pelaporan dan perbarui	1. Apakah insiden I&T (misalnya <i>downtime</i> aplikasi, serangan siber, kebocoran data) dikategorikan secara resmi menurut tingkat keparahan? <i>Policies</i>: SOP kategorisasi insiden. 2. Bagaimana organisasi menentukan apakah suatu insiden sudah melewati ambang batas toleransi risiko? <i>Processes</i>: mekanisme penilaian toleransi. 3. Siapa yang berwenang melakukan validasi kategori insiden dan memutuskan langkah eskalasi? <i>Organizational Structures (RACI)</i>: pejabat <i>risk owner</i>,	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
		profil risiko.	Kepala Dinas, tim TI. 4. Apakah hasil perbandingan insiden dengan toleransi risiko terdokumentasi dan masuk ke profil risiko organisasi? <i>Information Items:</i> risk register, laporan insiden. 5. Bagaimana dampak bisnis dari insiden I&T dikomunikasikan kepada pengambil keputusan? <i>Information Flows:</i> laporan resmi, rapat pimpinan, dashboard. 6. Bagaimana budaya organisasi dalam menyikapi insiden yang melewati toleransi risiko, apakah terbuka membahasnya atau cenderung menutupinya? <i>Culture & Behavior:</i> keterbukaan pimpinan/staf.			
35	<i>Examine past adverse events/losses and missed opportunities and determine root causes.</i>	Memeriksa kejadian/kerugian buruk di masa lalu dan kesempatan yang hilang, serta menentukan akar penyebabnya.	1. Apakah organisasi memiliki catatan resmi terkait insiden atau kerugian I&T di masa lalu (misalnya <i>downtime</i> panjang, kebocoran data, proyek I&T gagal)? <i>Information Items:</i> laporan insiden, audit, <i>lessons learned</i>. 2. Bagaimana organisasi menganalisis akar penyebab	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			(<i>root cause</i>) dari insiden atau kerugian tersebut? <i>Processes</i>: metode <i>root cause analysis</i> (misalnya <i>fishbone</i>, <i>5-why</i>). 3. Siapa saja yang biasanya dilibatkan dalam proses investigasi akar penyebab insiden I&T? <i>Organizational Structures (RACI)</i>: tim TI, manajemen risiko, pimpinan. 4. Apakah ada prosedur formal untuk melakukan evaluasi pasca-insiden (<i>post-mortem review</i>)? <i>Policies</i>: SOP evaluasi insiden. 5. Apakah faktor eksternal (regulasi, vendor, cuaca, tren industri) juga dipertimbangkan dalam analisis kerugian masa lalu? <i>Processes</i>: analisis faktor eksternal. 6. Bagaimana budaya organisasi dalam menyikapi insiden masa lalu, apakah terbuka mencari solusi atau cenderung menyalahkan pihak tertentu? <i>Culture & Behavior</i>: sikap staf/pimpinan. 7. Apakah hasil analisis insiden masa lalu digunakan			

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			sebagai bahan pembelajaran untuk memperbaiki kebijakan atau SOP? <i>Processes:</i> siklus perbaikan berkelanjutan.			
36	<i>Communicate root cause, additional risk response requirements and process improvements to appropriate decision makers. Ensure that the cause, response requirements and process improvement are included in risk governance processes.</i>	Mengomunikasikan akar permasalahan, persyaratan respons risiko tambahan, dan perbaikan proses kepada para pengambil keputusan yang tepat. Pastikan bahwa penyebab, persyaratan respons, dan perbaikan proses disertakan dalam proses tata kelola risiko.	1. Apakah hasil analisis akar penyebab (<i>root cause</i>) insiden I&T secara rutin disampaikan ke pimpinan atau pengambil keputusan? <i>Information Flows:</i> laporan resmi, rapat evaluasi. 2. Bagaimana organisasi memastikan bahwa kebutuhan respons tambahan (misalnya kontrol baru, peningkatan keamanan) disampaikan dengan jelas kepada pengambil keputusan? <i>Processes:</i> mekanisme eskalasi kebutuhan respons. 3. Siapa yang bertanggung jawab mengomunikasikan hasil analisis akar penyebab dan rekomendasi perbaikan? <i>Organizational Structures (RACI):</i> manajemen risiko, Kepala Bidang Telematika, tim investigasi. 4. Apakah ada kebijakan formal yang mewajibkan penyampaian hasil analisis akar penyebab kepada level	R		

APO12 Managed Risk						
No. Akt	Aspek yang Diuji			Butir Penilaian		Saran
	Activity Description	Deskripsi Aktivitas	Detail pertanyaan	R	TR	
			manajemen tertentu? <i>Policies:</i> aturan eskalasi hasil investigasi. 5. Bagaimana budaya organisasi dalam menerima rekomendasi perbaikan, apakah proaktif untuk memperbaiki atau cenderung menunda? <i>Culture & Behavior:</i> sikap pimpinan dan staf. 6. Apakah hasil rekomendasi perbaikan biasanya diintegrasikan ke dalam kebijakan atau prosedur manajemen risiko? <i>Processes:</i> pembaruan SOP, kebijakan risiko. 7. Apakah organisasi pernah mengevaluasi efektivitas perbaikan proses setelah implementasi rekomendasi? <i>Information Items:</i> laporan evaluasi, hasil audit tindak lanjut.			

Hasil Validasi Uji Instrumen FGD Oleh Ahli
Dalam Rangka Penelitian Skripsi Pengukuran Kapabilitas Manajemen Risiko
Informasi dan Teknologi (I&T) pada Dinas Komunikasi dan Informatika
Kabupaten Klungkung Menggunakan *Framework* COBIT 2019

Data Penguji Ahli

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

Hasil Instrumen FGD

1. –



Penguji Ahli,

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

NIP. 198908272019031008

Semarapura, 07 November 2025
 Peneliti,

Ketut Ananda Dharmawati

NIM 2215091035

Lampiran 6. Hasil FGD Penilaian Kapabilitas Proses

INSTRUMEN FGD

Komponen	Keterangan
Domain	EDM03 <i>Ensured Risk Optimization</i>
Tanggal	Jumat, 14 November 2025
Tempat	Ruang Kepala Dinas
Metode	<i>Focus Group Discussion</i> (FGD)
Peneliti	Ketut Ananda Dharmawati-2215091035
Informan	1. Kepala Dinas Komunikasi dan Informatika Kabupaten Klungkung 2. Kepala Bidang Telematika (atau yang mewakili) 3. Kepala Bidang Statistik dan Persandian (atau yang mewakili) 4. Kepala Bidang Komunikasi (atau yang mewakili) 5. JF Perencana Ahli Muda 6. JF Sandiman Ahli Muda

PETUNJUK PENGISIAN INSTRUMEN CETAK FGD

Instrumen ini digunakan oleh peneliti sebagai lembar kerja utama selama proses FGD dengan informan. Pengisian dilakukan secara manual selama FGD berlangsung. Panduan berikut menjelaskan cara penggunaan setiap kolom agar hasil pencatatan konsisten dan dapat dipertanggungjawabkan:

1. Kolom “Detail Pertanyaan”

Berisi daftar pertanyaan turunan dari setiap aktivitas COBIT 2019. Peneliti membacakan satu per satu pertanyaan kepada informan sesuai urutan aktivitas (EDM03.01 s.d. APO12.06). Pertanyaan tidak perlu dibaca secara kaku; peneliti boleh melakukan *probing* (pertanyaan lanjutan) untuk memperjelas jawaban informan.

2. Kolom “Jawaban Informan”

Diisi dengan ringkasan jawaban informan menggunakan kalimat singkat dan faktual, tanpa interpretasi. Bila ada perbedaan pendapat antar informan, tulis semua variasi secara ringkas dengan menyebutkan jabatan informan.

3. Kolom “Bukti Dokumen yang Ditunjukkan”

Diisi dengan nama dokumen yang disebutkan atau ditunjukkan informan (misalnya *Risk Register 2025*, *SOP Keamanan Informasi*, *Renstra Diskominfo*). Bila dokumen belum sempat diverifikasi, beri catatan “belum dicek” di kolom Catatan Peneliti.

4. Kolom “Status (N/P/L/F)”

Setelah FGD selesai, peneliti memberikan penilaian awal terhadap tiap aktivitas menggunakan skala NPLF:

N (Not Achieved): Aktivitas tidak dilakukan / tidak ada bukti. Kurang dari 15%

P (Partially Achieved): Aktivitas sebagian dijalankan, tetapi belum konsisten atau belum ada bukti lengkap. (15–50%)

L (Largely Achieved): Aktivitas sebagian besar sudah berjalan, bukti tersedia, namun ada kekurangan minor. (50–85%)

F (Fully Achieved): Aktivitas sepenuhnya diterapkan, bukti lengkap dan konsisten dengan deskripsi COBIT 2019. (>85%)

Penilaian akhir dapat dikonfirmasi kembali setelah verifikasi dokumen (studi dokumentasi).

5. Kolom “Catatan Peneliti”

Digunakan untuk mencatat klarifikasi penting, inkonsistensi, atau temuan tambahan selama FGD. Misalnya: “dokumen ada tapi belum ditandatangani pimpinan” atau “praktik informal belum tertulis dalam SOP”.

Tujuan	
<i>Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.</i>	Memastikan bahwa risiko perusahaan yang terkait dengan I&T tidak melebihi selera risiko dan toleransi risiko perusahaan, dampak risiko I&T terhadap nilai perusahaan diidentifikasi dan dikelola, dan potensi kegagalan kepatuhan diminimalkan.

EDM03 Ensured Risk Optimization						
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
EDM03.01 Evaluate risk management (Mengevaluasi manajemen risiko).						
1	Memahami organisasi dan konteksnya terkait dengan risiko I&T..	1. Apakah organisasi memiliki dokumen yang menggambarkan risiko I&T dalam konteks pelayanan publik (misalnya Renstra Diskominfo atau <i>Masterplan I&T</i>)? <i>Policies</i>: aturan tertulis, rencana strategis. 2. Bagaimana pimpinan mengidentifikasi faktor eksternal (peraturan pemerintah, ancaman siber nasional) yang dapat memengaruhi risiko I&T? <i>Processes</i>: prosedur evaluasi eksternal. 3. Apakah ada forum khusus untuk membahas faktor internal yang menambah risiko I&T (misalnya keterbatasan SDM, anggaran, atau infrastruktur)?	Ada Mengidentifikasi kasi melalui forum / rapat Ada Forum Konsultasi Publik	Renstra Perbup 21/2023 Masterplan SC Notulen Rapat SK Tim Tanggap Insiden Siber Tahun 2023 Notulen rapat etap lengkap Diskominfo	F (Fully Achieved)	Valid Dokumen sudah dicek Surat forum OPD 4 Maret 2023.pdf Disebut, belum diverifikasi peneliti

✓
Diverifikasi pada studi tahap 2

✓

EDM03 Ensured Risk Optimization						
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
		<i>Organizational Structures</i>: siapa yang ikut forum (Kepala Dinas, Bidang TI). 4. Bagaimana risiko I&T dipetakan terhadap layanan publik yang dikelola Diskominfo (contoh: <i>e-government</i>, data kependudukan)? <i>Processes</i>: cara organisasi memetakan risiko. 5. Apakah hasil identifikasi konteks risiko I&T biasanya didokumentasikan? <i>Information Items</i>: notulen rapat, <i>risk register</i>. 6. Bagaimana budaya pimpinan/staf dalam membahas risiko I&T, terbuka, formal, atau memiliki kecenderungan menutupi masalah? <i>Culture & Behavior</i>: kebiasaan staf/pimpinan.	Dipetakan dalam risk register OPO Terdokumentasi Terbuka	Risk Register 2025 TTE.pdf beserta lampiran Form 4, 5, 9 Risk Register 2025 TTE.pdf Notulen rapat staf lengkap diskominfo Laporan Evaluasi Risiko Semester I 2025		Valid Dokumen sudah dicek Valid Sudah diverifikasi dalam studi dokumen tahap 1 Berdasarkan wawancara langsung, blm ada bukti dok setelah studi lanjutan ditaman kan bukti ✓
2	Menentukan selera risiko organisasi, yaitu tingkat risiko terkait I&T yang	1. Apakah organisasi memiliki pernyataan formal tentang tingkat risiko I&T yang masih bisa ditoleransi? <i>Policies</i>: dokumen tingkat risiko SK, kebijakan risiko. 2. Siapa yang berwenang menentukan dokumen tingkat risiko organisasi?	Ada Pimpinan	Surat Laporan x Risk Register 2025. Renstra 2024-2026 SK TTIS Tahun 2025	L (Largely Achieved)	Valid Dokumen sudah dicek Disebut narasumber, belum diverifikasi ✓

EDM03 Ensured Risk Optimization						
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	bersedia diambil perusahaan dalam mengejar tujuan perusahaan.	<i>Organizational Structures (RACI)</i>: Kepala Dinas, Sekda, atau komite. 3. Apakah dokumen tingkat risiko berbeda untuk tiap bidang (contoh: keamanan data vs layanan jaringan)? <i>Processes</i>: cara organisasi menetapkan dokumen tingkat risiko berbeda. 4. Bagaimana dokumen tingkat risiko dikaitkan dengan tujuan strategis Diskominfo (misalnya digitalisasi layanan publik)? <i>Information Items</i>: strategi TI, KPI organisasi. 5. Apakah dokumen tingkat risiko pernah direvisi/ditinjau ulang secara berkala? <i>Processes</i>: siklus review. 6. Bagaimana pimpinan menyampaikan dokumen tingkat risiko kepada staf teknis? <i>Information Flows</i>: rapat, edaran, sosialisasi. 7. Apakah ada contoh nyata risiko yang dianggap “masih bisa diterima”? <i>Culture & Behavior</i>: contoh sikap pimpinan/staf.	Berbeda Berdasarkan laporan dari masing-masing bidang dipermulési oleh Suprog dibandingkan dengan tujuan organisasi Ditinjau berkala tiap tahun Penyampaian Tatap muka, Rapat staf, Media daring Disiplin, Pola komunikasi	Risk Register Lampiran 1-3 Renstra PERBUP 21/2023 Laporan Evaluasi SMT 1 2023 Notulen rapat Risk Register 2023 TTE		Tidak disebut narasumber Valid Dokumen sudah dicek Valid Dokumen sudah dicek Tidak ditemukan ada notulen rapat Valid Dokumen sudah dicek

✓
Ditemukan saat studi dokumen

↓
Diversifikasi pada studi bab 2

EDM03 Ensured Risk Optimization						
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
3	Menentukan tingkat toleransi risiko terhadap selera risiko, yaitu penyimpangan yang dapat diterima sementara dari selera risiko.	1. Apakah organisasi memiliki standar formal terkait toleransi risiko (misalnya <i>downtime server</i> maksimal 30 menit)? <i>Policies</i>: SLA, SOP. 2. Bagaimana proses penetapan batas toleransi risiko dilakukan? <i>Processes</i>: prosedur penetapan toleransi. 3. Apakah toleransi berbeda antara sistem kritis (contoh: data kependudukan) dan sistem pendukung (contoh: website informasi)? <i>Information Items</i>: dokumen SLA/kontrak. 4. Siapa yang memutuskan kapan suatu risiko sudah melampaui toleransi dan harus diekskalasi? <i>Organizational Structures (RACI)</i>: pejabat yang berwenang. 5. Bagaimana toleransi risiko dikomunikasikan ke staf operasional? <i>Information Flows</i>: SOP, pelatihan, <i>briefing</i>. 6. Apakah pernah terjadi pelanggaran batas toleransi risiko? Bagaimana tindak lanjutnya? <i>Processes</i>: tindakan korektif.	Ada Rapat Berbeda Pimpinan Dengan Briefing Sampai saat ini belum	SOP Risk Register - SOP Pengelolaan Web OPD, SOP Server (VPS) Briefing langsung	P (Partially Achieved)	No. 29, 34, 35, 43-47 dlm bab 500 Tidak disebut narasumber Tidak disebut narasumber, Ditemukan pada studi dokumentasi

✓ Ditemukan saat studi dokumen tahap 2

EDM03 Ensured Risk Optimization						
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
		7. Apakah toleransi risiko dipengaruhi oleh regulasi eksternal (misalnya standar keamanan nasional)? <i>Culture & Behavior</i>: kesadaran staf terhadap aturan luar. 8. Bagaimana organisasi membedakan toleransi jangka pendek (sementara) dengan <u>risk appetite</u> jangka panjang? <i>dokumen tingkat risiko</i> <i>Processes</i>: mekanisme pembedaan.	Iya dipengaruhi Menggunakan standar nasional	PERBUP 87/2019 PERBUP 21/2023 Risk Register Laporan Evaluasi SMT 1 2025		Bukti tidak disebut, ditemukan saat studi dokumen Valid RG → pendek LE → panjang
4	Menentukan tingkat keselarasan strategi risiko I&T dengan strategi risiko perusahaan dan memastikan selera risiko berada di bawah kapasitas	1. Apakah strategi risiko I&T pernah dibandingkan atau diselaraskan dengan strategi risiko organisasi secara keseluruhan? <i>Processes</i>: mekanisme evaluasi strategi. 2. Siapa yang bertanggung jawab memastikan keselarasan ini? <i>Organizational Structures (RACI)</i>: Kepala Dinas, Komite Risiko (divisi / tim ad-hoc). 3. Apakah ada dokumen yang menunjukkan integrasi antara strategi risiko I&T dan strategi risiko organisasi? <i>Information Items</i>: risk strategy document, Renstra, laporan risiko.	Pernah Pimpinan Ada	Arsitektur SPBE sesuai standar nasional Renstra Risk Register Laporan Evaluasi Risiko SMT 1 2025	L (Largely Achieved)	Valid Diverifikasi pada studi tahap 2 Valid Dokumen sudah direk + Ditemukan saat studi dokumen

EDM03 Ensured Risk Optimization						
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	risiko organisasi.	4. Bagaimana pimpinan memastikan bahwa <i>risk appetite</i> I&T tidak melebihi kapasitas risiko organisasi? <i>Policies</i>: prinsip atau batas resmi dalam dokumen. 5. Apakah ada forum lintas unit (I&T dan non-I&T) untuk meninjau keselarasan strategi risiko? <i>Organizational Structures</i>: kolaborasi antar-unit. 6. Apakah ada contoh keputusan strategis yang memperlihatkan keterkaitan langsung antara risiko I&T dan strategi organisasi? <i>Culture & Behavior</i>: kesadaran pimpinan.	Disesuaikan dengan Renstra Ada dengan Brieda Ada TTIS	Surat forum OPD 4 Maret 2025 TTE. PAF Notulen rapat staf lengkap (Telanah staf 1)		Valid Diverifikasi pada studi tahap 2 Minta ke Pak MS
5	Mengevaluasi faktor risiko I&T secara proaktif sebelum mengambil keputusan strategis perusahaan dan	1. Apakah organisasi selalu menilai risiko I&T sebelum mengambil keputusan strategis (misalnya terkait digitalisasi layanan)? <i>Processes</i>: <i>risk assessment</i> pra-keputusan. 2. Siapa yang wajib memberikan masukan risiko I&T dalam rapat pengambilan keputusan strategis? <i>Organizational Structures (RACI)</i>: Kepala Dinas, Bidang TI. 3. Apakah ada prosedur baku yang mengatur penyampaian risiko I&T sebelum keputusan dibuat? <i>Policies</i>: SOP, aturan rapat.	Ya Seluruh staf Tidak ada	Risk Register 2025 TTE Renstra 2024-2026	L (Largely Achieved)	Valid Dokumen sudah dicek

✓ Valid Diverifikasi pada studi tahap 2

EDM03 Ensured Risk Optimization						
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	memastikan bahwa pertimbangan risiko menjadi bagian dari proses pengambilan keputusan strategis perusahaan.	4. Bagaimana informasi risiko I&T disampaikan ke pimpinan sebelum keputusan? <i>Information Flows</i>: notulen, laporan, presentasi. 5. Apakah faktor risiko I&T selalu menjadi agenda dalam rapat pimpinan strategis? <i>Policies</i>: tata tertib rapat. 6. Bagaimana pimpinan merespons masukan risiko I&T dalam rapat? <i>Culture & Behavior</i>: sikap pimpinan terhadap masukan risiko. 7. Apakah ada kasus nyata di mana keputusan strategis berubah karena pertimbangan risiko I&T? <i>Processes</i>: bukti integrasi risiko ke pengambilan keputusan. 8. Apakah hasil evaluasi risiko I&T terdokumentasi sebagai bahan pembelajaran untuk keputusan berikutnya? <i>Information Items</i>: laporan evaluasi, lessons learned.	Laporan lisan tertulis setelah menjadi dokumen Tidak selalu Merespons secara terbuka Belum ada Iya	— Laporan Risiko Evaluasi		SMT 1 2015 TTD.pdf Valid
6	Mengevaluasi aktivitas manajemen risiko untuk	1. Apakah ada evaluasi formal terhadap kegiatan manajemen risiko I&T? <i>Processes</i>: audit internal, review tahunan.	Ada, laporan dibuat tiap semester	Laporan Evaluasi Risiko	F (Fully Achieved)	Valid Dokumen sudah dicek

EDM03 Ensured Risk Optimization						
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	memastikan keselarasan dengan kapasitas perusahaan terhadap kerugian terkait I&T dan toleransi pimpinan terhadap kerugian tersebut..	2. Bagaimana organisasi memastikan kegiatan manajemen risiko sesuai kapasitas keuangan atau sumber daya? <i>Policies</i>: batas anggaran, pedoman alokasi SDM. 3. Apakah pimpinan menetapkan batas toleransi kerugian terkait I&T (misalnya <i>downtime</i> maksimal, batas kehilangan data)? <i>Organizational Structures (RACI)</i>: pimpinan, dewan. 4. Bagaimana hasil evaluasi manajemen risiko I&T dilaporkan? <i>Information Items</i>: laporan risiko, hasil audit. 5. Apakah kegiatan manajemen risiko I&T pernah dikoreksi karena dianggap melampaui kapasitas organisasi? <i>Processes</i>: <i>corrective actions</i>. 6. Bagaimana sikap pimpinan terhadap hasil evaluasi yang menunjukkan potensi kerugian besar? <i>Culture & Behavior</i>: penerimaan pimpinan atas risiko. 7. Apakah ada mekanisme eskalasi jika aktivitas manajemen risiko I&T dinilai tidak sesuai kapasitas organisasi? <i>Information Flows</i>: jalur eskalasi resmi.	Dengan Renja Iya menetapkan Dilaporkan tiap bulan Belum Menerima dan memaklumi, mengevaluasi Ada melalui pelaporan / surat	Dokumen Renja La Laporan Evaluasi Risiko Tidak ada notulen rapatnya		Dokumen belum dicek Minta ke Pak D Valid, tetapi tiap semester (periode 6 bulan)
7	Merekrut dan mempertahankan	1. Apakah organisasi memiliki staf khusus yang menangani manajemen risiko I&T?	Ada	SK TTIS	L	Dokumen belum dicek Minta ke Pak S

✓
Valid diverifikasi pada studi tahap 2

✓
Valid

EDM03 Ensured Risk Optimization						
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	an keterampilan dan personel yang diperlukan untuk Manajemen Risiko I&T.	<i>Organizational Structures (RACI)</i>: posisi formal di struktur organisasi. 2. Bagaimana organisasi mengidentifikasi kebutuhan keterampilan staf untuk manajemen risiko I&T? <i>Processes</i>: analisis kebutuhan SDM. 3. Apakah tersedia program pelatihan internal maupun eksternal atau sertifikasi khusus untuk staf terkait risiko I&T? <i>People, Skills & Competencies</i>: pelatihan, <i>workshop</i>. 4. Bagaimana organisasi memastikan staf baru memahami kebijakan manajemen risiko I&T? <i>Policies</i>: materi induksi/briefing. 5. Apakah ada program retensi untuk mempertahankan staf yang kompeten di bidang risiko I&T? <i>Culture & Behavior</i>: penghargaan, promosi. 6. Bagaimana organisasi mengatasi kekurangan staf berkompeten di bidang risiko I&T? <i>Processes</i>: strategi rekrutmen, outsourcing.	Menyusun Renja Ada Eksternal Dengan Briefing Arahan Belum Melalui surat penugasan	Dokumen Renja Laporan Work-shop penguatan TTIS 5-3 November 2025.pdf SK TTIS	(Largely Achieved)	Dokumen belum dicek Minta ke Pak O. Umma Minta ke Pak S Minta ke Pak S

EDM03 Ensured Risk Optimization						
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
		7. Apakah ada perencanaan jangka panjang untuk pengembangan kompetensi staf risiko I&T? <i>Policies:</i> dokumen HR, Renstra SDM. 8. Bagaimana organisasi memanfaatkan infrastruktur (contoh: <i>e-learning, platform</i> pelatihan <i>online</i>) untuk mendukung pengembangan staf? <i>Services & Infrastructure:</i> sistem pendukung pelatihan. 9. Apakah kompetensi staf di bidang risiko I&T pernah dievaluasi secara formal (misalnya melalui asesmen)? <i>People, Skills & Competencies:</i> uji kompetensi.	Ada Dengan CORPU (corporate university) Belum	Renstra 2024-2026. pap Halaman CORPU di Web CSIRT		Valid Dokumen sudah dicek Valid terbatas. Peneliti terlibat dalam project pembantuan sehingga penilaian validitas didasarkan pada keberadaan dan pemanfaatan aktual.
EDM03.02 Direct risk management (Mengarahkan manajemen risiko).						
8	Mengarahkan penerjemahan dan integrasi strategi risiko I&T ke dalam praktik manajemen risiko dan	1. Apakah strategi risiko I&T yang dimiliki organisasi sudah diterjemahkan menjadi praktik operasional sehari-hari? <i>Processes:</i> bukti implementasi dalam SOP atau <i>workflow</i>. 2. Siapa yang bertanggung jawab memastikan strategi risiko I&T diintegrasikan ke kegiatan operasional? <i>Organizational Structures (RACI):</i> Kepala Dinas, Bidang TI, tim manajemen risiko.	Iya Sudah Kepala Dinas	Masuk ruangan dengan Sidik Jari	F (Fully Achieved)	Valid Ada SOP (No. 29, 34, 35, 43-47) dan tabel sop

EDM03 Ensured Risk Optimization							
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti	
	aktivitas operasional.	3. Apakah ada dokumen yang menjelaskan bagaimana strategi risiko I&T diturunkan ke tingkat operasional? <i>Information Items</i>: pedoman, manual kerja, SOP. 4. Bagaimana organisasi memastikan staf memahami strategi risiko I&T dalam pekerjaannya sehari-hari? <i>Culture & Behavior</i>: komunikasi & sosialisasi. 5. Apakah ada rapat rutin untuk meninjau sejauh mana strategi risiko I&T dijalankan di <i>level</i> operasional? <i>Information Flows</i>: laporan rapat, notulen. 6. Apakah terdapat contoh nyata kegiatan operasional yang sudah menyesuaikan strategi risiko I&T? <i>Processes</i>: contoh implementasi. 7. Bagaimana organisasi mengukur efektivitas integrasi strategi risiko I&T ke operasional? <i>Policies</i>: indikator kinerja, KPI. 8. Apakah strategi risiko I&T pernah gagal diterapkan di lapangan? Jika ya, apa penyebabnya? <i>Processes</i>: evaluasi kegagalan.	Ada Komunikasi Sosialisasi Ada Iya ada hanya admin baru password Dengan capaian indikator kinerja Tidak	SOP Risiko TI (No. 20.34, 35, 43-47) Laporan Workshop Telaah Staf SOP Risiko TI (No. 35, 43-47) Renstra 2024-2026 Laporan Evaluasi Risiko PMTI Laporan Evaluasi Rengas TW II 2023		Disebut Narasumber, Valid Dokumen sudah di cek Minta ke Pak S Minta ke Pak Mang S Tidak disebut narasumber Diverifikasi sebagian Ada Rekap IKK	✓ Valid diverifikasi pada studi tahap 2 ✓ Valid ✓ ditemukan saat studi dokumentasi ✓ Valid diverifikasi lanjutan pada tahap 2

EDM03 Ensured Risk Optimization						
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
9	Mengarahkan pengembangan rencana komunikasi risiko (mencakup semua tingkatan perusahaan).	1. Apakah organisasi memiliki rencana komunikasi risiko yang formal dan tertulis? <i>Policies</i>: dokumen komunikasi risiko. 2. Siapa yang bertanggung jawab mengembangkan rencana komunikasi risiko? <i>Organizational Structures (RACI)</i>: Bidang TI, Sekretariat, pimpinan. 3. Bagaimana informasi risiko disampaikan ke level pimpinan, staf teknis, dan pemangku kepentingan eksternal? <i>Information Flows</i>: jalur komunikasi resmi. 4. Apakah ada perbedaan cara komunikasi risiko untuk level manajemen dan staf operasional? <i>Processes</i>: metode komunikasi berbeda. 5. Bagaimana budaya organisasi memengaruhi keterbukaan dalam komunikasi risiko? <i>Culture & Behavior</i>: keterbukaan vs tertutup. 6. Apakah ada pelatihan atau sosialisasi mengenai komunikasi risiko? <i>People, Skills & Competencies</i>: program pelatihan.	Tidak memiliki Sekretariat (Tu) Forum Konsultasi Publik Tidak Terbuka Belum	Tidak ada notulen	P (Partially Achieved)	

EDM03 Ensured Risk Optimization						
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
		7. Bagaimana efektivitas komunikasi risiko dievaluasi? <i>Processes:</i> feedback, survei kepuasan komunikasi.	Melalui SPI (Sasaran Penguasaan Internal)	Laporan Evaluasi Risiko SMT 1 2025		Valid
10	Mengarahkan penerapan mekanisme yang tepat untuk merespons perubahan risiko dengan cepat dan segera melaporkannya ke tingkat manajemen yang sesuai, didukung oleh prinsip-prinsip eskalasi yang	1. Apakah organisasi memiliki mekanisme resmi untuk merespons perubahan risiko I&T secara cepat? <i>Processes:</i> prosedur tanggap risiko. 2. Bagaimana staf melaporkan risiko baru atau perubahan risiko yang muncul? <i>Information Flows:</i> jalur pelaporan resmi. 3. Siapa yang bertugas menerima dan menindaklanjuti laporan risiko baru? <i>Organizational Structures (RACI):</i> pejabat pengelola risiko. 4. Apakah ada peningkatan yang jelas (apa yang dilaporkan, kapan, kepada siapa)? <i>Policies:</i> dokumen rencana tindak lanjut 5. Bagaimana organisasi memastikan laporan risiko segera sampai ke pimpinan terkait? <i>Processes:</i> mekanisme komunikasi cepat.	Tidak Dengan telah siap Sunprog Ada Dengan mencari TTD	 SOP No. 34 dan SOP No. 29 Dokumen rencana tindak lanjut ada di laporan Evaluasi Risiko SMT 1 2025	L (Largely Achieved)	Tidak disebut narasumber Valid ✓ ditemukan saat studi dokumentasi

EDM03 Ensured Risk Optimization						
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	disepakati (apa yang harus dilaporkan, kapan, di mana, dan bagaimana).	6. Apakah tersedia media khusus untuk laporan risiko darurat (misalnya <i>hotline</i>, aplikasi <i>internal</i>)? <i>Services & Infrastructure</i>: sistem pelaporan. 7. Apakah ada contoh kasus nyata di mana eskalasi risiko berhasil dilakukan dengan cepat? <i>Processes</i>: studi kasus. 8. Bagaimana pimpinan biasanya menanggapi laporan eskalasi risiko? <i>Culture & Behavior</i>: respons pimpinan. 9. Apakah efektivitas mekanisme eskalasi risiko pernah dievaluasi secara formal? <i>Information Items</i>: laporan evaluasi.	Ada pengaduan di web Belum ada Responsif Belum	Website CSIRT Laporan Monitoring Web Terdampak Serangan Cyber Mei 2021		Ditemukan saat studi dokumentasi Ada
11	Mengarahkan agar risiko, peluang, isu, dan kekhawatiran dapat diidentifikasi	1. Apakah ada kebijakan yang memperbolehkan semua pegawai melaporkan risiko atau isu tanpa batasan hierarki? <i>Policies</i>: kebijakan pelaporan terbuka 2. Bagaimana staf biasanya menyampaikan risiko, peluang, atau isu yang mereka temukan? <i>Information Flows</i>: jalur komunikasi resmi maupun informal.	Tidak Komunikasi secara langsung di kantor		P (Partially Achieved)	

EDM03 Ensured Risk Optimization						
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	dan dilaporkan oleh siapa pun kepada pihak yang tepat kapan saja. Risiko harus dikelola sesuai dengan kebijakan dan prosedur yang dipublikasikan dan dieskalasikan kepada para pengambil keputusan yang relevan.	3. Siapa yang menerima laporan risiko dari staf? <i>Organizational Structures (RACI)</i>: pejabat penerima laporan. 4. Apakah laporan risiko bisa dilakukan secara anonim untuk menghindari hambatan budaya? <i>Culture & Behavior</i>: keberanian/keterbukaan staf. 5. Apakah organisasi menyediakan media resmi untuk laporan terbuka (aplikasi, kotak saran, hotline)? <i>Services & Infrastructure</i>: sarana pelaporan. 6. Apakah ada prosedur bagaimana laporan staf ditindaklanjuti? <i>Processes</i>: alur tindak lanjut. 7. Apakah peluang yang dilaporkan staf juga dipertimbangkan sebagai masukan strategis? <i>Processes</i>: integrasi peluang ke strategi. 8. Apakah ada contoh nyata risiko/isu dari staf yang berhasil mencegah masalah besar di organisasi? <i>Information Items</i>: catatan kasus.	Kepala Bidang Tidak Iya menyediakan Ada Iya dipertimbangkan Serangan DDOS pada jaringan digital Disko-minfo	Aplikasi Klungkung Mesadu SOP No. 29, 34 dan 35 Renstra 2021-2026 Laporan Bidang Telematika ke pimpinan		Valid Valid Minta ke Pakta Telematika

✓
Diverifikasi pada studi tahap 2

EDM03 Ensured Risk Optimization						
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
12	Mengidentifikasi tujuan dan metrik utama dari proses tata kelola dan manajemen risiko yang akan dipantau, dan menyetujui pendekatan, metode, teknik, dan proses untuk menangkap dan melaporkan informasi pengukuran.	1. Apakah organisasi memiliki tujuan utama yang jelas untuk tata kelola risiko I&T? <i>Policies</i>: dokumen tujuan risiko. 2. Bagaimana indikator keberhasilan manajemen risiko I&T ditentukan? <i>Processes</i>: penetapan KPI. 3. Siapa yang menyetujui metrik dan indikator risiko yang digunakan? <i>Organizational Structures (RACI)</i>: pimpinan, komite risiko. 4. Apakah ada metode formal untuk mengukur kinerja manajemen risiko? <i>Processes</i>: teknik pengukuran, audit. 5. Bagaimana informasi hasil pengukuran risiko disampaikan ke pimpinan? <i>Information Flows</i>: laporan kinerja. 6. Apakah organisasi menggunakan sistem/tools untuk mengumpulkan data metrik risiko? <i>Services & Infrastructure</i>: aplikasi monitoring.	Iya Dengan Risk Register Pimpinan Dengan Risk Register Dengan pelaporan Tidak ada	Renja Risk Register SK Nomor 23 Tahun 2025 Risk Register Laporan Evaluasi Laporan Evaluasi Risiko SMT I LAP_110102-2025-032-20250702-1427-ASET.xlsx	F (Fully Achieved) valid valid valid valid Ditemukan saat studi dokumentasi	Dokumen belum dicek Minta ke Pak D Valid Valid diverifikasi pada studi tahap 2 Ada Spreadsheet

EDM03 Ensured Risk Optimization						
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
		7. Bagaimana pimpinan menilai apakah indikator risiko sesuai dengan tujuan strategis? <i>Culture & Behavior</i>: kesadaran pimpinan. 8. Apakah hasil <i>monitoring</i> indikator risiko terdokumentasi secara rutin? <i>Information Items</i>: laporan bulanan, tahunan. 9. Apakah metrik risiko pernah direvisi karena dianggap tidak relevan? <i>Processes</i>: siklus perbaikan metrik.	Menilai berdasarkan dampaknya Iya tahunan Pernah dengan BSNN	Risk Register Risk Register 2025 TTE.pdf (form baru)		Valid Valid
EDM03.03 Monitor risk management (Memantau manajemen risiko).						
13	Melaporkan setiap permasalahan terkait manajemen risiko kepada Dewan Komisaris atau komite	1. Apakah organisasi memiliki mekanisme resmi untuk melaporkan masalah manajemen risiko ke pimpinan/komite eksekutif? <i>Policies</i>: aturan pelaporan risiko. 2. Siapa yang bertanggung jawab menyusun laporan masalah manajemen risiko ke pimpinan? <i>Organizational Structures (RACI)</i>: Bidang TI, Kepala Dinas.	Ada, melalui surat Bidang TI	Laporan Evaluasi SK Nomor 23 Tahun 2021	F (Fully Achieved)	Valid Valid

EDM03 Ensured Risk Optimization						
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	eksekutif.	3. Bagaimana laporan masalah manajemen risiko biasanya disampaikan? (tertulis, presentasi, rapat) <i>Information Flows:</i> media komunikasi. 4. Apakah laporan masalah manajemen risiko terdokumentasi secara formal? <i>Information Items:</i> notulen, laporan resmi. 5. Bagaimana sikap pimpinan saat menerima laporan masalah manajemen risiko? <i>Culture & Behavior:</i> keseriusan pimpinan menindaklanjuti.	Tertulis Iya Menanggapi dengan serius dan mencari solusi	Notulen rapat staf Laporan Evaluasi		Valid Valid
14	Memantau sejauh mana profil risiko dikelola dalam selera risiko dan ambang batas toleransi perusahaan.	1. Apakah organisasi memantau apakah profil risiko I&T sesuai dengan dokumen tingkat risiko dan <i>tolerance</i> yang telah ditetapkan? <i>Processes:</i> mekanisme monitoring. 2. Siapa yang memantau kesesuaian profil risiko terhadap dokumen tingkat risiko? <i>Organizational Structures (RACI):</i> pejabat <i>risk owner</i>. 3. Apakah ada sistem/<i>tools</i> yang digunakan untuk memantau profil risiko? <i>Services & Infrastructure:</i> aplikasi <i>monitoring</i>.	Iya Sunprog Belum	Risk Register 2025 TTE.pdf Laporan Evaluasi Risiko SMT 2025.pdf	L (Largely Achieved)	Valid

EDM03 Ensured Risk Optimization						
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
		4. Bagaimana hasil pemantauan disampaikan ke pimpinan? <i>Information Flows</i>: laporan periodik. 5. Apakah profil risiko pernah melebihi batas tolerance? <i>Information Items</i>: bukti laporan pelanggaran. 6. Bagaimana budaya organisasi ketika terjadi pelanggaran peningkatan risiko/tolerance? <i>Culture & Behavior</i>: reaksi staf/pimpinan. 7. Apakah hasil monitoring digunakan untuk memperbarui strategi risiko I&T? <i>Processes</i>: siklus perbaikan.	Laporan Tidak Belum pernah Belum	Laporan Evaluasi Risk Register (ada pembaruan dan mitigasi risiko)		Valid Ditemukan saat studi dokumentasi
15	Memantau tujuan dan metrik utama tata kelola risiko dan proses manajemen terhadap target,	1. Apakah organisasi memiliki target jelas untuk tujuan dan metrik tata kelola risiko TI? <i>Policies</i>: dokumen KPI risiko. 2. Bagaimana kinerja tata kelola risiko I&T dipantau dan dibandingkan terhadap target? <i>Processes</i>: metode <i>monitoring</i>. 3. Siapa yang melakukan analisis jika ada penyimpangan dari target? <i>Organizational Structures (RACI)</i>: unit analisis, pimpinan.	Iya Evaluasi Pengelola risiko Pimpinan	Risk Register Renstra 2024-2025.pdf Laporan Evaluasi SMT 1 2025 SK Nomor 23 Tahun 2025	L (Largely Achieved)	Valid Valid Valid

Digunakan

EDM03 Ensured Risk Optimization						
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	menganalisis penyebab penyimpangan, dan mengambil tindakan perbaikan untuk mengatasi penyebab yang mendasarinya.	4. Apakah hasil monitoring metrik risiko terdokumentasi? <i>Information Items</i>: laporan kinerja risiko. 5. Apakah penyebab penyimpangan risiko biasanya dicatat dan dianalisis? <i>Processes</i>: root cause analysis. 6. Bagaimana budaya pimpinan saat membahas penyimpangan risiko? Apakah mencari solusi atau menyalahkan? <i>Culture & Behavior</i>: sikap pimpinan. 7. Apakah organisasi memiliki prosedur untuk tindakan korektif bila metrik risiko menyimpang jauh dari target? <i>Policies</i>: pedoman tindakan korektif. 8. Apakah remedial action pernah berhasil mengembalikan kinerja risiko ke target? <i>Processes</i>: contoh nyata <i>corrective action</i>.	Iya Tidak ada Mencari solusi Tidak memiliki Belum	RTP terdapat pada bagian RTL di Laporan Evaluasi Risiko SMT 1 2025.pdf		Minta ke Pak KA Telematika
16	Memungkinkan peninjauan oleh pemangku kepentingan	1. Apakah pemangku kepentingan (internal maupun eksternal) dilibatkan dalam peninjauan kemajuan pencapaian tujuan risiko I&T? <i>Organizational Structures (RACI)</i>: pemangku kepentingan utama.	Dilibatkan	Berita Acara Forum OPD 2025. pdf Surat Forum OPD 4 Maret 2025. pdf	F (Fully Achieved)	Dokumen belum dicek

Valid ditemukan saat studi dokumentasi tahap 2

✓ Valid diverifikasi pada studi dokumentasi tahap 2

EDM03 Ensured Risk Optimization							
No. Akt	Deskripsi Aktivitas	Detail Pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti	
	utama atas kemajuan perusahaan terhadap tujuan yang telah ditetapkan.	2. Apakah ada forum khusus untuk melakukan peninjauan bersama pemangku kepentingan? <i>Processes</i>: rapat evaluasi, forum koordinasi. 3. Bagaimana hasil peninjauan pemangku kepentingan didokumentasikan? <i>Information Items</i>: notulen, laporan hasil peninjauan 4. Apakah masukan pemangku kepentingan digunakan untuk memperbaiki manajemen risiko I&T? <i>Processes</i>: siklus perbaikan. 5. Bagaimana budaya organisasi dalam menerima masukan dari pemangku kepentingan? <i>Culture & Behavior</i>: keterbukaan terhadap kritik. 6. Apakah organisasi menggunakan laporan khusus untuk menunjukkan progres kepada pemangku kepentingan? <i>Information Flows</i>: laporan publik, dashboard.	Ada Menggunakan Zoom Iya Terbuka, bisa menerima kritik Menggunakan	Forum Konsultasi Publik Ada Rekaman Dokumen Renjo Rancangan Final Laporan SKM 3 bulan sekali		Valid Berita Acara Forum OPD Belum dicet Minta ke Pak A (TU)	Valid diverifikasi pada studi dokumen tahap 2. ✓ Valid diverifikasi pada studi dokumentasi tahap 2

INSTRUMEN FGD

Komponen	Keterangan
Domain	APO12 <i>Managed Risk</i>
Tanggal	Senin, 17 November 2025
Tempat	Ruang Kepala Dinas
Metode	<i>Focus Group Discussion</i> (FGD)
Peneliti	Ketut Ananda Dharmawati-2215091035
Informan	1. Kepala Dinas Komunikasi dan Informatika Kabupaten Klungkung 2. Kepala Bidang Telematika (atau yang mewakili) 3. Kepala Bidang Statistik dan Persandian (atau yang mewakili) 4. Kepala Bidang Komunikasi (atau yang mewakili) 5. JF Perencana Ahli Muda 6. JF Sandiman Ahli Muda

PETUNJUK PENGISIAN INSTRUMEN CETAK FGD

Instrumen ini digunakan oleh peneliti sebagai lembar kerja utama selama proses FGD dengan informan. Pengisian dilakukan secara manual selama FGD berlangsung. Panduan berikut menjelaskan cara penggunaan setiap kolom agar hasil pencatatan konsisten dan dapat dipertanggungjawabkan:

1. Kolom “Detail Pertanyaan”

Berisi daftar pertanyaan turunan dari setiap aktivitas COBIT 2019. Peneliti membacakan satu per satu pertanyaan kepada informan sesuai urutan aktivitas (EDM03.01 s.d. APO12.06). Pertanyaan tidak perlu dibaca secara kaku; peneliti boleh melakukan *probing* (pertanyaan lanjutan) untuk memperjelas jawaban informan.

2. Kolom “Jawaban Informan”

Diisi dengan ringkasan jawaban informan menggunakan kalimat singkat dan faktual, tanpa interpretasi. Bila ada perbedaan pendapat antar informan, tulis semua variasi secara ringkas dengan menyebutkan jabatan informan.

3. Kolom “Bukti Dokumen yang Ditunjukkan”

Diisi dengan nama dokumen yang disebutkan atau ditunjukkan informan (misalnya *Risk Register 2025*, *SOP Keamanan Informasi*, *Renstra Diskominfo*). Bila dokumen belum sempat diverifikasi, beri catatan “belum dicek” di kolom Catatan Peneliti.

4. Kolom “Status (N/P/L/F)”

Setelah FGD selesai, peneliti memberikan penilaian awal terhadap tiap aktivitas menggunakan skala NPLF:

N (Not Achieved): Aktivitas tidak dilakukan / tidak ada bukti. Kurang dari 15%

P (Partially Achieved): Aktivitas sebagian dijalankan, tetapi belum konsisten atau belum ada bukti lengkap. (15–50%)

L (Largely Achieved): Aktivitas sebagian besar sudah berjalan, bukti tersedia, namun ada kekurangan minor. (50–85%)

F (Fully Achieved): Aktivitas sepenuhnya diterapkan, bukti lengkap dan konsisten dengan deskripsi COBIT 2019. (>85%)

Penilaian akhir dapat dikonfirmasi kembali setelah verifikasi dokumen (studi dokumentasi).

5. Kolom “Catatan Peneliti”

Digunakan untuk mencatat klarifikasi penting, inkonsistensi, atau temuan tambahan selama FGD. Misalnya: “dokumen ada tapi belum ditandatangani pimpinan” atau “praktik informal belum tertulis dalam SOP”.

Tujuan	
<i>Integrate the management of I&T-related enterprise risk with overall enterprise risk management (ERM) and balance the costs and benefits of managing I&T-related enterprise risk.</i>	Mengintegrasikan pengelolaan risiko perusahaan terkait I&T dengan manajemen risiko perusahaan (ERM) secara keseluruhan dan seimbangkan biaya dan manfaat pengelolaan risiko perusahaan terkait I&T.

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
APO12.01 Collect data (Mengumpulkan data).						
1	Membangun dan memelihara metode untuk pengumpulan, klasifikasi, dan analisis data terkait risiko I&T.	1. Apakah organisasi memiliki metode resmi untuk mengumpulkan dan menganalisis data risiko I&T ? <i>Policies:</i> SOP atau pedoman resmi pengumpulan risiko 2. Apakah klasifikasi data risiko sudah ditetapkan (misalnya insiden keamanan, <i>downtime</i>, kesalahan manusia)? <i>Processes:</i> mekanisme klasifikasi risiko 3. Bagaimana prosedur memastikan data yang dikumpulkan valid dan konsisten? <i>Processes:</i> verifikasi data risiko	Tidak Ada Tidak Ada Verifikasi dari BSSN	Risk Register 2025 RTE.pdf Lampiran 1 Form 4.pdf Lampiran 2 Form 5 Laporan TMP1 Feb. Klungkung	L (Largely Achieved) Bukti tidak disebut, ditemukan saat studi dokumen Bukti tidak disebut, ditemukan saat studi dokumen Valid Diverifikasi pada studi tahap 2	Valid Ada Valid Diklasifikasi berdasarkan kategori risiko dan dampak

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
		4. Apakah metode ini didokumentasikan dalam bentuk SOP atau pedoman resmi? <i>Information Items:</i> dokumen SOP, pedoman risiko	Tidak			
2	Mencatat data risiko I&T yang relevan dan signifikan pada lingkungan operasi internal dan eksternal perusahaan..	1. Jenis data risiko I&T apa saja yang biasanya dicatat (internal vs eksternal)? <i>Information Items:</i> risk log, laporan eksternal 2. Apakah ada format baku untuk pencatatan data risiko? <i>Policies:</i> format standar pencatatan risiko 3. Siapa yang biasanya mencatat data risiko I&T? <i>Organizational Structures:</i> staf bidang TI / manajemen risiko 4. Bagaimana data eksternal (misalnya regulasi pemerintah, tren industri) ikut didokumentasikan? <i>Processes:</i> integrasi data eksternal ke pencatatan	Insiden Siber Tidak Staf di masing masing bidang Belum	Laporan Eksternal Data Risiko Risk Register Form 4 dan Form 9 Risk Register Form 9	L (Largely Achieved)	Minta ke Pak KA Telematika Bukti tidak disebut, ditemukan saat studi dokumen Bukti tidak disebut, ditemukan saat studi dokumen
3	Mengadopsi atau menetapkan taksonomi risiko untuk definisi skenario risiko dan	1. Apakah organisasi memiliki taksonomi risiko I&T (misalnya kategori dampak: finansial, reputasi, layanan publik)? <i>Policies:</i> dokumen taksonomi risiko	Tidak	Form 4	L (Largely Achieved)	Bukti tidak disebut, ditemukan saat studi dokumen

Tidak ada cek tabel APO12 file studi dokumen

Ada ✓

Memiliki ✓

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	kategori dampak serta kemungkinan yang konsisten.	2. Apakah kategori risiko dan probabilitasnya konsisten dipakai semua bidang? <i>Processes:</i> penerapan klasifikasi risiko 3. Bagaimana taksonomi risiko ini dikomunikasikan kepada staf yang terlibat? <i>Information Flows:</i> sosialisasi taksonomi risiko 4. Apakah pernah ada revisi/penyesuaian taksonomi risiko? <i>Culture & Behavior:</i> kesadaran untuk memperbarui taksonomi	Tidak Untuk sementara belum Tidak	Risk Register Form 5 dan Form 9		Bukti tidak disebut, ditemukan saat studi dokumen Iya ✓
4	Mencatat data tentang peristiwa risiko yang telah menyebabkan atau mungkin menyebabkan dampak bisnis sesuai kategori dampak yang ditetapkan dalam taksonomi risiko. Menangkap data yang	1. Apakah insiden risiko I&T (<i>downtime</i>, serangan siber) selalu dicatat sesuai kategori dampak? <i>Processes:</i> pencatatan insiden sesuai kategori risiko 2. Apakah ada integrasi data dari laporan insiden, problem, atau investigasi? <i>Information Items:</i> laporan insiden, investigasi 3. Siapa yang bertanggung jawab memastikan pencatatan insiden sesuai kategori risiko? <i>Organizational Structures:</i> tim TI / manajemen risiko	Dicatat tapi tidak diklasifikasikan Investigasi tidak ada insiden ada Staf bidang persandian	Laporan Monitoring Web Terdamak Serangan Siber Mei 2015 Laporan Insiden Risk Register Form 9	L (Largely Achieved)	Bukti tidak disebut, ditemukan saat studi dokumen Minta ke Pak KA Telematika Bukti tidak disebut, ditemukan saat studi dokumen Tidak ada JF Perencana ✓

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	relevan dari isu, insiden, masalah, dan investigasi terkait.	4. Apakah catatan insiden digunakan untuk perbaikan layanan? <i>Processes: feedback loop ke perbaikan layanan</i>	Iya	Laporan Telematika		Minta ke Pak KA Telematika EDM03. Akt10 pertanyaan 8 Valid Diverifikasi pada studi tahap 2 Iya ✓
5	Melakukan survei dan analisis data risiko I&T historis dan pengalaman kerugian dari data dan tren yang tersedia secara eksternal, rekan industri melalui log peristiwa berbasis industri, basis data, dan perjanjian industri untuk pengungkapan peristiwa umum.	1. Apakah organisasi menganalisis data risiko historis internal? <i>Processes: analisis data historis</i> 2. Apakah data eksternal (tren industri, data asosiasi pemerintah/kominfo) juga digunakan? <i>Information Items: laporan tren eksternal</i> 3. Bagaimana data eksternal dibandingkan dengan kondisi internal organisasi? <i>Processes: benchmarking internal-eksternal</i> 4. Apakah ada contoh perbaikan kebijakan/teknis yang diambil dari analisis tren eksternal? <i>Culture & Behavior: keterbukaan untuk belajar dari eksternal</i>	Internal tidak Iya dari BSSN Dibandingkan Ada	Laporan Evaluasi Risiko SMT 1 2025 - PdP Laporan BSSN Tidak ada bukti Laporan Perbaikan	L (Largely Achieved)	Bukti tidak disertakan, ditanyakan saat studi dokumen Minta ke Pak MS Persandian Minta ke Pak KA Telematika Valid Diverifikasi pada studi tahap 2 Tidak ada
6	Untuk kelas kejadian yang serupa, menyusun data yang terkumpul dan	1. Apakah organisasi mengelompokkan insiden serupa (misalnya serangan <i>malware</i> berulang)? <i>Processes: klasifikasi insiden serupa</i>	Tidak ada klasifikasi		P (Partially Achieved)	

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	soroti faktor-faktor yang berkontribusi. Tentukan faktor-faktor yang berkontribusi secara umum pada beberapa kejadian.	2. Faktor penyebab umum apa saja yang biasanya diidentifikasi? <i>Information Items:</i> catatan faktor penyebab 3. Apakah hasil analisis faktor penyebab digunakan untuk mencegah kejadian serupa? <i>Culture & Behavior:</i> kesadaran mencegah insiden berulang	Malware Iya	Laporan Evaluasi Risiko SMT 1 2015 Laporan Form 3		Tidak disebut tapi terbukti dalam laporan Minta ke Pak KA Telematika Tidak disebut Keterbatasan SDM, Konfigurasi Keamanan bkn optimal ✓ Tidak ada Valid ✓
7	Menentukan kondisi spesifik yang ada atau tidak ada saat peristiwa risiko terjadi dan cara kondisi tersebut memengaruhi frekuensi peristiwa dan besarnya kerugian.	1. Apakah kondisi tertentu (misalnya kurang staf, beban server tinggi) selalu dicatat saat insiden terjadi? <i>Processes:</i> pencatatan kondisi insiden 2. Bagaimana kondisi tersebut memengaruhi frekuensi kejadian/tingkat kerugian? <i>Information Items:</i> laporan analisis insiden 3. Apakah organisasi melakukan analisis <i>root cause</i> berbasis kondisi lingkungan/operasional? <i>Processes:</i> <i>root cause analysis</i> <i>Root cause</i> = penyebab paling mendasar suatu masalah/insiden, bukan sekadar gejala permukaan.	Dicatat tidak selalu Mempengaruhi Analisisnya tidak pernah	Laporan Monitoring Web Mei 2015 Laporan	P (Partially Achieved)	Tidak disebut ditemukan saat studi dokumen Minta ke Pak KA Telematika ✓ Tidak ada

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
8	Melakukan analisis kejadian dan faktor risiko secara berkala untuk mengidentifikasi masalah risiko baru atau yang muncul dan untuk memperoleh pemahaman tentang faktor risiko internal dan eksternal terkait.	1. Seberapa sering dilakukan analisis risiko I&T berkala? <i>Policies:</i> kebijakan <i>review</i> berkala 2. Siapa yang terlibat dalam analisis berkala ini? <i>Organizational Structures:</i> tim Manajemen Risiko, bidang TI 3. Apakah hasil analisis digunakan untuk memperbarui daftar risiko organisasi? <i>Processes:</i> pembaruan daftar risiko 4. Apakah ada contoh risiko baru yang teridentifikasi dari analisis periodik (misalnya tren <i>ransomware</i>)? <i>Information Items:</i> laporan analisis risiko	Tidak Pernah "	Laporan Evaluasi Risiko SMT 1 2023 Risk Register Form 9 Form 7-9	L (Largely Achieved)	Tidak disebut tetapi terbukti dalam dokumen ✓ Tidak disebut ✓ 3F Perencana Tim Bidang TI ✓ iya X
APO12.02 Analyze risk (Menganalisis risiko).						
9	Menentukan cakupan upaya analisis risiko yang tepat, dengan mempertimbangkan semua faktor risiko dan/atau kekritisitas aset	1. Bagaimana organisasi menentukan lingkup analisis risiko I&T (misalnya hanya pada aplikasi tertentu atau seluruh layanan publik)? <i>Processes:</i> prosedur penetapan lingkup analisis. 2. Siapa yang memutuskan ruang lingkup analisis risiko?	Tidak Pernah	Risk Register 2025 TTE.ppt Form 9	P (Partially Achieved)	Tidak disebut tetapi terbukti ✓ pelayanan Tidak disebut ditemukan saat studi dok ✓ 3F Perencana Kepala Bidang

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	dalam bisnis.	<i>Organizational Structures (RACI)</i>: Kepala Dinas, Bidang TI, Tim Manajemen Risiko. 3. Apakah ada kriteria formal untuk memilih aset mana yang dianggap kritis dalam analisis risiko? <i>Policies</i>: pedoman kritikalitas aset. 4. Bagaimana hasil penentuan lingkup analisis risiko didokumentasikan? <i>Information Items</i>: risk analysis scope document.	11			× ×
10	Menyusun dan memperbarui skenario risiko I&T secara berkala; paparan kerugian terkait I&T; dan skenario terkait risiko reputasi, termasuk skenario gabungan dari jenis dan peristiwa ancaman yang berjenjang dan/atau	1. Apakah organisasi memiliki daftar atau katalog skenario risiko I&T yang terdokumentasi? <i>Policies</i>: dokumen risk scenario register. <i>Risk scenario</i> = gambaran terstruktur tentang kemungkinan kejadian risiko, dampak, dan penyebabnya. 2. Seberapa sering skenario risiko diperbarui (tahunan, per proyek besar, setelah insiden)? <i>Processes</i>: siklus update skenario. 3. Apakah organisasi pernah menyusun skenario gabungan (contoh: serangan siber + kegagalan	Tidak Ada Tidak Pernah Tidak	Risk Register Form 4 Laporan Evaluasi Risiko	P (Partially Achieved)	Dokumen tidak disebut, ditanyakan saat studi dokumen Tidak disebut ditemukan saat studi dok ×

Ada ✓

Tiap Semester ✓

APO12 Managed Risk							
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti	
	bersamaan. Mengembangkan ekspektasi untuk aktivitas dan kemampuan kontrol tertentu untuk mendeteksi.	infrastruktur jaringan terjadi bersamaan)? <i>Processes</i> : penyusunan skenario multi-event. 4. Siapa yang terlibat dalam penyusunan dan pembaruan skenario risiko I&T? <i>Organizational Structures (RACI)</i> : Bidang TI, Kepala Dinas, tim keamanan informasi. 5. Apakah ada metode standar dalam memperkirakan dampak reputasi dari sebuah skenario risiko I&T? <i>Policies</i> : panduan analisis reputasi. 6. Bagaimana pengalaman dari insiden sebelumnya digunakan untuk memperbaiki atau menambah skenario risiko baru? <i>Information Items</i> : catatan insiden, laporan audit. 7. Bagaimana organisasi menentukan kontrol apa saja yang harus tersedia untuk setiap skenario risiko? <i>Processes</i> : <i>mapping</i> skenario ke kontrol. <i>Control</i> = mekanisme/prosedur untuk mengurangi atau mendeteksi risiko. 8. Apakah pimpinan atau <i>stakeholder</i> pernah		Risk Register Form 9 Risk Register Form 9 Laporan Evaluasi		Tidak disebut ditemukan saat studi dokumen X Tidak disebut ditemukan saat studi dokumen Tidak disebut	Valid ✓ Valid ✓ Kolom "Tindakan Pengendalian" Valid ✓

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
		dilibatkan dalam validasi skenario risiko sebelum dipakai dalam analisis formal? <i>Culture & Behavior</i> : keterlibatan pimpinan, tingkat keseriusan validasi.		Risiko SMT 1 2025		ditemukan saat studi dokumen
11	Memperkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario risiko I&T. Mempertimbangkan semua faktor risiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.	1. Bagaimana organisasi memperkirakan seberapa sering risiko I&T bisa terjadi? <i>Processes</i> : metode estimasi frekuensi. 2. Bagaimana memperkirakan besarnya kerugian (atau keuntungan) bila risiko terjadi? <i>Information Items</i> : data historis, perhitungan biaya. 3. Apakah faktor-faktor risiko eksternal (misalnya regulasi, tren siber) ikut dipertimbangkan? <i>Policies</i> : pedoman analisis risiko. 4. Bagaimana pengendalian yang ada dievaluasi saat memperkirakan dampak risiko? <i>Processes</i> : evaluasi kontrol.	Tidak bisa diperkirakan Tidak Ada Iya Tidak Ada	Tidak ada dokumen	N (Not Achieved)	

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
12	Membandingkan risiko saat ini (paparan kerugian terkait I&T) dengan selera risiko dan toleransi risiko yang dapat diterima. Mengidentifikasi risiko yang tidak dapat diterima atau tinggi.	1. Apakah organisasi pernah membandingkan profil risiko saat ini dengan dokumen tingkat risiko yang sudah ditetapkan? <i>Processes: risk profile vs appetite.</i> 2. Siapa yang berwenang menyatakan risiko melebihi batas <i>appetite</i>/tolerance? <i>Organizational Structures (RACI):</i> pimpinan, komite risiko. 3. Apakah ada format laporan resmi untuk menyampaikan risiko yang tidak dapat diterima? <i>Information Items:</i> laporan eksposur risiko. 4. Bagaimana pimpinan menindaklanjuti risiko yang melebihi toleransi? <i>Culture & Behavior:</i> reaksi pimpinan terhadap pelanggaran batas.	Tidak " Tidak "	Laporan Evaluasi	N (Not Achieved)	Tidak disebut ditemukan saat studi dokumen Valid ✓ Kepala Dinas
13	Mengusulkan respons risiko untuk risiko yang melampaui selera risiko	1. Bagaimana organisasi menentukan opsi respons (menghindari, mengurangi, transfer, menerima)? <i>Processes: risk response planning.</i>	Menerima	Form 9	P (Partially)	Tidak disebut ditemukan saat studi dokumen Valid ✓

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	dan tingkat toleransi..	2. Siapa yang berwenang mengusulkan atau memilih opsi respons risiko? <i>Organizational Structures (RACI):</i> pimpinan, tim manajemen risiko. 3. Apakah ada dokumen yang mencatat usulan respons risiko? <i>Information Items: risk response proposal.</i> 4. Bagaimana respons risiko disesuaikan dengan kebijakan organisasi? <i>Policies: pedoman respons risiko.</i>	Tim CSIRT Sementara Belum Tidak	SK TTIS Laporan Evaluasi	Achieved)	Valid Tidak disebut ditemukan saat studi dokumen ✓ dilakukan oleh Kepala Bidang disahkan oleh Kepala Dinas
14	Menetapkan persyaratan tingkat tinggi untuk proyek atau program yang akan menerapkan respons risiko yang dipilih. Identifikasi persyaratan dan harapan untuk kontrol utama yang sesuai untuk	1. Bagaimana organisasi menentukan proyek/program untuk mengurangi risiko I&T? <i>Processes: perencanaan proyek mitigasi.</i> 2. Apakah ada dokumen resmi yang menjelaskan kebutuhan & harapan kontrol utama? <i>Information Items: project charter, TOR, Business Case</i>	Membuat Program Kiwa Tengen Ada	Usulan Pak Kadiis Ringkasan Eksekutif KT Telaah staf Kiwa Tengen	L (Largely Achieved)	Dokumen Belum dicek Minta ke Pak MS Persandian ✓ Valid ✓ Valid

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	respons mitigasi risiko.	<i>Project Charter</i> = dokumen awal proyek yang memuat tujuan, scope, risiko, dan high-level requirement. <i>TOR (Terms of Reference)</i> = dokumen yang menjelaskan detail kebutuhan, ruang lingkup, dan harapan dari suatu program/proyek. Dokumen <i>Business Case</i> = justifikasi proyek, sering kali berisi requirement kontrol risiko. 3. Siapa yang menyetujui requirement mitigasi risiko I&T? <i>Organizational Structures (RACI)</i>: pimpinan proyek, Kepala Dinas. 4. Bagaimana requirement tersebut dikomunikasikan ke tim pelaksana? <i>Information Flows</i>: rapat, dokumen tertulis.	Pimpinan Rapat	Tidak ada Notulen Rapat		
15	Memvalidasi hasil analisis risiko dan analisis dampak bisnis	1. Apakah hasil analisis risiko/BIA pernah diverifikasi ulang sebelum dipakai untuk keputusan? <i>Processes</i>: validasi analisis.	Analisis risiko nya tidak ada		N (Not)	

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	(BIA) sebelum menggunakannya dalam pengambilan keputusan. Pastikan analisis tersebut sesuai dengan persyaratan perusahaan dan verifikasi bahwa estimasi telah dikalibrasi dengan benar dan diteliti untuk mengetahui biasnya.	BIA = analisis dampak bisnis, menilai seberapa parah dampak jika layanan terganggu. 2. Siapa yang melakukan validasi hasil analisis risiko? <i>Organizational Structures (RACI)</i>: tim independen, pimpinan. 3. Bagaimana memastikan hasil analisis bebas bias? <i>Policies</i>: prinsip validasi objektif. 4. Apakah ada bukti dokumentasi validasi (notulen, laporan)? <i>Information Items</i>: dokumen validasi.	Tidak Ada		Achieved	Lampiran studi dokumen fase
16	Menganalisis biaya/manfaat dari opsi respons risiko potensial seperti menghindari, mengurangi/meringankan, mentransfer/membagi, dan menerima serta	1. Apakah organisasi memiliki prosedur formal dalam membandingkan biaya dan manfaat dari berbagai opsi respons risiko? <i>Policies</i>: pedoman analisis <i>cost and benefit</i>. 2. Bagaimana cara organisasi menilai manfaat dari suatu respons risiko (misalnya pengurangan downtime, peningkatan kepercayaan publik)? <i>Processes</i>: metode analisis manfaat.	Tidak		N (Not Achieved)	Tidak ditemukan juga saat studi dokumen X

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	memanfaatkan/merebut. Mengonfirmasikan respons risiko yang optimal.	3. Apakah ada standar atau indikator keuangan yang digunakan dalam menghitung biaya (contoh: ROI, <i>payback period</i>)? <i>Information Items</i>: laporan keuangan, proyeksi biaya. 4. Siapa yang biasanya memutuskan opsi respons risiko yang dipilih (misalnya Kepala Dinas, komite risiko, atau bagian keuangan)? <i>Organizational Structures (RACI)</i>: pengambil keputusan. 5. Bagaimana organisasi memastikan bahwa opsi respons risiko yang dipilih sesuai dengan <i>risk appetite</i> dan <i>tolerance</i> yang berlaku? <i>Processes</i>: <i>alignment</i> dengan <i>risk appetite</i>. 6. Apakah organisasi pernah menggunakan pendekatan transfer risiko (misalnya asuransi, outsourcing) dan bagaimana analisis biayanya dibanding mitigasi internal? <i>Processes</i>: evaluasi opsi transfer.				Tidak ditemukan dokumen dengan perhitungan ROI Kepala Dinas berdasarkan rekomendasi bidang Teknis X X Tidak ditemukan bukti

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
		7. Apakah budaya organisasi cenderung lebih memilih menghindari risiko (<i>risk averse</i>) atau berani mengambil risiko untuk peluang strategis (<i>risk seeking</i>)? <i>Culture & Behavior</i>: sikap organisasi terhadap risiko. 8. Apakah hasil analisis <i>cost/benefit</i> didokumentasikan dan dilaporkan secara formal untuk mendukung keputusan manajemen? <i>Information Flows</i>: laporan analisis risiko ke pimpinan.		Laporan Evaluasi Risiko SMT 1 2025		Tidak disebut ditemukan saat studi dok X
APO12.03 Maintain a risk profile (Memelihara profile risiko).						
17	Menginventarisasi proses bisnis dan dokumentasikan ketergantungannya pada proses manajemen layanan I&T dan sumber daya infrastruktur TI. Mengidentifikasi	1. Apakah organisasi memiliki inventaris proses bisnis yang terdokumentasi? <i>Information Items</i>: dokumen inventaris proses bisnis. 2. Bagaimana ketergantungan proses bisnis pada sistem I&T dicatat? <i>Processes</i>: pemetaan <i>dependency</i>. 3. Apakah personel pendukung, aplikasi, infrastruktur, vendor juga dicatat dalam inventaris	Sementara belum Infrastruktur-nya ada dikelola aset	Catatan Infrastruktur	P (Partially Achieved)	Minta ke Pak KA

Valid ✓
Cenderung berhati-hati✓
Valid

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	personel pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan pihak yang melakukan alih daya.	ini? <i>Policies</i>: aturan kelengkapan inventaris. 4. Siapa yang bertanggung jawab memelihara inventaris tersebut? <i>Organizational Structures (RACI)</i>: Bidang TI, unit perencanaan.	Masing-masing Bidang			
18	Menentukan dan menyetujui layanan I&T dan sumber daya infrastruktur TI mana yang penting untuk mempertahankan operasi proses bisnis. Menganalisis ketergantungan dan mengidentifikasi titik lemah.	1. Bagaimana organisasi menentukan layanan I&T mana yang sangat kritis untuk layanan publik? <i>Processes</i>: analisis layanan esensial. 2. Apakah ada dokumen resmi yang menyatakan layanan/infrastruktur esensial? <i>Information Items</i>: daftar layanan kritis, BCP. 3. Siapa yang menyetujui daftar layanan/infrastruktur esensial? <i>Organizational Structures (RACI)</i>: pimpinan, manajemen risiko. 4. Bagaimana titik lemah dalam ketergantungan layanan dianalisis?	Tidak Ada Tidak Punya		N (Not Achieved)	

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
		<i>Processes:</i> weak link analysis.				
19	Mengumpulkan skenario risiko saat ini berdasarkan kategori, lini bisnis, dan area fungsional.	1. Apakah skenario risiko I&T pernah dikategorikan (contoh: operasional, keamanan data, layanan publik)? <i>Processes:</i> risk categorization. 2. Bagaimana skenario risiko dikonsolidasikan lintas unit? <i>Information Flows:</i> laporan konsolidasi. 3. Siapa yang menyetujui agregasi risiko lintas fungsi? <i>Organizational Structures (RACI):</i> komite risiko, pimpinan.	Tidak	Risk Register 2025 TTE Risk Register 2025 TTE	L (Largely Achieved)	Tidak disebut ditemukan saat studi dok Tidak disebut ditemukan saat studi dok Pimpinan
20	Secara berkala menangkap semua informasi profil risiko dan menggabungkannya menjadi profil risiko agregat.	1. Bagaimana organisasi menyatukan seluruh informasi risiko ke dalam profil risiko terkini? <i>Processes:</i> konsolidasi profil risiko. 2. Apakah ada sistem/<i>tools</i> yang digunakan untuk mengelola profil risiko? <i>Services & Infrastructure:</i> aplikasi GRC, spreadsheet, dsb.	Kita tidak punya Profil Risiko Tidak Ada		N (Not Achieved)	Valid ✓ operasional Valid ✓

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
		3. Bagaimana hasil konsolidasi dibagikan ke <i>stakeholder</i> ? <i>Information Flows</i> : laporan <i>risk profile</i> .	—			
21	Menangkap informasi tentang status rencana tindakan risiko untuk dimasukkan dalam profil risiko I&T perusahaan.	1. Apakah setiap tindakan mitigasi risiko memiliki <i>action plan</i> resmi? <i>Policies</i> : pedoman penyusunan <i>action plan</i> . 2. Bagaimana status pelaksanaan <i>action plan</i> dipantau? <i>Processes</i> : monitoring rencana aksi. 3. Siapa yang bertanggung jawab melaporkan progres <i>action plan</i> ? <i>Organizational Structures (RACI)</i> : pemilik risiko, pimpinan unit.	Tidak 		N (Not Achieved)	
22	Berdasarkan semua data profil risiko, tentukan serangkaian indikator risiko yang memungkinkan identifikasi dan	1. Apakah organisasi memiliki indikator risiko utama (KRI) untuk memantau tren risiko? <i>Policies</i> : definisi KRI. 2. Bagaimana KRI ditentukan dari data profil risiko? <i>Processes</i> : metode penetapan indikator.	Tidak 		N (Not Achieved)	

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	pemantauan cepat risiko terkini dan tren risiko.	3. Apakah indikator risiko digunakan secara rutin dalam rapat pimpinan? <i>Information Items:</i> laporan KRI. 4. Siapa yang menyetujui indikator risiko sebelum digunakan? <i>Organizational Structures (RACI):</i> pimpinan, komite risiko. KRI (<i>Key Risk Indicator</i>) = indikator pengukuran kuantitatif atau kualitatif yang digunakan organisasi	II			
23	Menangkap informasi tentang peristiwa risiko I&T yang telah terwujud untuk dimasukkan dalam profil risiko TI perusahaan	1. Apakah organisasi memiliki catatan formal untuk insiden atau peristiwa risiko I&T? <i>Information Items:</i> log insiden, laporan keamanan. 2. Bagaimana data insiden dikumpulkan (manual, sistem otomatis)? <i>Processes:</i> mekanisme pencatatan insiden. 3. Siapa yang bertanggung jawab melaporkan insiden risiko I&T? <i>Organizational Structures (RACI):</i> unit operasional, helpdesk TI.	Ada Manual Bidang TI	Laporan Log Insiden Laporan Monitoring Web Terdampak Serangan Cyber Mei 2025	F (Fully Achieved)	Minta ke Pak KA Telematika Lampiran Studi Dokumentasi

Tidak ada

Pertanyaan
1-3 Valid
✓

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
APO12.04 <i>Articulate risk</i> (Mengartikulasikan Risiko).						
24	Melaporkan hasil analisis risiko kepada semua pemangku kepentingan yang terpengaruh dalam bentuk dan format yang berguna untuk mendukung keputusan perusahaan. Jika memungkinkan, sertakan probabilitas dan rentang kerugian atau keuntungan beserta tingkat keyakinan, untuk memungkinkan manajemen menyeimbangkan risiko-imbal hasil.	1. Bagaimana hasil analisis risiko disampaikan ke <i>stakeholder</i>? <i>Information Flows</i>: laporan, <i>dashboard</i>. 2. Apakah laporan analisis risiko mencantumkan probabilitas dan range kerugian? <i>Information Items</i>: format laporan risiko. 3. Siapa yang meninjau laporan analisis risiko sebelum didistribusikan? <i>Organizational Structures (RACI)</i>: pimpinan, tim analisis.	Laporan Tidak mencantumkan Pimpinan	Laporan Insiden Form 9	F (Fully Achieved)	Minta ke Pak KA Telematika Tidak disebut ditemukan saat studi dok

Tidak ada Valid Lampiran studi dok APO12

Mencantumkan ✓

✓

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
25	Memberikan para pengambil keputusan pemahaman tentang skenario terburuk dan paling mungkin, paparan kerugian terkait I&T, serta reputasi signifikan, pertimbangan hukum dan peraturan, atau kategori dampak lainnya sesuai taksonomi risiko.	1. Bagaimana pengambil keputusan mendapat gambaran skenario terburuk/terbaik dari risiko I&T? <i>Processes: briefing risiko.</i> 2. Apakah aspek reputasi, hukum, dan regulasi juga disampaikan dalam laporan risiko? <i>Policies: pedoman laporan risiko.</i> 3. Bagaimana kejelasan laporan disesuaikan dengan kebutuhan pimpinan? <i>Culture & Behavior: komunikasi yang dipahami non-teknis.</i>	Briefing Risiko Regulasi Ada Kolaborasi antara teknis dan non teknis	Langsung Laporan Risiko Laporan Evaluasi Risiko SMTI	L (largely Achieved)	Minta ke Pak ICA Telematika
26	Melaporkan profil risiko terkini kepada semua pemangku kepentingan. Sertakan informasi tentang efektivitas proses manajemen risiko, efektivitas pengendalian,	1. Apakah organisasi secara rutin melaporkan profil risiko terkini ke <i>stakeholder</i>? <i>Processes: siklus pelaporan risiko.</i> 2. Apa saja informasi yang disertakan (efektivitas kontrol, kesenjangan, status remediasi)? <i>Information Items: laporan profil risiko.</i>	Tidak		N (Not Achieved)	

Tidak ada
Ada Dokumen
Jawaban tetap
TIDAK

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	kesenjangan, inkonsistensi, redundansi, status perbaikan, dan dampaknya terhadap profil risiko.	3. Siapa yang menerima laporan profil risiko? <i>Organizational Structures (RACI):</i> pimpinan, auditor, regulator.				
27	Secara berkala, untuk area dengan risiko relatif dan paritas kapasitas risiko, mengidentifikasi peluang terkait I&T yang akan memungkinkan penerimaan risiko lebih besar dan peningkatan pertumbuhan dan laba.	1. Apakah organisasi pernah mengidentifikasi peluang I&T saat risiko relatif rendah? <i>Processes:</i> analisis peluang risiko. 2. Bagaimana peluang tersebut dievaluasi terhadap kapasitas risiko organisasi? <i>Policies:</i> pedoman evaluasi peluang. 3. Apakah ada contoh peluang I&T yang dimanfaatkan untuk pertumbuhan? <i>Information Items:</i> studi kasus peluang.	Tidak " 	Laporan Evaluasi Risiko TW 11 2025 — " — Laporan SKM SISUKMA TW 11 2025	P (Partially Achieved)	Tidak disebut ditemukan saat studi dokumentasi Valid semua tertera di Lampiran Studi Dokumentasi tabel APO 12
28	Meninjau hasil penilaian pihak ketiga yang objektif dan tinjauan	1. Apakah hasil audit eksternal/asesmen pihak ketiga dimasukkan ke dalam profil risiko? <i>Processes:</i> integrasi hasil audit.	Tidak		N C Not	

✓

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	audit internal serta jaminan kualitas. Sertakan hasil tersebut dalam profil risiko. Tinjau kesenjangan yang teridentifikasi dan paparan kerugian terkait I&T untuk menentukan perlunya analisis risiko tambahan.	2. Bagaimana kesenjangan yang ditemukan ditindaklanjuti? <i>Processes: corrective action.</i> 3. Siapa yang meninjau hasil asesmen tersebut? <i>Organizational Structures (RACI): pimpinan, auditor internal.</i>	1 11 1		Achieved)	
APO12.05 Define a risk management action portfolio (Menentukan portofolio tindakan manajemen risiko).						
29	Memelihara inventaris aktivitas pengendalian yang ada untuk mengurangi risiko dan yang memungkinkan risiko ditangani sesuai dengan selera dan	1. Apakah organisasi memiliki daftar resmi kontrol mitigasi risiko? <i>Information Items: control inventory.</i> 2. Bagaimana kontrol diklasifikasikan dan dipetakan ke skenario risiko? <i>Processes: kontrol mapping.</i> 3. Siapa yang bertanggung jawab memperbarui	Tidak 1		N (Not Achieved)	

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	toleransi risiko. Mengklasifikasikan aktivitas pengendalian dan memetakannya ke skenario risiko I&T tertentu dan agregasi skenario risiko I&T.	inventaris kontrol? <i>Organizational Structures (RACI)</i> : tim pengendalian internal, Bidang TI.	11 			
30	Menentukan apakah setiap entitas organisasi memantau risiko dan menerima akuntabilitas untuk beroperasi dalam tingkat toleransi individu dan portofolionya.	1. Apakah tiap unit organisasi diminta memantau risiko sendiri? <i>Policies</i> : aturan akuntabilitas risiko. 2. Bagaimana akuntabilitas risiko dibuktikan? <i>Information Items</i> : laporan risiko unit. 3. Siapa yang menilai apakah unit sudah sesuai toleransi? <i>Organizational Structures (RACI)</i> : manajemen risiko, pimpinan.	Diminta memantau sendiri Laporan Insiden Pimpinan	tapi aturannya tidak ada Laporan Insiden	N (Not Achieved)	Minta ke Pak KA Telematika

Tidak ada

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
31	Menentukan serangkaian proposal proyek yang seimbang yang dirancang untuk mengurangi risiko dan/atau proyek yang memungkinkan peluang perusahaan strategis, dengan mempertimbangkan biaya, manfaat, dampak pada profil risiko dan peraturan saat ini.	4. Bagaimana organisasi menilai proyek mitigasi risiko vs proyek peluang? <i>Processes:</i> penilaian biaya-manfaat proyek. 5. Apakah biaya, manfaat, dan regulasi dijadikan pertimbangan formal? <i>Policies:</i> pedoman seleksi proyek. 6. Siapa yang memutuskan proposal proyek mana yang dijalankan? <i>Organizational Structures (RACI):</i> pimpinan, tim perencanaan.	Tidak //		N (Not Achieved)	
APO12.06 Respond to risk (Menanggapi risiko).						
32	Menyiapkan, memelihara, dan menguji rencana yang mendokumentasikan langkah-langkah	1. Apakah organisasi memiliki dokumen rencana penanganan insiden risiko I&T yang formal? <i>Policies:</i> disaster recovery plan (DRP), business continuity plan (BCP).	Tidak		P (Partially Achieved)	

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	spesifik yang harus diambil ketika suatu peristiwa risiko dapat menyebabkan insiden operasional atau pengembangan yang signifikan dengan dampak bisnis yang serius. Pastikan bahwa rencana tersebut mencakup jalur eskalasi di seluruh perusahaan.	2. Bagaimana rencana penanganan insiden tersebut disusun? Apakah ada prosedur baku? <i>Processes:</i> mekanisme penyusunan rencana. 3. Siapa yang terlibat dalam penyusunan dan pemeliharaan rencana ini? <i>Organizational Structures (RACI):</i> tim TI, pimpinan, manajemen risiko, pihak eksternal. 4. Apakah rencana ini secara berkala diuji melalui simulasi/drill? Jika ya, seberapa sering? <i>Processes:</i> uji coba dan review periodik. 5. Apakah tersedia jalur eskalasi resmi bila insiden signifikan terjadi (contoh: siapa yang dihubungi pertama, siapa yang memberi keputusan)? <i>Information Flows:</i> diagram eskalasi, SOP eskalasi. 6. Apakah ada sarana/infrastruktur khusus untuk mendukung eksekusi rencana (misalnya backup site, hotline darurat)? <i>Services & Infrastructure:</i> fasilitas pendukung.	Tidak Ada	Risk Register Form 9 Risk Register Form 9 Laporan Monitoring Web Mei 2025		Tidak disebut ditemukan saat studi dokumen Kolom Penanggung Jawab × × ✓ Ada

Jawaban
Tetap Belum
Ada Prosedur
Baku (SOP)

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
		3. Bagaimana proses koordinasi antar-unit dilakukan saat rencana respons dijalankan? <i>Processes:</i> mekanisme koordinasi lintas unit. 4. Apakah tersedia sarana pendukung untuk memfasilitasi eksekusi respons (contoh: sistem monitoring <i>real-time</i>, ruang kendali)? <i>Services & Infrastructure:</i> tools dan fasilitas darurat. 5. Bagaimana budaya staf saat menghadapi insiden – apakah tenang dan mengikuti prosedur, atau panik dan improvisasi? <i>Culture & Behavior:</i> reaksi nyata staf/pimpinan. 6. Apakah hasil penerapan rencana respons dievaluasi untuk memperbaiki SOP atau prosedur yang ada? <i>Processes:</i> siklus pembelajaran pasca-insiden.	Dikoordinasikan Tidak Ada Tenang Tidak ada evaluasi	Laporan Monitoring		Ada ditemukan saat studi dok
34	Mengategorikan insiden dan bandingkan paparan kerugian terkait I&T terhadap ambang batas	1. Apakah insiden I&T (misalnya <i>downtime</i> aplikasi, serangan siber, kebocoran data) dikategorikan secara resmi menurut tingkat keparahan? <i>Policies:</i> SOP kategorisasi insiden.	Tidak Ada		L (Largely Achieved)	

APO12 Managed Risk							
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti	
	toleransi risiko. Komunikasikan dampak bisnis kepada para pengambil keputusan sebagai bagian dari pelaporan dan perbarui profil risiko.	2. Bagaimana organisasi menentukan apakah suatu insiden sudah melewati ambang batas toleransi risiko? <i>Processes</i> : mekanisme penilaian toleransi. 3. Siapa yang berwenang melakukan validasi kategori insiden dan memutuskan langkah eskalasi? <i>Organizational Structures (RACI)</i> : pejabat risk owner, Kepala Dinas, tim TI. 4. Apakah hasil perbandingan insiden dengan toleransi risiko terdokumentasi dan masuk ke profil risiko organisasi? <i>Information Items</i> : risk register, laporan insiden. 5. Bagaimana dampak bisnis dari insiden I&T dikomunikasikan kepada pengambil keputusan? <i>Information Flows</i> : laporan resmi, rapat pimpinan, dashboard. 6. Bagaimana budaya organisasi dalam menyikapi insiden yang melewati toleransi risiko, apakah terbuka membahasnya atau cenderung menutupinya?		Laporan Evaluasi Risiko Kepala Dinas Risk Register Melalui Rapat laporan Resmi Semesteran		Tidak disebut ditemukan saat studi dok Tidak disebut ditemukan saat studi dok Ditemukan saat studi dokumentasi Lampiran studi dokumen aneksi Tabel APO 12	✓ Valid ✓ Iya Valid ✓ Valid

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
		<i>Culture & Behavior</i> : keterbukaan pimpinan/staf.				
35	Memeriksa kejadian/kerugian buruk di masa lalu dan kesempatan yang hilang, serta menentukan akar penyebabnya.	1. Apakah organisasi memiliki catatan resmi terkait insiden atau kerugian I&T di masa lalu (misalnya <i>downtime</i> panjang, kebocoran data, proyek I&T gagal)? <i>Information Items</i>: laporan insiden, audit, <i>lessons learned</i>. 2. Bagaimana organisasi menganalisis akar penyebab (<i>root cause</i>) dari insiden atau kerugian tersebut? <i>Processes</i>: metode <i>root cause analysis</i> (misalnya <i>fishbone</i>, 5-why). 3. Siapa saja yang biasanya dilibatkan dalam proses investigasi akar penyebab insiden I&T? <i>Organizational Structures (RACI)</i>: tim TI, manajemen risiko, pimpinan. 4. Apakah ada prosedur formal untuk melakukan evaluasi pasca-insiden (<i>post-mortem review</i>)? <i>Policies</i>: SOP evaluasi insiden.	Ada Untuk sementara tidak Bidang Persandian Tidak	Laporan Insiden Laporan Evaluasi Risiko Laporan Evaluasi Risiko	L (Largely Achieved)	Minta ke Pak KA Telematika Lampiran Tidak disebut ditemukan saat studi dokumentasi

APO12 Managed Risk							
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti	
		5. Apakah faktor eksternal (regulasi, vendor, cuaca, tren industri) juga dipertimbangkan dalam analisis kerugian masa lalu? <i>Processes:</i> analisis faktor eksternal. 6. Bagaimana budaya organisasi dalam menyikapi insiden masa lalu, apakah terbuka mencari solusi atau cenderung menyalahkan pihak tertentu? <i>Culture & Behavior:</i> sikap staf/pimpinan. 7. Apakah hasil analisis insiden masa lalu digunakan sebagai bahan pembelajaran untuk memperbaiki kebijakan atau SOP? <i>Processes:</i> siklus perbaikan berkelanjutan.	Iya dipertimbangkan Terbuka mencari solusi Iya	Laporan BSSN Laporan Evaluasi Risiko		Minta ke Pak MS Persandian Valid Valid	Valid ③ studi dokumen
36	Mengomunikasikan akar permasalahan, persyaratan respons risiko tambahan, dan perbaikan proses kepada para pengambil keputusan yang tepat.	1. Apakah hasil analisis akar penyebab (<i>root cause</i>) insiden I&T secara rutin disampaikan ke pimpinan atau pengambil keputusan? <i>Information Flows:</i> laporan resmi, rapat evaluasi. 2. Bagaimana organisasi memastikan bahwa kebutuhan respons tambahan (misalnya kontrol baru, peningkatan keamanan) disampaikan dengan jelas	Tidak secara rutin Sesuai mekanisme kebutuhan	Telaah Staf	P (Partially Achieved)	Minta ke Pak G. H Telematika	

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
	Pastikan bahwa penyebab, persyaratan respons, dan perbaikan proses disertakan dalam proses tata kelola risiko.	kepada pengambil keputusan? <i>Processes</i>: mekanisme eskalasi kebutuhan respons. 3. Siapa yang bertanggung jawab mengomunikasikan hasil analisis akar penyebab dan rekomendasi perbaikan? <i>Organizational Structures (RACI)</i>: manajemen risiko, Kepala Bidang TI, tim investigasi. 4. Apakah ada kebijakan formal yang mewajibkan penyampaian hasil analisis akar penyebab kepada level manajemen tertentu? <i>Policies</i>: aturan eskalasi hasil investigasi. 5. Bagaimana budaya organisasi dalam menerima rekomendasi perbaikan, apakah proaktif untuk memperbaiki atau cenderung menunda? <i>Culture & Behavior</i>: sikap pimpinan dan staf. 6. Apakah hasil rekomendasi perbaikan biasanya diintegrasikan ke dalam kebijakan atau prosedur manajemen risiko? <i>Processes</i>: pembaruan SOP, kebijakan risiko.	Tidak Ada Tidak Ada Proaktif untuk memperbaiki Iya	Laporan Evaluasi Risiko SMT 1 2025		Valid

APO12 Managed Risk						
No. Akt	Deskripsi Aktivitas	Detail pertanyaan	Jawaban	Bukti Dokumen yang Ditunjukkan	Status (N/P/L/F)	Catatan Peneliti
		7. Apakah organisasi pernah mengevaluasi efektivitas perbaikan proses setelah implementasi rekomendasi? <i>Information Items:</i> laporan evaluasi, hasil audit tindak lanjut.	Iya pernah	Laporan Evaluasi Risiko SMT 1 2025		Valid Ada tindak lanjut penilaian efektivitas mitigasi

1. Apakah telah dilakukan audit?

2. Apakah telah dilakukan audit?

3. Apakah telah dilakukan audit?

4. Apakah telah dilakukan audit?

5. Apakah telah dilakukan audit?

6. Apakah telah dilakukan audit?

7. Apakah telah dilakukan audit?

8. Apakah telah dilakukan audit?

9. Apakah telah dilakukan audit?

10. Apakah telah dilakukan audit?

11. Apakah telah dilakukan audit?

12. Apakah telah dilakukan audit?

13. Apakah telah dilakukan audit?

14. Apakah telah dilakukan audit?

Lampiran 7. Hasil Studi Dokumen

7.1 Tabel Hasil Studi Dokumen

No	Nama Dokumen	Bukti Kegiatan / Isi Utama	Domain COBIT 2019	Validitas
1	<i>Risk Register</i> 2025 TTE.pdf	Dokumen ini memuat daftar lengkap risiko strategis dan operasional I&T, termasuk nilai kemungkinan, dampak, dan mitigasi yang direncanakan. Risiko seperti kehilangan data, gangguan jaringan, dan keamanan informasi dibahas dengan penanggung jawab serta jadwal pengendalian. Dokumen memuat daftar risiko, penyebab, dampak, mitigasi, dan penanggung jawab risiko yang digunakan oleh Diskominfo Klungkung dalam pengelolaan risiko I&T.	EDM03, APO12	Valid
2	Lampiran 1 <i>Risk Register</i> Form 4 (Risiko Prioritas)	Berisi klasifikasi risiko prioritas per bidang layanan publik, lengkap dengan skor risiko dan tanggung jawab mitigasi. Format penilaian menunjukkan penerapan proses pengumpulan dan pemetaan risiko yang konsisten dengan COBIT 2019.	APO12, EDM03	Valid
3	Lampiran 2 <i>Risk Register</i> Form 5	Menampilkan daftar risiko utama dengan nilai dampak dan kemungkinan. Mencerminkan pelaksanaan <i>risk profiling</i> dan pengarahannya oleh pimpinan Diskominfo.	EDM03, APO12	Valid

No	Nama Dokumen	Bukti Kegiatan / Isi Utama	Domain COBIT 2019	Validitas
4	Lampiran 3 <i>Risk Register</i> Form 9 (Risiko Perencana)	Menunjukkan kegiatan pengendalian dan pemantauan risiko, termasuk backup data, pembaruan sistem, serta evaluasi pelaksanaan mitigasi. Formatnya menggambarkan tahapan <i>respond</i> dan <i>monitor</i> dalam siklus manajemen risiko.	EDM03, APO12	Valid
5	Renstra 2024–2026.pdf	Dokumen strategis yang menetapkan arah kebijakan I&T, keamanan informasi, dan tata kelola digital. Risiko I&T diintegrasikan dalam sasaran strategis dan indikator kinerja.	EDM03, APO12	Valid
6	Laporan Evaluasi Risiko Semester I 2025.pdf	Menyajikan hasil pemantauan dan tindak lanjut mitigasi risiko I&T bidang. Data kuantitatif dan narasi evaluasi membuktikan pelaksanaan pemantauan risiko berkala.	EDM03, APO12	Valid
7	Perbup 21/2023 – Masterplan Smart City 2023-2032	Mengatur arah kebijakan digital daerah dan penguatan keamanan data, menjadi dasar strategi pengendalian risiko I&T daerah.	EDM03	Valid
8	Perbup 87/2019 – Penerapan Smart City	Dokumen regulasi penerapan Smart City yang mencakup kebijakan pengelolaan risiko dan keamanan informasi.	EDM03, APO12	Valid
9	SK Nomor 23 Tahun 2025	Menetapkan pejabat dan tim pelaksana risiko I&T. Menunjukkan struktur tanggung jawab dan mekanisme kontrol risiko berbasis	EDM03, APO12	Valid

No	Nama Dokumen	Bukti Kegiatan / Isi Utama	Domain COBIT 2019	Validitas
		organisasi.		
10	Laporan Aset TI (LAP_IIO102-2025-032-20250702-1427_ASET.xlsx)	Berisi inventarisasi aset I&T dan status penggunaannya. Dokumen ini mendukung kegiatan identifikasi aset kritis dan risiko terkait infrastruktur digital.	APO12	Valid
11	Daftar SOP Lengkap Diskominfo	Menunjukkan prosedur teknis pengendalian risiko I&T, keamanan data, serta layanan publik. Mendukung bukti penerapan proses formal risiko I&T.	APO12, EDM03	Valid
12	Laporan Evaluasi Renja TW II 2025.pdf	Memuat capaian dan kendala kegiatan yang berkaitan dengan manajemen risiko I&T dan efektivitas kegiatan SPBE.	EDM03	Cukup Valid
13	Laporan SKM SISUKMA OPD TW II 2025.pdf	Menilai kepuasan masyarakat terhadap layanan I&T pemerintah. Berfungsi sebagai media evaluasi dan komunikasi risiko reputasi.	EDM03	Cukup Valid
14	SK Tim Tanggap Insiden Siber 2025.pdf	Membentuk TTIS sebagai unit tanggap insiden resmi. Struktur dan tugasnya sesuai praktik pengendalian risiko siber COBIT 2019.	APO12, EDM03	Valid
15	Surat Forum OPD (4 Maret 2025)	Bukti koordinasi lintas OPD dalam evaluasi rencana kerja dan risiko. Tanda tangan digital menunjukkan integritas dan keamanan informasi.	EDM03	Valid
16	Notulen Rapat Staf Diskominfo (9	Mencatat pembahasan pembentukan TTIS dan inovasi <i>Kiwa Tengen</i> .	EDM03	Valid

No	Nama Dokumen	Bukti Kegiatan / Isi Utama	Domain COBIT 2019	Validitas
	Oktober 2025)	Menunjukkan kesadaran pimpinan terhadap risiko eksternal.		
17	Laporan BerAKHLAK 2025.pdf	Menggambarkan nilai budaya kerja dan etika ASN yang mendukung kesadaran dan mitigasi risiko.	EDM03	Cukup Valid
18	Renja Rancangan Final 2026.pdf	Menunjukkan integrasi hasil evaluasi risiko tahun sebelumnya ke dalam rencana kerja baru.	EDM03, APO12	Valid
19	Berita Acara Forum OPD 2025.pdf	Bukti kesepakatan formal atas arah kebijakan dan kegiatan penguatan tata kelola I&T.	EDM03	Valid
20	Laporan Monitoring Web Terdampak Serangan Siber Mei 2025.pdf	Laporan resmi insiden siber yang mencatat serangan, pemulihan, dan hasil mitigasi. Bukti langsung pelaksanaan kontrol keamanan I&T.	APO12, EDM03	Valid
21	Laporan Workshop Penguatan TTIS (5–7 Nov 2025)	Bukti kegiatan pelatihan dan peningkatan kapasitas SDM dalam tanggap insiden dan mitigasi risiko siber.	APO12, EDM03	Valid
22	Kajian Arsitektur SPBE – Laporan Akhir Review.pdf	Hasil evaluasi arsitektur SPBE yang mengidentifikasi risiko dan rekomendasi mitigasi keamanan informasi.	EDM03, APO12	Cukup Valid
23	Laporan TMPI Kabupaten Klungkung.pdf	Laporan evaluasi eksternal dari BSSN mengenai tingkat kesiapan penanganan insiden siber di Diskominfo.	APO12	Valid
24	Laporan Monitoring Anomali Trafik (Jan–	Hasil analisis aktivitas anomali jaringan yang mendeteksi potensi	APO12	Valid

No	Nama Dokumen	Bukti Kegiatan / Isi Utama	Domain COBIT 2019	Validitas
	Mei 2025)	serangan dan rekomendasi mitigasi teknis.		
25	SK TTIS 2025 (Duplikat)	Dokumen legal tambahan untuk verifikasi pembentukan Tim Tanggap Insiden Siber.	APO12	Valid
26	Ringkasan Eksekutif Kiwa Tengen.pdf	Rencana proyek penguatan mitigasi risiko siber daerah dengan enam pilar strategi (edukasi, kebijakan, dan kontrol I&T).	APO12, EDM03	Valid
27	Telaahan Staf Kiwa Tengen.pdf	Nota dinas analisis risiko dan pembentukan inovasi keamanan daerah. Menunjukkan penetapan kebutuhan kontrol utama risiko I&T.	APO12	Valid
28	Laporan Monitoring Server November 2025.pdf	Hasil pemantauan kondisi server dan tindakan korektif, menunjukkan aktivitas kontrol dan pemeliharaan infrastruktur risiko I&T.	APO12	Valid

TABEL SOP LENGKAP

No	Nama SOP	Analisis Relevansi	Domain COBIT 2019	Komponen Tata Kelola	Validitas
7–8	Surat Masuk/Surat Keluar E-Surat	Mengatur pengelolaan dokumen digital dan tanda tangan elektronik → bukti sistem SPBE berjalan.	APO12.01, APO12.03	<i>Processes, Information Items</i>	Valid (SOP TI)

No	Nama SOP	Analisis Relevansi	Domain COBIT 2019	Komponen Tata Kelola	Validitas
27	Pelayanan Pembuatan Hosting Web	Proses penyediaan server & hosting → pengelolaan infrastruktur I&T.	APO12.05, APO12.06	<i>Processes, Infrastructure</i>	Valid (SOP I&T)
29	Fasilitasi Laporan Gangguan Internet/Wi-Fi	Menunjukkan kegiatan pemantauan risiko konektivitas I&T.	EDM03.03, APO12.05	<i>Processes, Information Items</i>	Valid (SOP Risiko I&T)
31	Pelayanan Video Conference (Rapat Virtual)	Mengatur keamanan & ketersediaan layanan komunikasi digital pemerintah.	APO12.06, EDM03.02	<i>Processes, Organizational Structures</i>	Valid (SOP I&T)
32	Review Rekaman CCTV	Pengendalian keamanan fisik & bukti audit I&T.	APO12.01, EDM03.03	<i>Processes, Information Items</i>	Valid (SOP Risiko I&T)
33	Pelayanan Fasilitasi Aplikasi untuk OPD	Pengembangan & pengelolaan aplikasi → bukti proses manajemen aplikasi I&T.	APO12.05, APO12.06	<i>Processes</i>	Valid (SOP I&T)
34	Pengelolaan Web OPD	Menunjukkan kebijakan kontrol akses dan keamanan konten web.	EDM03.02, APO12.05	<i>Processes, Organizational Structures</i>	Valid (SOP Risiko I&T)

No	Nama SOP	Analisis Relevansi	Domain COBIT 2019	Komponen Tata Kelola	Validitas
35	Fasilitasi Penyediaan Server (VPS)	Bukti pengendalian infrastruktur dan backup data.	APO12.06, EDM03.03	<i>Processes, Infrastructure</i>	Valid (SOP Risiko I&T)
43–47	SOP Sertifikat Elektronik (OSD LU, AMS), Reset Password, Kehilangan Sertifikat	Pengendalian keamanan identitas digital dan mitigasi insiden → bukti risk control formal.	EDM03.02, APO12.05–12.06	<i>Processes, Information Items, Culture & Behavior</i>	Valid kuat (SOP Risiko I&T)
50	Koordinasi dan Sinkronisasi Pengumpulan Data Statistik Sektoral	Mengandung aspek keamanan dan integritas data sektoral.	APO12.01, APO12.03	<i>Information Items</i>	Valid terbatas (parsial I&T)

Rentang No	Jenis SOP	Alasan Tidak Valid
1–6	Kepegawaian dan surat menyurat manual	Tidak memuat aspek I&T atau risiko sistem.
9–26	Keuangan, pajak, pelaporan anggaran	Administratif, bukan risiko I&T.
28	“Klungkung Mesadu”	Lebih ke inovasi komunikasi publik, tidak memuat mitigasi risiko I&T.
37–41	Informasi publik / PPID	Berkaitan dengan transparansi, bukan keamanan I&T langsung.
48–49	Konten media sosial & statistik sosial	Fokus pada komunikasi publik.

7.2 Bukti Dokumen Pendukung Studi Dokumentasi

Dokumen 1. *Risk Register 2025 TTE.pdf*

IDENTIFIKASI RISIKO STRATEGIK
Unit kerja : Diskominfo Kabupaten Klungkung
Tahun 2025

No	Tujuan Strategik	Risiko				Penyebab		Controlable/Uncontrolable	Kemungkinan Terjadinya Risiko	Dampak			Pilihan Mitigasi (Upaya mengatasi Risiko)	Pengendalian yang sudah ada	Keterangan
		Uraian/Pernyataan Risiko	Pemilik	Jenis	Keterkaitan dengan Tujuan SPIP	Uraian	Sumber			Skor	Uraian	Pihak yang Terkena			
1	2	3	4	5	6	7	8	9	10	11	12	13	14		16
1	Meningkatnya kemudahan memperoleh informasi	Kehilangan seluruh data elektronik pemerintah Kab. Klungkung	Diskominfo	Risiko Lainnya	Tercapainya tujuan organisasi melalui kegiatan yang efektif dan efisien (mengacu pada dokumen visi, misi, renstra, tapkin, dll)	Serangan siber, kerusakan hardware, human error	internal	Uncontrollable	sangat sering	Kurang signifikan	Kurang lancarnya komunikasi	Diskominfo, masyarakat dan wisatawan	Mitigate	Melakukan Backupdata; dan Update system security	
		Aplikasi bisa terkena Hack dan eror pada saat digunakan; dan Terputusnya Jaringan Intra Pemerintah Daerah Kab_Kota				System security kurang bagus dan system belum diupdate; dan Kabel putus								Pemantauan JIP; melakukan monitoring secara berkala dan memberikan pemahaman kepada masyarakat setempat	
		rusaknya sarana prasarana alat komunikasi				Arus listrik yang tidak stabil dan faktor SDM OPD yang kurang paham tentang perangkat jaringan								melakukan monitoring secara berkala dan memberikan pemahaman kepada masyarakat setempat	

Disusun Oleh :
Direvisi Oleh :

Catatan:

Semarapura, 24 Desember 2024



Ditandatangani secara elektronik oleh:
Ptt. Kepala Dinas Komunikasi dan Informatika
I Gusti Ketut Suardika, AP., MSI
Pembina Utama Muda (IV/c)
NIP. : 197405061993111001

Keterangan:

Halaman ini menunjukkan hasil identifikasi risiko I&T yang memuat uraian risiko, penyebab, kemungkinan terjadinya risiko, dampak, mitigasi, dan pengendalian yang telah diterapkan. Dokumen ini digunakan sebagai bukti bahwa aktivitas identifikasi dan pengelolaan risiko telah dilaksanakan di Diskominfo Klungkung.

Dokumen 2. Lampiran 1 *Risk Register* Form 4 (Risiko Prioritas)

Lampiran 1

Form 4
Format Daftar Risiko Prioritas

Nama Pemda : Pemerintah Kabupaten Klungkung, Provinsi Bali Tahun : 2025 Penilaian : Tujuan Strategis : Meningkatnya Kemudahan Memperoleh Informasi Urusan Pemerintahan : Wajib yang tidak berkaitan dengan pelayanan dasar					
No.	"Risiko" yang Teridentifikasi	Kode Risiko	Analisis Risiko		
			Skala Dampak ¹⁾	Skala Kemungkinan ²⁾	Skala Risiko ³⁾
a	b	c	d	e	f=dxe
	I Risiko Strategis				0
	II Risiko Strategis OPD				
1	Kehilangan seluruh data elektronik Pemerintah Kabupaten Klungkung	RSO.24.14.26.23	3	3	9
	Aplikasi bisa terkena hack dan error saat digunakan	RSO.24.14.26.23	3	3	9

Keterangan:

Halaman ini menunjukkan daftar risiko prioritas yang telah diidentifikasi oleh Diskominfo Klungkung beserta kode risiko, nilai dampak, nilai kemungkinan, dan tingkat risiko yang dihasilkan. Dokumen ini digunakan sebagai bukti bahwa proses analisis dan prioritisasi risiko telah dilaksanakan sebagai bagian dari pengelolaan risiko I&T.

Dokumen 3. Lampiran 2 Risk Register Form 5

Lampiran II

Lampiran 3 Form 5/1 - 1
Peraturan Bupati Klungkung Nomor
Tanggal

Form 5
Format Daftar Risiko Prioritas

Nama Pemda : Pemerintah Kabupaten Klungkung, Provinsi Bali
 Tahun Penilaian : 2025
 Tujuan Strategis : Meningkatnya Kemudahan Memperoleh Informasi
 Urusan Pemerintahan : Wajib yang tidak berkaitan dengan pelayanan dasar

No	Risiko Prioritas	Kode Risiko	Skala Risiko	Pemilik Risiko	Penyebab	Dampak
a	b	c	d	e	f	g
I	Risiko Strategis					
II	Risiko Strategis OPD					
	Kehilangan seluruh data elektronik Pemerintah Kabupaten Klungkung	RSO.24.14.26.23	9	Dinas Komunikasi dan Informatika	Gangguan listrik, kerusakan hardware, human error	Perencanaan pembangunan tidak berjalan lancar
	Aplikasi bisa terkena hack dan error saat digunakan	RSO.24.14.26.23	9	Dinas Komunikasi dan Informatika	System security kurang bagus dan system belum diadit	data pada system bisa disalah gunakan
	Rusaknya sarana dan prasarana alat komunikasi	RSO.24.14.26.23	9	Dinas Komunikasi dan Informatika	Arus listrik yang tidak stabil dan faktor SDM yang kurang paham tentang penggunaan alat tersebut	Layanan Internet yang disediakan tidak dapat diakses
III	Risiko Operasional OPD					
1	Penyusunan Dokumen Perencanaan tidak tepat waktu	RSO.24.14.26.23	1	Dinas Komunikasi dan Informatika	Keterlambatan data perencanaan dari Bidang dan penyusunan dokumen perencanaan dibebankan pada pejabat yang menangani perencanaan saja	terlambatnya penyusunan dokumen perencanaan

Keterangan:

Halaman ini menunjukkan daftar risiko prioritas beserta pemilik risiko, penyebab, dampak, dan tingkat risiko yang telah ditetapkan oleh Diskominfo Klungkung. Dokumen ini menjadi bukti bahwa organisasi telah melakukan identifikasi dan analisis risiko secara lebih rinci sebagai dasar pengelolaan risiko I&T.

Dokumen 4. Lampiran 3 *Risk Register* Form 9

Lampiran 3 Form 9/1 - 1
Peraturan Bupati Klungkung Nomor
Tanggal

Lampiran : III

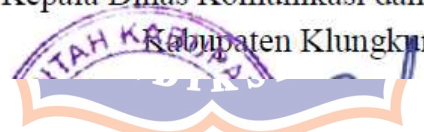
Form 9
FORMAT RENCANA DAN REALISASI PEMANTAUAN ATAS KEGIATAN PENGENDALIAN INTERN YANG DIBUTUHKAN

Nama Pemda		: Pemerintah Kabupaten Klungkung, Provinsi Bali				
Tahun Penilaian		: 2025				
Tujuan Strategis		: Meningkatnya Kemudahan Memperoleh Informasi				
Urusan Pemerintahan		: Wajib yang tidak berkaitan dengan pelayanan dasar				
No	Kegiatan Pengendalian yang Dibutuhkan	Bentuk/Metode Pemantauan yang Diperlukan	Penanggung Jawab Pemantauan	Rencana Waktu Pelaksanaan Pemantauan	Realisasi Waktu Pelaksanaan	Keterangan
a	b	c	d	e	f	g
1	melakukan koordinasi ke bidang-bidang dan meningkatkan pemahaman penyusunan dokumen perencanaan PD	Dokumen Perencanaan	JF Perencana	Januari dan Agustus 2025	Januari dan Agustus 2025	
2	Meningkatkan peran masing-masing bidang dalam pelaksanaan evaluasi PD	dokumen perencanaan	JF Perencana	Januari, April, Juli dan Oktober 2025	Januari, April, Juli dan Oktober 2025	
3	Pegimputan data dukung rencana aksi sudah dilaksanakan sesuai dengan batas waktu yang sudah ditentukan	Laporan Kinerja bulanan, triwulanan dan tahunan	JF Perencana	Januari s/d Desember 2025	Januari s/d Desember 2025	

Keterangan:

Halaman ini menunjukkan rencana dan realisasi pemantauan atas kegiatan pengendalian internal yang telah ditetapkan oleh Diskominfo Klungkung. Dokumen memuat kegiatan pengendalian, metode pemantauan, penanggung jawab, serta jadwal pelaksanaan dan realisasi pemantauan. Dokumen ini menjadi bukti bahwa aktivitas pengendalian dan pemantauan risiko telah dilakukan secara terencana dan terdokumentasi.

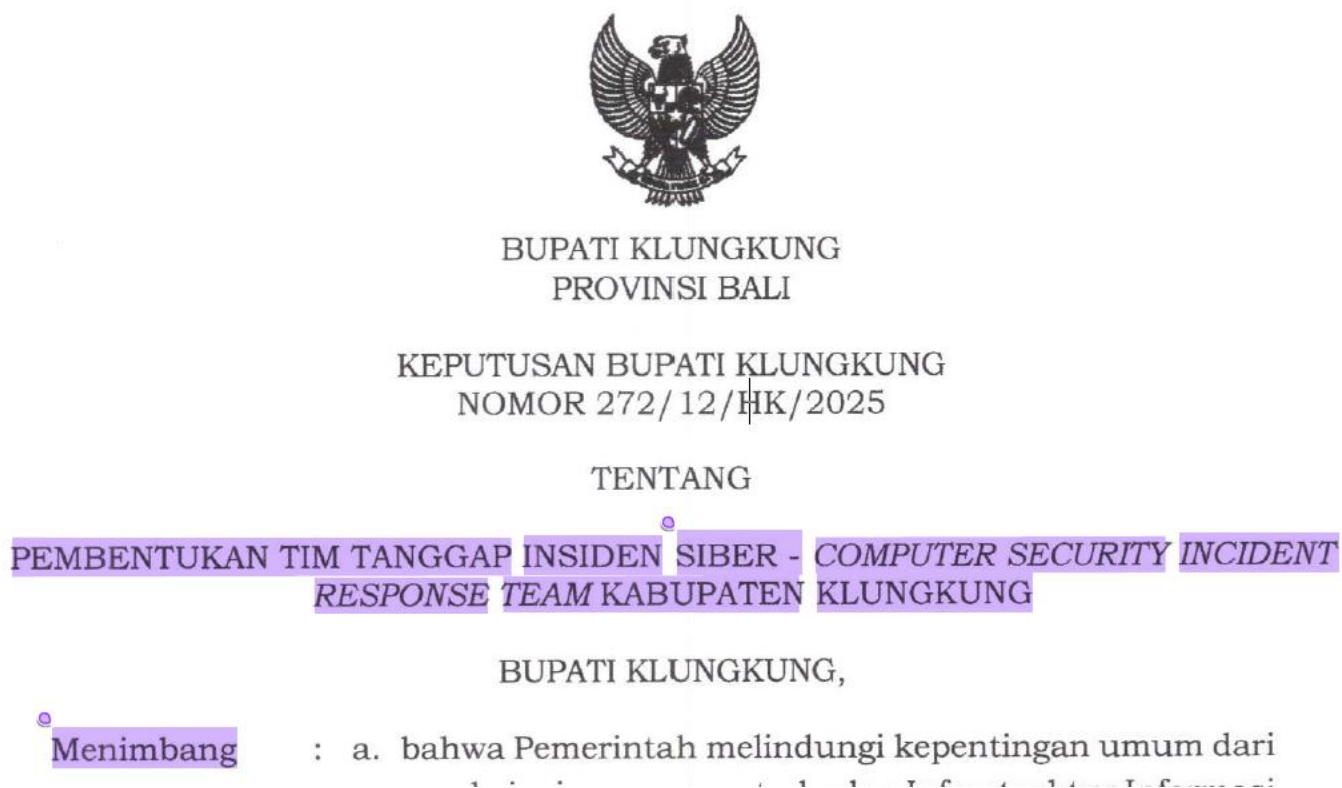
Dokumen 5. Laporan Evaluasi Risiko Semester I 2025

rencana yang seharusnya dilaksanakan pada triwulan berikutnya.	
d. Pemantauan Keterjadian Risiko Tidak terdapat kejadian risiko yang muncul sampai dengan Triwulan II/Semester I. Demikian kami sampaikan. Atas perhatian Bapak, kami mengucapkan terima kasih. Demikian disampaikan atas berkenannya kami ucapkan terima kasih Kepala Dinas Komunikasi dan Informatika Kabupaten Klungkung 	    2 2 ^

Keterangan:

Halaman ini menunjukkan hasil pemantauan keterjadian risiko pada Semester I Tahun 2025. Berdasarkan hasil evaluasi yang dilakukan, tidak terdapat kejadian risiko yang muncul sampai dengan Triwulan II/Semester I. Dokumen ini menjadi bukti bahwa kegiatan evaluasi dan pemantauan risiko telah dilaksanakan secara berkala oleh Diskominfo Klungkung.

Dokumen 6. SK Tim Tanggap Insiden Siber Tahun 2025



Keterangan:

Halaman ini menunjukkan pembentukan Tim Tanggap Insiden Siber sebagai mekanisme respons insiden keamanan informasi.

Dokumen 7. Laporan Monitoring Web Terdampak Serangan Siber Mei 2025

LAPORAN PERBAIKAN WEBSITE PASCA SERANGAN CYBER

Kepada Yth. : Kepala Dinas Komunikasi dan Informatika Kabupaten Klungkung

Perihal : Laporan Perbaikan Website Pasca Serangan Cyber Bulan Mei tahun 2025

I. Pendahuluan

Website merupakan salah satu aset digital yang sangat penting dalam menunjang kegiatan operasional dan layanan informasi. Namun, website juga rentan terhadap berbagai ancaman keamanan siber yang dapat mengganggu ketersediaan, integritas, dan kerahasiaan data. Pada tanggal 28 April 2025, website kami mengalami serangan cyber yang menyebabkan gangguan layanan dan potensi kebocoran data. Laporan ini disusun sebagai dokumentasi atas insiden tersebut, serta upaya yang telah dilakukan dalam penanganan dan pencegahannya.

II. Kronologi Kejadian

Pada tanggal 28 April 2025 pukul 13:30 WITA, ditemukan perubahan tidak sah pada tampilan

Keterangan:

Halaman ini menunjukkan laporan perbaikan website pasca serangan siber yang terjadi pada tahun 2025. Dokumen memuat informasi mengenai insiden yang terjadi, dampak terhadap layanan, serta upaya penanganan dan pencegahan yang dilakukan oleh Diskominfo Klungkung. Dokumen ini menjadi bukti bahwa organisasi telah melakukan pemantauan, penanganan, dan tindak lanjut terhadap insiden keamanan informasi.

Dokumen 8. Laporan Monitoring Server November 2025

LAPORAN TEKNIS MONITORING SERVER

Kepada Yth. : Kepala Dinas Komunikasi dan Informatika Kabupaten Klungkung

Perihal : Monitoring Server yang dikelola Diskominfo Bulan November tahun 2025

I. PENDAHULUAN

Pemeliharaan server mencakup serangkaian kegiatan yang meliputi pengawasan, pengukuran, dan analisis terhadap berbagai parameter kinerja server, seperti penggunaan CPU, memori, disk, serta jaringan. Kegiatan ini dilakukan secara rutin untuk mendeteksi anomali atau masalah sejak dini, sehingga dapat diambil tindakan proaktif untuk mencegah terjadinya gangguan yang lebih serius.

Keterangan:

Halaman ini menunjukkan laporan teknis monitoring server yang dikelola oleh Diskominfo Klungkung pada November 2025. Dokumen ini menjadi bukti bahwa organisasi melaksanakan kegiatan pemantauan infrastruktur I&T secara rutin untuk mendeteksi gangguan, anomali, dan potensi risiko yang dapat memengaruhi keberlangsungan layanan teknologi informasi.

Dokumen 9. Kajian Arsitektur SPBE

TABEL 23. METADATA ARSITEKTUR KEAMANAN SPBE - IDENTIFIKASI KERENTANAN KEAMANAN SPBE

ID	Nama Identifikasi Kerentanan	Deskripsi	Tanggal Kegiatan	→Instansi (Dependency)
DAK.02.02.01	Identifikasi Kerentanan Lingkungan Data	Identifikasi celah keamanan dan kerentanan data pada masing-masing server dengan beragam kondisi	Maret 2025	Pemkab Klungkung

TABEL 24. METADATA ARSITEKTUR KEAMANAN SPBE - PENINGKATAN KEAMANAN SPBE

ID	Nama Kegiatan Peningkatan Keamanan	Deskripsi	Tanggal Kegiatan	→Instansi (Dependency)
DAK.02.03.01	Penggunaan Aplikasi Monitoring Jaringan	Penggunaan Aplikasi Monitoring Jaringan	Januari 2025	Pemkab Klungkung
DAK.02.03.02	Penggunaan Firewall	Penggunaan Firewall dan pembuatan laporannya	November 2025	Pemkab Klungkung
DAK.02.03.03	Penggunaan Aplikasi Monitoring Serangan	Aplikasi Monitoring serangan yang terhubung dengan firewall	November 2025	Pemkab Klungkung

Keterangan:

Halaman ini menunjukkan aktivitas identifikasi kerentanan keamanan SPBE dan upaya peningkatan keamanan yang dilakukan oleh Pemerintah Klungkung. Kegiatan tersebut meliputi identifikasi kerentanan lingkungan data, penggunaan aplikasi monitoring jaringan, penggunaan firewall, serta monitoring serangan. Dokumen ini menjadi bukti adanya aktivitas identifikasi, pengendalian, dan mitigasi risiko keamanan informasi dalam pengelolaan I&T.

Dokumen 10. Renstra 2024–2026

2) Kelemahan

- a) Belum adanya Regulasi/peraturan daerah yang mengatur pengembangan SPBE maupun pelaksanaan aplikasi,
- b) Kuantitas Sumber daya manusia yang ada belum sebanding dengan beban.
- c) Terbatasnya Infrastruktur Telekomunikasi dan Jaringan untuk intergrasi antar Perangkat Daerah
- d) Terbatasnya anggaran yang tersedia di dalam pelaksanaan kegiatan.

Keterangan:

Dokumen ini memuat identifikasi permasalahan strategis, tantangan, dan risiko yang dihadapi Diskominfo dalam penyelenggaraan SPBE, pengelolaan data, dan keamanan informasi. Terdapat uraian mengenai ancaman perkembangan teknologi informasi, kerentanan terhadap serangan siber, keterbatasan infrastruktur TIK, serta kebutuhan penguatan tata kelola keamanan informasi. Informasi tersebut digunakan sebagai dasar identifikasi konteks risiko dan tujuan organisasi dalam pengelolaan risiko I&T. (Bab III Permasalahan dan Isu Strategis Perangkat Daerah, hlm. 45–46).

Lampiran 8. Justifikasi Nilai EDM03

No	Aktivitas	Nilai	Alasan / Justifikasi
1	Memahami organisasi dan konteksnya terkait dengan risiko I&T.	F	Konteks risiko I&T telah dipahami melalui forum rapat staf dan koordinasi TTIS yang membahas ancaman eksternal. Bukti formal berupa Renstra 2024–2026, Perbup 21/2023, <i>Risk Register</i> 2025, SK TTIS 2025, Laporan Evaluasi Risiko SMT I 2025, serta notulen rapat staf menunjukkan bahwa identifikasi risiko dilakukan secara rutin dan terdokumentasi. Seluruh komponen tata kelola COBIT 2019 telah terpenuhi, yaitu: <i>Processes</i>: identifikasi dan analisis risiko dilakukan melalui forum dan laporan berkala; <i>Organizational Structures</i>: TTIS bertugas secara formal menangani isu dan respons risiko I&T; <i>Information Items</i>: <i>Risk Register</i> dan laporan evaluasi menjadi dasar pengambilan keputusan; <i>Policies, Principles, and Frameworks</i>: arah pengendalian risiko diatur dalam Perbup 21/2023 dan Renstra; <i>Culture, Ethics, and Behavior</i>: kesadaran lintas bidang dalam membahas risiko I&T sudah terbangun; <i>People, Skills, and Competencies</i>: staf Bidang Telematika memahami konteks risiko sesuai arahan pimpinan. Aktivitas ini telah dilaksanakan sepenuhnya sesuai COBIT 2019 dan dinilai <i>Fully Achieved</i> (F).
2	Menentukan selera risiko organisasi, yaitu tingkat risiko terkait I&T yang bersedia diambil perusahaan dalam mengejar tujuan perusahaan.	L	Selera risiko organisasi ditetapkan melalui hasil evaluasi dan pembahasan lintas bidang yang diformulasikan oleh Subbag Program (Sunprog) dan disesuaikan dengan arah strategis Diskominfo. Informan menjelaskan bahwa penentuan selera risiko mengacu pada laporan dari masing-masing bidang, kemudian dibandingkan dengan tujuan organisasi dalam Renstra 2024–2026. Bukti dukung berasal dari

No	Aktivitas	Nilai	Alasan / Justifikasi
			<i>Risk Register</i> 2025 Lampiran 1–3, SK TTIS, Renstra 2024–2026, Perbup 21/2023, serta Laporan Evaluasi Risiko SMT I 2025, yang menggambarkan bagaimana organisasi menentukan batas risiko yang masih bisa diterima dalam mendukung strategi digitalisasi dan tata kelola I&T. Komponen COBIT 2019 yang terpenuhi: <i>Processes</i>: proses evaluasi risiko dilakukan melalui analisis kegiatan per bidang dan pembahasan lintas bagian; <i>Organizational Structures</i>: Sunprog dan pimpinan Diskominfo berperan sebagai pengambil keputusan terkait batas risiko; <i>Information Items</i>: dokumen <i>Risk Register</i> dan Renstra digunakan sebagai dasar penetapan arah risiko; <i>Policies, Principles, and Frameworks</i>: Perbup 21/2023 menjadi pedoman umum pengelolaan risiko strategis; <i>Culture, Ethics, and Behavior</i>: kesadaran kolektif tentang pentingnya menyeimbangkan risiko dan peluang sudah terbentuk; <i>People, Skills, and Competencies</i>: staf bidang program dan I&T terlibat aktif dalam penyusunan dan pembahasan risiko. Diskominfo memang sudah menentukan dan membahas batas risiko (risk appetite) dalam rapat dan laporan, tetapi tidak ada notulen rapat dan belum ada dokumen resmi atau peraturan tertulis (misalnya <i>Risk Appetite Statement</i> atau panduan selera risiko I&T organisasi) yang secara langsung menyebutkan batas risiko apa yang boleh diambil, atau bagaimana menentukannya.. Oleh karena itu, aktivitas ini dinilai <i>Largely Achieved</i> (L).
3	Menentukan	P	Berdasarkan hasil FGD dan studi dokumentasi,

No	Aktivitas	Nilai	Alasan / Justifikasi
	tingkat toleransi risiko terhadap selera risiko, yaitu penyimpangan yang dapat diterima sementara dari selera risiko.		Diskominfo belum memiliki pedoman tertulis mengenai batas toleransi risiko I&T (misalnya waktu maksimal gangguan atau tingkat kehilangan data yang masih dapat diterima). Namun, penerapan toleransi dilakukan melalui pengalaman operasional, SOP teknis, dan arahan pimpinan. Informan menjelaskan bahwa standar nasional dan regulasi eksternal seperti Perbup 87/2019 tentang Smart City dan Perbup 21/2023 tentang Masterplan Smart City juga menjadi acuan dalam membedakan risiko jangka pendek (sementara) dan jangka panjang. Beberapa SOP Risiko I&T, seperti SOP Pengelolaan Web OPD, SOP Penyediaan Server, dan SOP Sertifikat Elektronik (AMS, Reset Password, Kehilangan Sertifikat), menunjukkan penerapan batas pengendalian risiko teknis, tetapi belum menjelaskan secara formal ambang toleransi risiko. Komponen COBIT 2019 yang terpenuhi: <i>Processes</i>: mekanisme toleransi risiko diterapkan lewat SOP operasional dan pengalaman lapangan; <i>Organizational Structures</i>: keputusan batas toleransi ditentukan oleh pimpinan bidang sesuai tanggung jawab masing-masing; <i>Information Items</i>: SOP dan Perbup menjadi dasar informasi dalam mengatur batas pengendalian risiko; <i>Policies, Principles, and Frameworks</i>: Perbup 21/2023 dan 87/2019 menjadi acuan umum pengaturan risiko, tetapi belum menetapkan nilai batas formal; <i>Culture, Ethics, and Behavior</i>: staf memahami batas risiko secara praktis berdasarkan arahan pimpinan dan pengalaman kerja; <i>People, Skills, and Competencies</i>: staf I&T menjalankan tindakan pengendalian sesuai arahan pimpinan dan prosedur kerja.

No	Aktivitas	Nilai	Alasan / Justifikasi
			Toleransi risiko sudah diterapkan secara praktik melalui SOP dan arahan pimpinan, namun belum diformalkan dalam dokumen resmi seperti SLA (<i>Service Level Agreement</i>) atau pedoman khusus toleransi risiko yang menetapkan batas toleransi risiko I&T. Oleh karena itu, aktivitas ini dinilai <i>Partially Achieved</i> (P).
4	Menentukan tingkat keselarasan strategi risiko I&T dengan strategi risiko perusahaan dan memastikan selera risiko berada di bawah kapasitas risiko organisasi.	L	Berdasarkan hasil FGD dan studi dokumentasi, strategi risiko I&T di Diskominfo telah dibandingkan dan diselaraskan dengan strategi risiko organisasi secara keseluruhan. Pimpinan memastikan keselarasan ini dengan mengacu pada Renstra 2024–2026, <i>Risk Register</i> 2025, dan Laporan Evaluasi Risiko SMT I 2025. Selain itu, kesesuaian antara strategi risiko I&T dan arah kebijakan nasional juga tercermin dalam Kajian Arsitektur SPBE yang mengikuti standar pemerintah. Forum lintas unit bersama BRIDA (Forum OPD 4 Maret 2025) digunakan untuk meninjau keselarasan program digital dan risiko antarunit. Contoh penerapan nyata terlihat dalam pembentukan Tim Tanggap Insiden Siber (TTIS) yang secara langsung menghubungkan strategi keamanan informasi dengan arah kebijakan organisasi. Komponen COBIT 2019 yang terpenuhi: <i>Processes</i>: mekanisme peninjauan keselarasan dilakukan melalui forum OPD dan evaluasi tahunan risiko; <i>Organizational Structures</i>: pimpinan berperan langsung memastikan arah risiko I&T tetap sesuai strategi organisasi; <i>Information Items</i>: Renstra, <i>Risk Register</i> 2025, Laporan Evaluasi Risiko SMT I 2025, dan Kajian Arsitektur SPBE menjadi bukti integrasi formal; <i>Policies, Principles, and Frameworks</i>:

No	Aktivitas	Nilai	Alasan / Justifikasi
			penyesuaian dilakukan dengan mengacu pada Renstra dan kebijakan SPBE nasional; <i>Culture, Ethics, and Behavior</i> : kesadaran pimpinan dan koordinasi lintas unit menunjukkan budaya kolaboratif dalam mengelola risiko I&T; <i>People, Skills, and Competencies</i> : staf Bidang Telematika dan perencanaan memahami peran mereka dalam menjaga keselarasan strategi risiko. Strategi risiko I&T telah diselaraskan dengan strategi organisasi dan kebijakan nasional, namun belum ada analisis kapasitas risiko yang kuantitatif. Oleh karena itu, aktivitas ini dinilai <i>Largely Achieved</i> (L).
5	Mengevaluasi faktor risiko I&T secara proaktif sebelum mengambil keputusan strategis perusahaan dan memastikan bahwa pertimbangan risiko menjadi bagian dari proses pengambilan keputusan strategis perusahaan.	L Level 3 Akt 1	Berdasarkan hasil FGD dan studi dokumentasi, Diskominfo telah melakukan penilaian risiko I&T sebelum pengambilan keputusan strategis, khususnya yang berkaitan dengan program digitalisasi dan layanan publik. Proses ini didukung oleh <i>Risk Register 2025 TTE</i> dan <i>Renstra 2024–2026</i> , yang mencatat risiko strategis dan langkah mitigasinya. Masukan terkait risiko I&T diberikan oleh seluruh staf dalam rapat, namun belum ada prosedur baku atau aturan tertulis yang mengatur penyampaian risiko sebelum keputusan dibuat. Informasi risiko biasanya disampaikan secara lisan dan tertulis setelah diformalkan dalam laporan atau dokumen kegiatan. Faktor risiko I&T belum selalu menjadi agenda tetap rapat pimpinan, tetapi pimpinan cenderung merespons secara terbuka terhadap masukan staf. Hasil evaluasi risiko terdokumentasi dalam Laporan Evaluasi Risiko SMT I 2025, namun belum ditemukan contoh nyata keputusan strategis yang diubah langsung karena pertimbangan risiko I&T. Komponen COBIT 2019 yang terpenuhi: <i>Processes</i> :

No	Aktivitas	Nilai	Alasan / Justifikasi
			proses penilaian risiko dilakukan sebelum keputusan strategis melalui <i>Risk Register</i> dan laporan evaluasi; <i>Organizational Structures</i>: seluruh staf berperan memberikan masukan risiko dalam rapat pimpinan; <i>Information Items</i>: laporan evaluasi risiko SMT I 2025 menjadi bukti dokumentasi hasil pertimbangan risiko; <i>Policies, Principles, and Frameworks</i>: belum tersedia aturan formal mengenai tata cara penyampaian risiko dalam rapat; <i>Information Flows</i>: komunikasi risiko dilakukan secara lisan dan tertulis setelah diformalkan; <i>Culture, Ethics, and Behavior</i>: pimpinan terbuka terhadap masukan risiko dari staf meskipun belum menjadi agenda tetap. Evaluasi risiko I&T dilakukan sebelum keputusan strategis, tetapi masih bersifat informal dan belum diatur dalam prosedur resmi. Oleh karena itu, aktivitas ini dinilai <i>Largely Achieved</i> (L).
6	Mengevaluasi aktivitas manajemen risiko untuk memastikan keselarasan dengan kapasitas perusahaan terhadap kerugian terkait I&T dan toleransi pimpinan terhadap kerugian tersebut.	F Level 3 Akt 2	Berdasarkan hasil FGD dan studi dokumentasi, kegiatan evaluasi manajemen risiko I&T dilakukan secara formal dan rutin setiap semester, dengan bukti Laporan Evaluasi Risiko SMT I 2025. Evaluasi ini memastikan seluruh kegiatan pengelolaan risiko sesuai kapasitas keuangan dan sumber daya yang ditetapkan dalam dokumen Renja 2025. Pimpinan juga menetapkan batas kerugian yang dapat ditoleransi, meskipun belum dituangkan dalam angka kuantitatif. Hasil evaluasi risiko dilaporkan setiap bulan kepada pimpinan untuk ditindaklanjuti. Belum ada kasus koreksi besar karena pelampauan kapasitas organisasi, namun mekanisme eskalasi risiko tetap tersedia melalui jalur pelaporan resmi dan surat dinas. Sikap pimpinan

No	Aktivitas	Nilai	Alasan / Justifikasi
			terhadap hasil evaluasi bersifat terbuka dan menerima, dengan langkah tindak lanjut melalui rapat evaluasi internal meskipun notulen rapat tidak ditemukan secara formal. Komponen COBIT 2019 yang terpenuhi: <i>Processes</i>: kegiatan evaluasi risiko dilakukan secara rutin dan terdokumentasi dalam laporan semesteran; <i>Organizational Structures</i>: pimpinan dan bidang terkait berperan langsung dalam menilai hasil evaluasi dan menentukan tindak lanjut; <i>Information Items</i>: laporan evaluasi risiko SMT I 2025 menjadi dokumen utama pelaporan hasil evaluasi; <i>Policies, Principles, and Frameworks</i>: kapasitas organisasi dan sumber daya ditetapkan dalam dokumen Renja; <i>Information Flows</i>: hasil evaluasi disampaikan secara formal melalui laporan dan surat pelaporan risiko; <i>Culture, Ethics, and Behavior</i>: pimpinan menunjukkan keterbukaan dan komitmen terhadap hasil evaluasi meskipun tanpa catatan notulen formal; <i>People, Skills, and Competencies</i>: staf Bidang Telematika dan perencanaan mampu menilai dan melaporkan hasil evaluasi risiko secara berkala. Evaluasi risiko I&T di Diskominfo telah dilakukan secara rutin, terdokumentasi, dan selaras dengan kapasitas organisasi. Semua komponen COBIT 2019 terpenuhi, sehingga aktivitas ini dinilai <i>Fully Achieved</i> (F).
7	Merekrut dan mempertahankan keterampilan dan personel yang	L Level 3 Akt 3	Diskominfo telah memiliki staf khusus yang menangani manajemen risiko I&T yang tertuang secara formal dalam SK TTIS Tahun 2025, menunjukkan struktur organisasi telah menetapkan peran dan tanggung jawab

No	Aktivitas	Nilai	Alasan / Justifikasi
	diperlukan untuk Manajemen Risiko I&T.		secara jelas. Identifikasi kebutuhan keterampilan dilakukan melalui proses perencanaan kerja tahunan (Renja 2025) yang mencantumkan kebutuhan SDM bidang keamanan informasi dan risiko I&T. Kegiatan peningkatan kapasitas staf juga dilakukan melalui pelatihan eksternal, salah satunya Workshop Penguatan TTIS (5–7 November 2025) yang menjadi bukti nyata pelaksanaan program peningkatan kompetensi. Staf baru diberi briefing langsung dari pimpinan untuk memahami kebijakan dan prosedur manajemen risiko. Namun, belum ada program retensi formal (seperti promosi, penghargaan, atau jalur karier) bagi staf berkompeten di bidang risiko I&T. Kekurangan staf berkompeten diatasi melalui penugasan tambahan berdasarkan SK TTIS. Perencanaan pengembangan kompetensi jangka panjang telah tercantum dalam Renstra 2024–2026, dan pembelajaran daring difasilitasi melalui platform CORPU (<i>Corporate University</i>) pada situs CSIRT. Meskipun demikian, evaluasi kompetensi formal terhadap staf risiko I&T belum pernah dilakukan. Komponen COBIT 2019 yang terpenuhi: <i>Organizational Structures</i>: keberadaan SK TTIS menegaskan struktur dan tanggung jawab staf risiko I&T; <i>Processes</i>: identifikasi kebutuhan SDM dan pelatihan dilakukan melalui Renja serta penugasan; <i>People, Skills & Competencies</i>: pelatihan eksternal dan CORPU sudah dimanfaatkan, namun evaluasi kompetensi belum rutin; <i>Policies, Principles & Frameworks</i>: rencana pengembangan SDM terdapat dalam Renstra 2024–2026; <i>Services & Infrastructure</i>:

No	Aktivitas	Nilai	Alasan / Justifikasi
			penggunaan platform CORPU sebagai sarana pembelajaran online; <i>Culture, Ethics & Behavior</i>: belum ada sistem penghargaan atau retensi yang mendorong keberlanjutan staf berkompeten. Aktivitas sudah dilaksanakan secara substansial dan terstruktur, tetapi belum disertai mekanisme retensi serta evaluasi kompetensi formal. Oleh karena itu, dinilai <i>Largely Achieved</i> (L).
8	Mengarahkan penerjemahan dan integrasi strategi risiko I&T ke dalam praktik manajemen risiko dan aktivitas operasional.	F Level 1 Akt 5	Strategi risiko I&T di Diskominfo Klungkung telah diterjemahkan secara nyata dalam kegiatan operasional sehari-hari. Bukti implementasi terlihat dari penerapan kontrol akses fisik menggunakan sidik jari untuk memasuki ruang server sebagai bagian dari pengendalian risiko. Penanggung jawab utama integrasi strategi ke operasional adalah Kepala Dinas, dengan pelaksanaan teknis dibantu oleh Bidang Telematika dan tim TTIS. Dokumen pendukung berupa SOP Risiko I&T (nomor 29, 34, 35, dan 43–47) menjelaskan mekanisme penerapan strategi di tingkat operasional, seperti pengelolaan gangguan, pemeliharaan server, dan kontrol keamanan sertifikat elektronik. Pemahaman staf terhadap strategi ini dilakukan melalui komunikasi dan sosialisasi, dibuktikan dengan Laporan Workshop Penguatan TTIS (5–7 November 2025). Pemantauan integrasi strategi dilakukan melalui rapat rutin dan telaah staf, dengan Telaahan Staf Kiwa Tengen sebagai bukti dokumentasi hasil evaluasi penerapan strategi di lapangan. Contoh nyata integrasi strategi risiko terlihat dari pembatasan akses hanya kepada admin tertentu yang mengetahui kata sandi sistem, sesuai ketentuan SOP nomor 35 dan 43–47. Efektivitas penerapan

No	Aktivitas	Nilai	Alasan / Justifikasi
			strategi risiko diukur menggunakan indikator kinerja (KPI) yang termuat dalam Renstra 2024–2026 serta diperbarui melalui Laporan Evaluasi Risiko Semester I 2025. Tidak ditemukan kasus kegagalan implementasi strategi di lapangan, sebagaimana diperkuat dalam Laporan Evaluasi Renja Triwulan II 2025 yang memuat rekapitulasi Indikator Kinerja Kegiatan (IKK). Komponen COBIT 2019 yang terpenuhi: <i>Processes</i>: strategi diterapkan ke SOP dan prosedur operasional; <i>Organizational Structures</i>: Kepala Dinas dan TTIS memastikan pelaksanaan di lapangan; <i>Information Items</i>: SOP Risiko I&T dan telaahan staf sebagai dokumen pendukung; <i>Policies, Principles & Frameworks</i>: KPI dan target dalam Renstra mendukung evaluasi efektivitas; <i>Information Flows</i>: laporan dan rapat rutin menjamin pemantauan berkelanjutan; <i>Culture & Behavior</i>: staf aktif menerapkan kontrol risiko dan menjaga kepatuhan operasional. Seluruh elemen penerapan strategi risiko ke aktivitas operasional telah berjalan sesuai praktik COBIT 2019 dan didukung bukti pendukung yang relevanserta konsisten. Oleh karena itu, aktivitas ini dinilai <i>Fully Achieved</i> (F).
9	Mengarahkan pengembangan rencana komunikasi risiko (mencakup semua tingkatan perusahaan).	P Level 1 Akt 6	Proses komunikasi risiko di Diskominfo sudah berjalan melalui forum konsultasi public meskipun belum ada dokumen resmi seperti rencana komunikasi risiko yang tertulis. Penyampaian informasi risiko dilakukan oleh Subbagian Umum dan Kepegawaian (Sekretariat) kepada pimpinan dan staf teknis melalui jalur komunikasi rutin. Bukti pendukung berupa Laporan Evaluasi Risiko Semester I Tahun 2025, yang

No	Aktivitas	Nilai	Alasan / Justifikasi
			menunjukkan adanya evaluasi efektivitas komunikasi melalui Satuan Pengawas Internal (SPI). Namun, tidak ditemukan notulen rapat atau dokumen tertulis yang secara spesifik mengatur tata cara komunikasi risiko lintas level. Komponen COBIT 2019 yang terpenuhi: <i>Processes</i>: komunikasi risiko sudah berjalan, tetapi belum ada panduan resmi; <i>Organizational Structures</i>: tanggung jawab berada di Sekretariat; <i>Information Flows</i>: komunikasi dilakukan melalui rapat dan forum publik; <i>People, Skills & Competencies</i>: belum ada pelatihan khusus tentang komunikasi risiko; <i>Culture & Behavior</i>: budaya kerja terbuka mendukung proses komunikasi informal. Dengan kondisi tersebut, aktivitas ini dinyatakan <i>Partially Achieved</i> (P) karena praktik komunikasi risiko sudah dilakukan tetapi belum memiliki panduan formal atau mekanisme resmi yang terdokumentasi.
10	Mengarahkan penerapan mekanisme yang tepat untuk merespons perubahan risiko dengan cepat dan segera melaporkannya ke tingkat manajemen yang sesuai, didukung oleh prinsip-	L Level 1 Akt 7	Diskominfo Klungkung belum memiliki mekanisme formal yang mengatur respons cepat terhadap perubahan risiko I&T, namun praktiknya sudah berjalan melalui telaah staf dan SOP terkait insiden TI, seperti SOP No. 29 (Laporan Gangguan Internet/Wi-Fi) dan SOP No. 34 (Pengelolaan Web OPD). Penanggung jawab pelaporan risiko adalah Subbagian Perencanaan (Sunprog) yang menindaklanjuti laporan dengan Rencana Tindak Lanjut sebagaimana tercantum pada Laporan Evaluasi Risiko SMT I 2025. Laporan diteruskan ke pimpinan untuk validasi melalui tanda tangan elektronik (TTD). Selain itu, terdapat sarana pengaduan insiden I&T melalui laman CSIRT

No	Aktivitas	Nilai	Alasan / Justifikasi
	prinsip eskalasi yang disepakati (apa yang harus dilaporkan, kapan, di mana, dan bagaimana).		Diskominfo yang memungkinkan pelaporan risiko secara cepat. Kasus pada Laporan Monitoring Web Terdampak Serangan Cyber Mei 2025 menunjukkan adanya respons langsung terhadap serangan, meskipun belum diformalkan dalam sistem eskalasi risiko. Komponen COBIT 2019 yang terpenuhi: <i>Processes</i>: SOP sudah mengatur pelaporan risiko namun belum ada prosedur tanggap formal; <i>Organizational Structures</i>: Subbagian Perencanaan (Sunprog) berperan sebagai penerima dan pelaksana tindak lanjut; <i>Information Items</i>: Bukti rencana tindak lanjut dalam laporan evaluasi risiko SMT I 2025; <i>Culture, Ethics & Behavior</i>: Pimpinan merespons laporan secara cepat dan terbuka; <i>People, Skills & Competencies</i>: Belum ada pelatihan atau penugasan staf khusus tanggap risiko; <i>Services, Infrastructure & Applications</i>: Sistem pelaporan insiden melalui laman CSIRT sudah digunakan. Dengan kondisi ini, aktivitas dinilai <i>Largely Achieved</i> (L) karena sebagian besar praktik telah dilakukan pada beberapa kondisi, namun belum ada mekanisme formal dan SDM khusus yang menangani respons risiko secara terstruktur.
11	Mengarahkan agar risiko, peluang, isu, dan kekhawatiran dapat diidentifikasi dan dilaporkan oleh siapa pun	P Level 1 Akt 8	Berdasarkan hasil FGD dan studi dokumentasi, mekanisme pelaporan risiko di Diskominfo Klungkung belum diatur dalam kebijakan formal yang memperbolehkan semua pegawai melaporkan risiko tanpa batasan hierarki. Tidak ditemukan peraturan atau surat keputusan yang mengatur <i>open risk reporting policy</i>. Namun secara praktik, staf dapat menyampaikan risiko,

No	Aktivitas	Nilai	Alasan / Justifikasi
	kepada pihak yang tepat kapan saja. Risiko harus dikelola sesuai dengan kebijakan dan prosedur yang dipublikasikan dan dieskalasikan kepada para pengambil keputusan yang relevan.		isu, atau peluang secara langsung kepada Kepala Bidang melalui komunikasi informal atau saat rapat koordinasi rutin. Organisasi telah menyediakan sarana resmi pelaporan publik melalui aplikasi “Klungkung Mesadu”, yang memungkinkan penyampaian keluhan atau temuan risiko layanan. Meskipun aplikasi ini tidak dirancang khusus untuk pelaporan risiko internal I&T, sarana ini menunjukkan adanya kanal terbuka yang dapat digunakan untuk isu terkait layanan digital. Dari sisi proses, SOP No. 29, 34, dan 35 sudah menjelaskan alur tindak lanjut laporan staf, terutama terkait gangguan jaringan, pengelolaan web OPD, dan Fasilitas Penyediaan Server (VPS). Laporan staf yang berisi potensi risiko operasional diteruskan oleh pejabat bidang ke pimpinan untuk diproses lebih lanjut. Selain itu, hasil FGD menunjukkan bahwa peluang atau masukan staf sering dipertimbangkan dalam perencanaan strategis, sebagaimana tercermin dalam <i>Renstra 2024–2026</i> yang memuat gagasan inovasi digital berasal dari bidang teknis. Kasus konkret yang memperkuat bukti adalah laporan serangan DDoS pada jaringan digital Diskominfo, yang pertama kali disampaikan staf Bidang Telematika kepada pimpinan, sehingga tindakan mitigasi dapat dilakukan lebih cepat. Laporan ini terdokumentasi dalam <i>Laporan Monitoring Web Terdampak Serangan Cyber Mei 2025</i>. Komponen COBIT 2019 yang terpenuhi: <i>Processes</i>: alur tindak lanjut laporan staf sudah dijelaskan melalui SOP No. 29, 34, dan 35; <i>Organizational Structures</i>: Kepala Bidang menjadi pejabat penerima laporan risiko; <i>Information Flows</i>: komunikasi risiko masih

No	Aktivitas	Nilai	Alasan / Justifikasi
			dilakukan secara langsung, belum melalui sistem pelaporan risiko khusus; <i>Policies, Principles & Frameworks</i>: belum ada kebijakan formal tentang pelaporan risiko terbuka; <i>Culture, Ethics & Behavior</i>: budaya pelaporan risiko masih bergantung pada inisiatif staf, tidak ada mekanisme anonim; <i>Services & Infrastructure</i>: tersedia aplikasi <i>Klungkung Mesadu</i> yang berfungsi sebagai sarana pelaporan umum; <i>Information Items</i>: laporan insiden DDoS menjadi contoh nyata efektivitas pelaporan risiko staf. Aktivitas ini sudah dijalankan secara substantif, karena risiko dapat dilaporkan oleh staf dan ditindaklanjuti oleh pimpinan melalui SOP operasional. Namun karena belum ada kebijakan formal, mekanisme anonim, atau sistem pelaporan risiko internal khusus, maka aktivitas ini dinilai <i>Partially Achieved</i> (P).
12	Mengidentifikasi tujuan dan metrik utama dari proses tata kelola dan manajemen risiko yang akan dipantau, dan menyetujui pendekatan, metode, teknik, dan proses untuk menangkap dan melaporkan informasi pengukuran.	F Level 3 Akt 4	Berdasarkan hasil FGD dan studi dokumentasi, Diskominfo Klungkung telah menetapkan tujuan utama dan indikator kinerja (KPI) manajemen risiko I&T secara jelas dan terdokumentasi. Tujuan tata kelola risiko I&T tertuang dalam Renja Diskominfo 2025, yang menyebutkan penguatan keamanan informasi dan peningkatan efektivitas layanan digital sebagai arah strategis utama pengelolaan risiko. Indikator keberhasilan manajemen risiko ditentukan dan diukur menggunakan dokumen <i>Risk Register 2025</i> . Setiap risiko memiliki parameter “kemungkinan” dan “dampak” serta status mitigasi yang diperbarui setiap semester. Hal ini berfungsi sebagai KPI fungsional untuk menilai efektivitas pengendalian risiko. Penyetujuan terhadap metrik dan indikator risiko

No	Aktivitas	Nilai	Alasan / Justifikasi
			dilakukan oleh pimpinan sebagaimana tertuang dalam Surat Keputusan Nomor 23 Tahun 2025 tentang Penetapan Penanggung Jawab Risiko Bidang, yang juga menetapkan pejabat terkait dalam proses validasi data risiko. SK ini menunjukkan struktur tanggung jawab yang jelas sesuai prinsip RACI (Responsible, Accountable, Consulted, Informed) COBIT 2019. Untuk pengukuran kinerja risiko, <i>Risk Register</i> dan Laporan Evaluasi Risiko Semester I 2025 berfungsi sebagai instrumen utama pengumpulan data. Meskipun belum ada aplikasi khusus, hasil studi dokumentasi menemukan berkas spreadsheet “LAP_110102-2025-032-20250702-1427-aset.xlsx” yang digunakan sebagai media monitoring aset dan risiko, menandakan bahwa tools sederhana (spreadsheet monitoring) telah digunakan secara sistematis. Dengan temuan dokumen tersebut, indikator pengumpulan data dinilai terpenuhi. Hasil pengukuran risiko dilaporkan secara formal kepada pimpinan melalui Laporan Evaluasi Risiko Semester I 2025, yang berisi rekapitulasi status mitigasi dan efektivitas kontrol risiko. Pimpinan menilai kesesuaian indikator dengan tujuan strategis berdasarkan dampak risiko terhadap layanan prioritas, bukan hanya skor numerik. Selain itu, <i>Risk Register</i> diperbarui tahunan dan pernah mengalami revisi indikator bersama BSSN untuk menyesuaikan dengan konteks ancaman siber 2025, menunjukkan adanya <i>continuous improvement</i> dalam metrik risiko. Komponen COBIT 2019 yang terpenuhi: <i>Policies, Principles & Frameworks</i>: Tujuan tata kelola risiko I&T tercantum dalam Renja Diskominfo 2025;

No	Aktivitas	Nilai	Alasan / Justifikasi
			<i>Processes</i>: Penetapan dan revisi KPI risiko dilakukan melalui <i>Risk Register</i> dan koordinasi dengan BSSN; <i>Organizational Structures</i>: SK Nomor 23 Tahun 2025 menetapkan pimpinan sebagai penanggung jawab validasi metrik risiko; <i>Information Flows</i>: Pelaporan risiko dilakukan melalui Laporan Evaluasi Risiko SMT I 2025; <i>Services & Infrastructure</i>: Tools pengumpulan data risiko menggunakan spreadsheet monitoring yang ditemukan saat studi dokumentasi; <i>Culture & Behavior</i>: Pimpinan aktif menilai dampak risiko terhadap tujuan strategis, menunjukkan kesadaran tinggi terhadap pentingnya indikator risiko; <i>Information Items</i>: Dokumentasi <i>Risk Register</i> tahunan dan revisi indikator menjadi bukti nyata pemantauan berkelanjutan. Dengan seluruh elemen COBIT 2019 telah terpenuhi, tujuan dan metrik risiko ditetapkan, dimonitor, dilaporkan, serta diperbarui secara berkala dengan dukungan bukti dokumen lengkap dan terbaru. Oleh karena itu, aktivitas ini dinilai <i>Fully Achieved</i> (F).
13	Melaporkan setiap permasalahan terkait manajemen risiko kepada Dewan Komisaris atau komite eksekutif.	F Level 1 Akt 9	Diskominfo Klungkung memiliki mekanisme resmi untuk melaporkan masalah manajemen risiko kepada pimpinan melalui surat dan laporan tertulis yang disahkan secara formal. Bukti yang mendukung mekanisme ini terdapat dalam Laporan Evaluasi Risiko Semester I Tahun 2025, yang berisi identifikasi risiko, kendala pelaksanaan, serta tindak lanjut yang telah dilakukan. Bidang Telematika bertanggung jawab menyusun dan menyampaikan laporan risiko kepada Kepala Dinas, sebagaimana diatur dalam SK Nomor 23 Tahun 2025 tentang Penetapan Penanggung Jawab Risiko Bidang. Struktur tanggung jawab ini sudah

No	Aktivitas	Nilai	Alasan / Justifikasi
			sesuai prinsip RACI COBIT 2019, di mana bidang bertindak sebagai <i>Responsible</i> dan pimpinan sebagai <i>Accountable</i> atas keputusan tindak lanjut risiko. Penyampaian laporan dilakukan secara tertulis melalui surat resmi dan rapat staf, dibuktikan dengan notulen rapat pimpinan yang mencatat pembahasan risiko operasional, termasuk risiko keamanan jaringan dan layanan digital. Semua laporan disimpan dan terdokumentasi dalam arsip resmi organisasi. Hasil FGD menunjukkan bahwa pimpinan menanggapi laporan risiko dengan serius, memberikan instruksi langsung untuk penanganan dan evaluasi lanjutan. Tindakan pimpinan mencerminkan budaya organisasi yang terbuka dan responsif terhadap permasalahan risiko. Komponen COBIT 2019 yang terpenuhi: <i>Policies, Principles & Frameworks</i>: mekanisme pelaporan diatur melalui surat resmi dan laporan evaluasi; <i>Organizational Structures</i>: Bidang Telematika bertugas menyusun laporan dan melapor ke Kepala Dinas (SK Nomor 23 Tahun 2025); <i>Information Flows</i>: pelaporan dilakukan tertulis dan dibahas dalam rapat staf; <i>Information Items</i>: laporan evaluasi risiko dan notulen rapat menjadi bukti dokumentasi formal; <i>Culture & Behavior</i>: pimpinan responsif dan serius menindaklanjuti laporan risiko. Seluruh komponen pelaporan dan dokumentasi telah berjalan sesuai prinsip COBIT 2019, dengan bukti pendukung yang relevan dan konsisten. Oleh karena itu, aktivitas ini dinilai <i>Fully Achieved</i> (F).
14	Memantau sejauh	L	Berdasarkan hasil FGD dan studi dokumentasi,

No	Aktivitas	Nilai	Alasan / Justifikasi
	mana profil risiko dikelola dalam selera risiko dan ambang batas toleransi perusahaan.	Level 3 Akt 5	Diskominfo Klungkung telah melakukan pemantauan rutin terhadap profil risiko I&T dan membandingkannya dengan tingkat risiko yang telah ditetapkan dalam <i>Risk Register 2025 TTE</i> serta Laporan Evaluasi Risiko Semester I Tahun 2025. Pemantauan dilakukan oleh Subbagian Perencanaan (Sunprog) sebagai <i>risk owner</i>, yang memastikan setiap bidang melaporkan status mitigasi dan tingkat risiko aktual. Hasil pemantauan disampaikan secara formal kepada pimpinan melalui laporan evaluasi risiko semesteran, yang mencakup perkembangan status risiko (tinggi, sedang, rendah) dan tindakan mitigasi yang sudah dilakukan. Namun, organisasi belum memiliki aplikasi atau sistem khusus untuk memantau profil risiko secara digital; pemantauan masih dilakukan secara manual melalui dokumen Excel dan laporan naratif. Dari hasil FGD, tidak pernah terjadi pelampauan batas toleransi risiko, sehingga belum ada reaksi atau evaluasi budaya organisasi terhadap kondisi tersebut. Temuan studi dokumentasi menunjukkan bahwa hasil pemantauan digunakan untuk memperbarui dan menambahkan mitigasi baru dalam <i>Risk Register</i>, sehingga dapat disimpulkan bahwa data monitoring sudah digunakan untuk perbaikan strategi secara tidak langsung. Komponen COBIT 2019 yang terpenuhi: <i>Processes</i>: mekanisme pemantauan profil risiko dilakukan rutin setiap semester dan tercatat dalam <i>Risk Register</i>; <i>Organizational Structures</i>: Sunprog bertanggung jawab sebagai pejabat pengelola risiko (<i>risk owner</i>); <i>Information Flows</i>: laporan hasil pemantauan disampaikan ke pimpinan melalui Laporan Evaluasi

No	Aktivitas	Nilai	Alasan / Justifikasi
			Risiko SMT I 2025; <i>Information Items</i>: dokumen <i>Risk Register</i> menunjukkan hasil pembaruan mitigasi risiko; <i>Services & Infrastructure</i>: belum ada sistem atau aplikasi khusus untuk monitoring risiko; <i>Culture & Behavior</i>: belum pernah ada pelanggaran toleransi, sehingga reaksi budaya belum terukur. Aktivitas ini sudah berjalan substansial dan rutin, tetapi masih dilakukan secara manual dan belum menggunakan sistem monitoring terintegrasi. Oleh karena itu, aktivitas ini dinilai <i>Largely Achieved</i> (L).
15	Memantau tujuan dan metrik utama tata kelola risiko dan proses manajemen terhadap target, menganalisis penyebab penyimpangan, dan mengambil tindakan perbaikan untuk mengatasi penyebab yang mendasarinya.	L Level 4 Akt 1	Diskominfo Klungkung memiliki target yang jelas untuk tata kelola risiko I&T, sebagaimana tercantum dalam <i>Risk Register 2025</i> dan <i>Renstra 2024–2026</i> yang menetapkan sasaran peningkatan keamanan informasi dan stabilitas layanan digital sebagai KPI utama. Kinerja risiko dipantau secara periodik melalui Laporan Evaluasi Risiko Semester I 2025, yang membandingkan status mitigasi terhadap target yang ditetapkan pada awal tahun. Analisis atas penyimpangan dilakukan oleh pengelola risiko (Sunprog) bersama pimpinan, sesuai pembagian tanggung jawab dalam SK Nomor 23 Tahun 2025. Hasil monitoring dan status kinerja risiko terdokumentasi secara formal pada bagian Rencana Tindak Lanjut (RTL) dalam laporan evaluasi, yang berfungsi sebagai <i>Risk Treatment Plan</i> (RTP) dan bukti pelaksanaan evaluasi risiko. Namun, organisasi belum memiliki prosedur formal untuk analisis akar penyebab (root cause analysis) terhadap penyimpangan risiko, dan belum ada pedoman tindakan korektif tertulis bila indikator tidak tercapai. Meskipun demikian, pimpinan menunjukkan sikap positif dengan mendorong

No	Aktivitas	Nilai	Alasan / Justifikasi
			pencarian solusi bersama, bukan menyalahkan staf. Belum ditemukan bukti adanya tindakan korektif yang secara terukur mengembalikan kinerja risiko ke target, namun hasil monitoring digunakan sebagai dasar perbaikan mitigasi pada periode berikutnya. Komponen COBIT 2019 yang terpenuhi: <i>Policies, Principles & Frameworks</i>: target dan KPI risiko ditetapkan dalam Renstra dan <i>Risk Register</i>; <i>Processes</i>: evaluasi dan perbandingan kinerja risiko dilakukan setiap semester, meski tanpa analisis penyebab formal; <i>Organizational Structures</i>: Sunprog dan pimpinan berperan aktif sesuai SK Nomor 23 Tahun 2025; <i>Information Items</i>: laporan evaluasi dan RTP menjadi bukti dokumentasi pemantauan; <i>Culture & Behavior</i>: pimpinan bersikap terbuka dan mencari solusi atas penyimpangan risiko; <i>Information Flows</i>: hasil evaluasi disampaikan secara resmi melalui laporan semesteran. Aktivitas ini telah berjalan dengan baik dan rutin, namun belum sepenuhnya memenuhi unsur COBIT karena tidak adanya analisis akar penyebab dan prosedur korektif formal. Oleh karena itu, aktivitas ini dinilai <i>Largely Achieved</i> (L).
16	Memungkinkan peninjauan oleh pemangku kepentingan utama atas kemajuan perusahaan terhadap tujuan yang telah	F Level 4 Akt 2	Diskominfo Klungkung secara aktif melibatkan pemangku kepentingan internal dan eksternal dalam meninjau kemajuan pencapaian tujuan risiko I&T. Bukti pelibatan terlihat pada Berita Acara Forum OPD 2025 dan Surat Forum OPD tertanggal 4 Maret 2025, yang menunjukkan koordinasi lintas unit dan pembahasan capaian kinerja risiko serta program digitalisasi. Forum formal seperti Forum Konsultasi Publik dan Forum OPD digunakan untuk meninjau

No	Aktivitas	Nilai	Alasan / Justifikasi
	ditetapkan.		kemajuan strategi dan pelaksanaan manajemen risiko. Proses peninjauan ini juga dilakukan secara daring melalui <i>Zoom Meeting</i>, dan rekamannya disimpan sebagai bukti pelaksanaan kegiatan. Masukan dari peserta forum digunakan untuk menyempurnakan dokumen perencanaan, dibuktikan dengan adanya revisi dalam Rancangan Final Renja. Hal ini menunjukkan bahwa siklus perbaikan berdasarkan masukan pemangku kepentingan telah berjalan. Selain itu, organisasi menyediakan laporan Survei Kepuasan Masyarakat (SKM) setiap tiga bulan sebagai bentuk transparansi dan pelaporan hasil kepada publik. Dari sisi budaya, pimpinan dan staf menunjukkan keterbukaan dalam menerima kritik dan saran dari pemangku kepentingan, baik secara langsung dalam forum maupun melalui media daring. Komponen COBIT 2019 yang terpenuhi: <i>Organizational Structures</i>: pelibatan aktif OPD dan pihak eksternal dalam forum resmi; <i>Processes</i>: forum peninjauan dilakukan rutin dan hasilnya digunakan untuk perbaikan; <i>Information Items</i>: rekaman Zoom dan dokumen berita acara sebagai bukti peninjauan; <i>Information Flows</i>: hasil peninjauan disampaikan melalui laporan SKM dan forum publik; <i>Culture & Behavior</i>: organisasi terbuka terhadap kritik dan menjadikannya masukan konstruktif. Seluruh aspek pelaksanaan peninjauan dan pelibatan pemangku kepentingan telah berjalan sesuai praktik COBIT 2019 dan didukung bukti pendukung yang relevan. Oleh karena itu, aktivitas ini dinilai <i>Fully Achieved</i> (F).

Lampiran 9. Justifikasi Nilai APO12

No	Aktivitas	Nilai	Alasan / Justifikasi
1	Membangun dan memelihara metode untuk pengumpulan, klasifikasi, dan analisis data terkait risiko I&T.	L	Diskominfo Klungkung telah memiliki metode untuk pengumpulan dan analisis data risiko yang tercermin dalam <i>Risk Register 2025 TTE</i> dan <i>Form Risiko Prioritas</i>. Dokumen tersebut berisi identifikasi risiko, kategori, nilai risiko, serta rencana pengendalian, yang menunjukkan adanya proses pengumpulan dan analisis yang berjalan. Verifikasi data risiko juga dilakukan bersama BSSN sebagaimana tercantum dalam <i>Laporan TMPI Kabupaten Klungkung</i>. Namun, tidak ditemukan SOP atau pedoman formal yang secara eksplisit mendeskripsikan metode pengumpulan dan klasifikasi data risiko. Dengan demikian, aktivitas ini berjalan secara substansial namun belum terdokumentasi formal. Komponen COBIT 2019 yang terpenuhi: <i>Policies, Principles & Frameworks</i>: belum ada dokumen SOP resmi; <i>Processes</i>: pengumpulan dan analisis risiko dilakukan melalui form <i>risk register</i>; <i>Information Items</i>: hasil pengumpulan risiko terdokumentasi dalam form risiko prioritas; <i>Organizational Structures</i>: verifikasi dilakukan lintas instansi (dengan BSSN). Aktivitas ini dinilai <i>Largely Achieved</i> (L) karena praktik sudah berjalan dengan bukti nyata, meskipun belum diformalisasi dalam bentuk kebijakan tertulis (SOP).

No	Aktivitas	Nilai	Alasan / Justifikasi
2	Mencatat data risiko I&T yang relevan dan signifikan pada lingkungan operasi internal dan eksternal perusahaan.	L	Diskominfo Klungkung telah melakukan pencatatan data risiko secara internal melalui <i>Risk Register Form 4 dan 9</i>, yang berisi kolom penyebab, dampak, kontrol, serta rencana tindak lanjut sebagai format baku pencatatan risiko. Penanggung jawab risiko juga dicantumkan secara jelas dalam kolom “JF Perencana” dan bidang terkait. Namun, pencatatan data risiko eksternal (seperti regulasi nasional atau tren industri) belum dilakukan secara sistematis. Dengan demikian, proses pencatatan telah terstruktur untuk risiko internal, tetapi belum mencakup risiko eksternal sebagaimana praktik COBIT 2019. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: format baku pencatatan risiko tersedia; <i>Processes</i>: pencatatan risiko dilakukan tiap bidang melalui <i>risk register</i>; <i>Organizational Structures</i>: tanggung jawab penanggung jawab risiko jelas; <i>Information Items</i>: dokumen <i>risk register</i> dan rekap risiko mendukung bukti pencatatan. Aktivitas ini dinilai <i>Largely Achieved</i> (L) karena pencatatan risiko internal sudah formal dan konsisten, tetapi belum mencakup risiko eksternal.
3	Mengadopsi atau menetapkan taksonomi risiko untuk definisi skenario risiko dan	L Level 3 akt 1	Diskominfo Klungkung telah menggunakan kategori risiko dan probabilitas secara konsisten di semua bidang, dengan skala “rendah, sedang, tinggi” sebagaimana

No	Aktivitas	Nilai	Alasan / Justifikasi
	kategori dampak serta kemungkinan yang konsisten.		tercantum dalam <i>Risk Register Lampiran 5 dan 9</i>. Kategori risiko yang dimuat meliputi dampak layanan publik dan reputasi, walaupun belum dituangkan dalam dokumen kebijakan taksonomi formal. Belum ditemukan bukti sosialisasi resmi maupun revisi taksonomi dari tahun sebelumnya, yang menunjukkan penerapan masih berbasis praktik, bukan kebijakan tertulis. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada kebijakan formal tentang taksonomi risiko; <i>Processes</i>: klasifikasi risiko digunakan secara konsisten di seluruh bidang; <i>Information Flows</i>: belum ada sosialisasi resmi; <i>Culture & Behavior</i>: kesadaran pembaruan taksonomi masih rendah. Aktivitas ini dinilai <i>Largely Achieved (L)</i> karena praktik klasifikasi risiko berjalan konsisten, namun tanpa panduan formal dan tanpa revisi periodik.
4	Mencatat data tentang peristiwa risiko yang telah menyebabkan atau mungkin menyebabkan dampak bisnis sesuai kategori dampak yang ditetapkan dalam taksonomi risiko. Menangkap data yang relevan dari isu, insiden, masalah, dan investigasi	L Level 3 akt 2	Diskominfo Klungkung telah mencatat insiden I&T yang berpotensi menimbulkan dampak terhadap layanan publik, meskipun belum seluruhnya dikategorikan secara formal. Bukti dokumentasi “Monitoring Web Terdampak Serangan Cyber Mei 2025” menunjukkan pencatatan detail waktu kejadian, jenis serangan, dan dampak layanan, walaupun belum mengikuti klasifikasi risiko yang baku.

No	Aktivitas	Nilai	Alasan / Justifikasi
	terkait.		Pencatatan dilakukan oleh staf bidang persandian, sebagaimana tertulis dalam “<i>Risk Register Form 9 Risiko Perencana.pdf</i>”, yang menetapkan JF Perencana sebagai penanggung jawab risiko. Hasil catatan insiden juga digunakan sebagai dasar perbaikan layanan, dibuktikan dengan adanya tindak lanjut dalam “Laporan Telematika”. Namun, integrasi antara laporan insiden dan hasil investigasi masih belum ada secara formal, sehingga pencatatan belum sepenuhnya terstruktur. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada SOP pencatatan insiden; <i>Processes</i>: pencatatan dilakukan tetapi belum selalu klasifikatif; <i>Organizational Structures</i>: penanggung jawab risiko telah ditetapkan (JF Perencana); <i>Information Flows and Items</i>: laporan insiden dan dokumen telematika menjadi bukti aliran informasi; <i>Culture, Ethics & Behavior</i>: staf menunjukkan kesadaran mencatat dan memperbaiki layanan; <i>Services, Infrastructure & Applications</i>: belum ada sistem pencatatan insiden berbasis aplikasi. Aktivitas ini dinilai <i>Largely Achieved</i> (L) karena aktivitas berjalan dan didukung bukti nyata, tetapi belum terdokumentasi dalam SOP formal.
5	Melakukan survei dan	L	Analisis risiko I&T dilakukan secara berkala

No	Aktivitas	Nilai	Alasan / Justifikasi
	analisis data risiko I&T historis dan pengalaman kerugian dari data dan tren yang tersedia secara eksternal, rekan industri melalui log peristiwa berbasis industri, basis data, dan perjanjian industri untuk pengungkapan peristiwa umum.	Level 4 akt 1	melalui Laporan Evaluasi Risiko Semester I 2025, yang mencantumkan risiko berulang dan residual dari tahun sebelumnya. Hal ini menunjukkan penggunaan data historis internal dalam evaluasi risiko. Selain itu, organisasi juga memperhatikan tren eksternal melalui laporan BSSN, meskipun belum ada perbandingan kuantitatif dengan kondisi internal. Tidak ditemukan bukti laporan perbaikan kebijakan berbasis hasil benchmarking eksternal, namun terdapat indikasi kesadaran untuk belajar dari tren nasional. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: tidak ada kebijakan eksplisit tentang analisis tren historis; <i>Processes</i>: proses analisis dilakukan per semester melalui laporan evaluasi; <i>Organizational Structures</i>: analisis dilakukan oleh tim perencana dan Bidang Telematika; <i>Information Flows and Items</i>: laporan BSSN dan laporan evaluasi risiko berfungsi sebagai sumber data; <i>Culture, Ethics & Behavior</i>: terbuka terhadap pembelajaran dari data eksternal; <i>Services, Infrastructure & Applications</i>: belum ada sistem terintegrasi untuk analisis historis. Aktivitas ini dinilai <i>Largely Achieved</i> (L) karena praktik analisis risiko telah dilakukan, namun belum didukung oleh mekanisme yang konsisten, dokumentasi formal, dan

No	Aktivitas	Nilai	Alasan / Justifikasi
			proses pembandingan eksternal yang terstruktur.
6	Untuk kelas kejadian yang serupa, menyusun data yang terkumpul dan soroti faktor-faktor yang berkontribusi. Tentukan faktor-faktor yang berkontribusi secara umum pada beberapa kejadian.	P Level 4 akt 2	Diskominfo Klungkung belum memiliki klasifikasi formal atas insiden yang serupa, namun laporan evaluasi risiko mencatat penyebab umum seperti keterbatasan SDM dan konfigurasi keamanan yang belum memadai. Data ini digunakan dalam <i>Risk Register</i> untuk menentukan rencana tindak lanjut pencegahan insiden berulang. Meskipun tidak ada dokumen khusus pengelompokan insiden, catatan faktor penyebab menunjukkan adanya kesadaran untuk mengidentifikasi akar masalah. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada kebijakan klasifikasi insiden berulang; <i>Processes</i>: analisis penyebab dilakukan secara sederhana melalui evaluasi semester; <i>Organizational Structures</i>: dilakukan oleh Bidang Telematika dan JF Perencana; <i>Information Flows and Items</i>: laporan evaluasi risiko dan <i>risk register</i> menjadi dasar; <i>Culture, Ethics & Behavior</i>: ada kesadaran mencegah kejadian berulang; <i>Services, Infrastructure & Applications</i>: belum ada alat bantu analisis insiden otomatis. Aktivitas ini dinilai <i>Partially Achieved</i> (P) karena aktivitas dilakukan sebagian, tanpa sistem klasifikasi dan kebijakan formal.
7	Menentukan kondisi	P	Kondisi operasional seperti lonjakan trafik

No	Aktivitas	Nilai	Alasan / Justifikasi
	spesifik yang ada atau tidak ada saat peristiwa risiko terjadi dan cara kondisi tersebut memengaruhi frekuensi peristiwa dan besarnya kerugian.	Level 4 akt 3	web dan peningkatan serangan telah dicatat dalam “Laporan Monitoring Web Terdampak Serangan Cyber Mei 2025”. Hal ini menunjukkan pencatatan faktor penyebab langsung. Namun, pencatatan belum dilakukan secara konsisten untuk setiap insiden, dan analisis pengaruh kondisi terhadap kerugian belum terdokumentasi. Tidak ada analisis akar penyebab formal berbasis kondisi lingkungan. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada pedoman pencatatan kondisi insiden; <i>Processes</i>: pencatatan dilakukan tetapi tidak konsisten; <i>Organizational Structures</i>: dilakukan oleh tim keamanan dan bidang persandian; <i>Information Flows and Items</i>: laporan serangan cyber menjadi bukti utama; <i>Culture, Ethics & Behavior</i>: staf tanggap terhadap insiden, meski analisis belum sistematis; <i>Services, Infrastructure & Applications</i>: belum ada sistem pelaporan insiden otomatis. Aktivitas ini dinilai <i>Partially Achieved</i> (P) karena praktik pencatatan sudah berjalan namun belum konsisten dan tanpa analisis lanjutan.
8	Melakukan analisis kejadian dan faktor risiko secara berkala untuk mengidentifikasi masalah	L Level 4 akt 4	Analisis risiko dilakukan setiap semester sesuai Laporan Evaluasi Risiko Semester I 2025, yang disahkan oleh Kepala Dinas. Pelaksana analisis terdiri dari JF Perencana

No	Aktivitas	Nilai	Alasan / Justifikasi
	risiko baru atau yang muncul dan untuk memperoleh pemahaman tentang faktor risiko internal dan eksternal terkait.		dan tim Bidang Telematika, sebagaimana tercantum dalam <i>Risk Register</i> Form 9. Hasil analisis digunakan untuk memperbarui daftar risiko organisasi, terbukti dengan revisi status mitigasi dan risiko baru dalam <i>Risk Register</i> 2025. Namun, identifikasi risiko baru masih terbatas dan tidak ditemukan laporan khusus tentang risiko emerging. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: kebijakan review per semester tercermin dalam rutinitas laporan; <i>Processes</i>: proses evaluasi dan pembaruan risiko dilakukan rutin; <i>Organizational Structures</i>: pelaksana analisis telah ditetapkan formal; <i>Information Flows and Items</i>: laporan evaluasi dan <i>risk register</i> menjadi bukti pembaruan; <i>Culture, Ethics & Behavior</i>: pimpinan mendukung pembaruan risiko secara periodik; <i>Services, Infrastructure & Applications</i>: masih manual, belum ada sistem berbasis aplikasi. Aktivitas ini dinilai <i>Largely Achieved</i> (L) karena aktivitas rutin berjalan baik meski belum ada mekanisme deteksi risiko baru yang eksplisit.
9	Menentukan cakupan upaya analisis risiko yang tepat, dengan mempertimbangkan semua faktor risiko dan/atau kekritisitas aset	P Level 3 akt 3	Lingkup analisis risiko difokuskan pada layanan prioritas seperti Tanda Tangan Elektronik (TTE) dan web Diskominfo, sebagaimana tercantum dalam <i>Risk Register</i> 2025. Keputusan ruang lingkup dilakukan di

No	Aktivitas	Nilai	Alasan / Justifikasi
	dalam bisnis.		tingkat Kepala Bidang dan JF Perencana, meski belum ada kriteria formal yang menetapkan aset kritis. Penentuan masih berdasarkan pengalaman dan urgensi layanan, serta belum ada dokumen eksplisit mengenai kriteria klasifikasi aset kritis. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada pedoman formal untuk klasifikasi aset kritis; <i>Processes</i>: penetapan lingkup dilakukan secara praktis berdasarkan kebutuhan; <i>Organizational Structures</i>: kewenangan ada di Kepala Bidang dan JF Perencana; <i>Information Flows and Items</i>: <i>Risk Register</i> mendokumentasikan ruang lingkup analisis; <i>Culture, Ethics & Behavior</i>: pengambil keputusan sadar prioritas layanan utama; <i>Services, Infrastructure & Applications</i>: belum ada sistem untuk pemetaan aset otomatis. Aktivitas ini dinilai <i>Partially Achieved</i> (P) karena analisis dilakukan namun belum berbasis kebijakan atau kriteria formal.
10	Menyusun dan memperbarui skenario risiko I&T secara berkala; paparan kerugian terkait I&T; dan skenario terkait risiko reputasi, termasuk skenario gabungan dari jenis dan peristiwa ancaman yang berjenjang	P Level 3 akt 4	Diskominfo Klungkung telah menyusun dan memperbarui skenario risiko I&T secara terbatas melalui <i>Risk Register</i> 2025 TTE dan Form 4 Risiko Prioritas, yang berisi uraian kejadian risiko, penyebab, serta nilai kemungkinan dan dampak. Secara substansi, formulir tersebut sudah mencerminkan keberadaan skenario risiko.

No	Aktivitas	Nilai	Alasan / Justifikasi
	dan/atau bersamaan. Mengembangkan ekspektasi untuk aktivitas dan kemampuan kontrol tertentu untuk mendeteksi.		Selain itu, Laporan Evaluasi Risiko Semester I 2025 menunjukkan bahwa pembaruan dilakukan setiap semester, sehingga terdapat praktik berkala dalam meninjau skenario risiko yang telah ditetapkan. Namun, belum terdapat dokumen formal khusus yang berjudul “Risk Scenario Register” ataupun pedoman yang menjelaskan metode penyusunan skenario risiko. Skenario gabungan (<i>multi-event</i>), seperti kombinasi serangan siber dan gangguan jaringan, juga belum disusun. Analisis terhadap dampak reputasi dilakukan secara umum tanpa menggunakan metode kuantitatif atau panduan tertentu. Keterlibatan pimpinan dalam validasi masih bersifat administratif (penandatanganan laporan), belum berupa proses <i>review</i> substansial terhadap isi skenario risiko. Meskipun demikian, keterlibatan Bidang Telematika dan pejabat perencanaan (JF Perencana) menunjukkan adanya struktur tanggung jawab yang berjalan. Komponen COBIT 2019 yang terpenuhi: <i>Policies, Principles & Frameworks</i>: belum terdapat panduan formal penyusunan skenario risiko; <i>Processes</i>: pembaruan skenario dilakukan secara berkala melalui <i>Risk Register</i> dan laporan evaluasi semesteran, namun belum mencakup skenario gabungan; <i>Organizational Structures</i>: Bidang

No	Aktivitas	Nilai	Alasan / Justifikasi
			Telematika dan JF Perencana terlibat aktif dalam pengisian dan pembaruan register; <i>Information Items</i>: dokumen <i>Risk Register</i> dan Laporan Evaluasi Risiko menjadi bukti aktivitas pembaruan; <i>Information Flows</i>: alur komunikasi hasil evaluasi melalui laporan resmi kepada pimpinan; <i>Culture & Behavior</i>: kesadaran terhadap pentingnya pembaruan risiko sudah ada, namun belum didukung kebiasaan dokumentasi formal dan analisis mendalam. Secara keseluruhan, aktivitas penyusunan dan pembaruan skenario risiko I&T telah dilakukan namun belum lengkap dan belum diformalkan dalam pedoman khusus. Karena pelaksanaan sudah substansial tapi belum sepenuhnya memenuhi deskripsi COBIT 2019, maka aktivitas ini dinilai <i>Partially Achieved</i> (P).
11	Memperkirakan frekuensi (atau kemungkinan) dan besarnya kerugian atau keuntungan yang terkait dengan skenario risiko I&T. Mempertimbangkan semua faktor risiko yang berlaku dan mengevaluasi pengendalian operasional yang diketahui.	N Level 3 akt 5	Diskominfo Klungkung belum memiliki metode formal untuk memperkirakan frekuensi atau probabilitas terjadinya risiko I&T maupun besarnya potensi kerugian yang mungkin timbul. Selama ini, penilaian risiko dilakukan secara kualitatif melalui <i>Risk Register</i> tanpa perhitungan frekuensi kejadian atau estimasi nilai kerugian finansial. faktor eksternal seperti regulasi nasional, ancaman siber, dan perkembangan lingkungan I&T belum dipertimbangkan

No	Aktivitas	Nilai	Alasan / Justifikasi
			secara sistematis dalam proses analisis risiko. Selain itu, pengendalian yang ada belum pernah dievaluasi untuk menilai sejauh mana pengendalian tersebut mampu menurunkan dampak atau probabilitas risiko. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada pedoman atau metode kuantitatif untuk estimasi risiko; <i>Processes</i>: tidak ada proses formal memperkirakan frekuensi atau besaran dampak; <i>Organizational Structures</i>: belum ditetapkan peran analisis kuantitatif risiko; <i>Information Flows and Items</i>: tidak ditemukan laporan atau perhitungan risiko berbasis data historis; <i>Culture, Ethics & Behavior</i>: belum terbentuk kebiasaan analisis risiko berbasis data; <i>Services, Infrastructure & Applications</i>: tidak tersedia alat bantu analisis risiko. Aktivitas ini dinilai <i>Not Achieved</i> (N) karena organisasi belum memiliki mekanisme formal untuk melakukan estimasi probabilitas dan dampak risiko secara terstruktur, serta belum didukung oleh metode analisis risiko yang terdokumentasi.
12	Membandingkan risiko saat ini (paparan kerugian terkait I&T) dengan selera risiko dan toleransi risiko yang dapat diterima. Mengidentifikasi risiko yang tidak dapat diterima	N Level 3 akt 6	Diskominfo Klungkung belum pernah melakukan perbandingan antara profil risiko I&T yang berjalan dengan selera risiko (<i>risk appetite</i>) atau batas toleransi risiko (<i>risk tolerance</i>). Tidak ada laporan resmi yang menyatakan apakah suatu risiko sudah melebihi batas yang dapat diterima.

No	Aktivitas	Nilai	Alasan / Justifikasi
	atau tinggi.		Meskipun Laporan Evaluasi Risiko Semester I 2025 memuat kolom persetujuan pimpinan, proses tersebut belum mencakup analisis formal terhadap ambang batas risiko. Tidak ditemukan format pelaporan atau pedoman khusus untuk menyampaikan risiko yang berada di luar toleransi. Pimpinan belum memiliki mekanisme tindak lanjut khusus terhadap risiko yang dianggap terlalu tinggi. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada pedoman formal untuk perbandingan profil risiko terhadap toleransi; <i>Processes</i>: tidak ada proses penilaian sistematis terhadap risiko yang melampaui batas; <i>Organizational Structures</i>: pimpinan menandatangani hasil evaluasi, namun tanpa mekanisme eskalasi; <i>Information Flows and Items</i>: laporan evaluasi belum memuat hasil analisis terhadap toleransi risiko; <i>Culture, Ethics & Behavior</i>: pimpinan belum menindaklanjuti risiko berlebih secara formal; <i>Services, Infrastructure & Applications</i>: belum ada sistem pemantauan risiko otomatis. Aktivitas ini dinilai <i>Not Achieved</i> (N) karena proses perbandingan risiko terhadap toleransi belum pernah dilakukan secara formal maupun terdokumentasi.
13	Mengusulkan respons risiko untuk risiko yang melampaui selera risiko	P Level 3 akt	Organisasi telah memiliki langkah mitigasi risiko yang dicantumkan dalam kolom “Kegiatan Pengendalian yang Dibutuhkan”

No	Aktivitas	Nilai	Alasan / Justifikasi
	dan tingkat toleransi.	7	pada <i>Risk Register</i> Form 9, namun belum ada proses formal untuk menentukan opsi respons (menghindari, mengurangi, mentransfer, atau menerima). Sebagian besar risiko dijawab dengan pendekatan penerimaan (acceptance). Tim CSIRT atau TTIS disebut sebagai pelaksana tanggung jawab mitigasi sesuai SK TTIS, sementara keputusan akhir berada di Kepala Dinas. Namun, belum ada dokumen yang secara eksplisit berfungsi sebagai proposal atau catatan usulan respons risiko. Tidak ditemukan pula pedoman yang mengarahkan kesesuaian tindakan dengan kebijakan organisasi. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada kebijakan formal tentang perencanaan respons risiko; <i>Processes</i>: mitigasi risiko tercatat di <i>Risk Register</i> tanpa mekanisme pemilihan opsi; <i>Organizational Structures</i>: TTIS dan pimpinan terlibat dalam persetujuan respons risiko; <i>Information Flows and Items</i>: laporan evaluasi risiko menjadi media dokumentasi tidak langsung; <i>Culture, Ethics & Behavior</i>: pimpinan menunjukkan kesadaran mitigasi meski belum sistematis; <i>Services, Infrastructure & Applications</i>: tidak ada sistem pendukung perencanaan mitigasi. Aktivitas ini dinilai <i>Partially Achieved</i> (P)

No	Aktivitas	Nilai	Alasan / Justifikasi
			karena respons risiko dilakukan secara substansi melalui <i>Risk Register</i> , namun tanpa panduan, dokumen, dan mekanisme penetapan opsi formal.
14	Menetapkan persyaratan tingkat tinggi untuk proyek atau program yang akan menerapkan respons risiko yang dipilih. Identifikasi persyaratan dan harapan untuk kontrol utama yang sesuai untuk respons mitigasi risiko.	L Level 3 akt 8	Diskominfo Klungkung telah membuat program mitigasi risiko yang diimplementasikan dalam kegiatan “Kiwa Tengen”, hasil usulan Kepala Dinas yang tertuang dalam Ringkasan Eksekutif dan didukung dokumen “Telaah Staf Kiwa Tengen”. Dokumen tersebut menjelaskan kebutuhan kontrol utama dan arah mitigasi risiko I&T. Persetujuan terhadap persyaratan mitigasi dilakukan oleh pimpinan, namun belum ditemukan notulen rapat atau dokumen komunikasi yang menjelaskan detail penyampaian ke tim pelaksana. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i> : belum ada kebijakan standar terkait perumusan requirement mitigasi risiko; <i>Processes</i> : penetapan <i>requirement</i> dilakukan melalui kegiatan operasional (Kiwa Tengen); <i>Organizational Structures</i> : persetujuan dilakukan langsung oleh Kepala Dinas; <i>Information Flows and Items</i> : dokumen telaah staf berfungsi sebagai media komunikasi internal; <i>Culture, Ethics & Behavior</i> : pimpinan berinisiatif langsung menetapkan arah mitigasi; <i>Services, Infrastructure & Applications</i> : tidak ditemukan sistem manajemen proyek formal.

No	Aktivitas	Nilai	Alasan / Justifikasi
			Aktivitas ini dinilai <i>Largely Achieved</i> (L) karena requirement mitigasi risiko sudah diterapkan melalui praktik nyata dan dokumen teknis, namun masih terbatas tanpa prosedur standar.
15	Memvalidasi hasil analisis risiko dan analisis dampak bisnis (BIA) sebelum menggunakannya dalam pengambilan keputusan. Pastikan analisis tersebut sesuai dengan persyaratan perusahaan dan verifikasi bahwa estimasi telah dikalibrasi dengan benar dan diteliti untuk mengetahui biasnya.	N Level 4 akt 5	Organisasi belum pernah melakukan validasi formal terhadap hasil analisis risiko atau analisis dampak bisnis (BIA) sebelum digunakan dalam pengambilan keputusan. Tidak ditemukan dokumen yang menunjukkan adanya proses pemeriksaan ulang, pembuktian silang, atau audit independen terhadap hasil analisis risiko. Validasi yang ada bersifat administratif, hanya berupa tanda tangan pimpinan tanpa proses teknis untuk menguji keakuratan data atau bias analisis. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada prinsip validasi analisis risiko yang objektif; <i>Processes</i>: tidak ada proses verifikasi atau kalibrasi analisis risiko; <i>Organizational Structures</i>: belum ditunjuk pihak independen untuk validasi; <i>Information Flows and Items</i>: tidak ada laporan validasi atau notulen verifikasi; <i>Culture, Ethics & Behavior</i>: kesadaran akan pentingnya validasi formal masih rendah; <i>Services, Infrastructure & Applications</i>: tidak tersedia sistem pendukung validasi data risiko. Aktivitas ini dinilai <i>Not Achieved</i> (N) karena tidak ada kegiatan validasi atau dokumentasi

No	Aktivitas	Nilai	Alasan / Justifikasi
			yang membuktikan proses peninjauan ulang hasil analisis risiko.
16	Menganalisis biaya/manfaat dari opsi respons risiko potensial seperti menghindari, mengurangi/meringankan, mentransfer/membagi, dan menerima serta memanfaatkan/merebut. Mengonfirmasikan respons risiko yang sesuai.	N Level 5 akt 1	Diskominfo Klungkung belum memiliki prosedur formal untuk melakukan analisis biaya dan manfaat dari berbagai opsi respons risiko. Tidak ada bukti perbandingan biaya (<i>cost</i>) dengan manfaat (<i>benefit</i>) atas tindakan mitigasi seperti pengurangan <i>downtime</i> , peningkatan keamanan, atau peningkatan kepercayaan publik. Tidak ditemukan penggunaan indikator keuangan seperti ROI atau payback period. Keputusan mengenai opsi respons risiko dilakukan oleh Kepala Dinas berdasarkan pertimbangan praktis, bukan analisis cost-benefit formal. Namun, budaya organisasi menunjukkan kecenderungan berhati-hati dalam mengambil risiko, sebagaimana tercermin dalam Laporan Evaluasi Risiko Semester I 2025 yang menggambarkan pendekatan konservatif dalam merespons ancaman TI. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i> : tidak ada pedoman analisis biaya-manfaat risiko; <i>Processes</i> : tidak dilakukan evaluasi cost-benefit secara formal; <i>Organizational Structures</i> : keputusan respons risiko berada di Kepala Dinas; <i>Information Flows and Items</i> : laporan evaluasi risiko menjadi satu-satunya dokumen pendukung; <i>Culture, Ethics & Behavior</i> : organisasi bersikap hati-hati (risk-

No	Aktivitas	Nilai	Alasan / Justifikasi
			averse); <i>Services, Infrastructure & Applications</i>: tidak ada sistem analisis keuangan risiko. Aktivitas ini dinilai <i>Not Achieved</i> (N) karena tidak ada proses atau dokumen yang menunjukkan pelaksanaan analisis biaya-manfaat risiko secara formal.
17	Menginventarisasi proses bisnis dan dokumentasikan ketergantungannya pada proses manajemen layanan I&T dan sumber daya infrastruktur I&T. Mengidentifikasi personel pendukung, aplikasi, infrastruktur, fasilitas, catatan manual penting, vendor, pemasok, dan pihak yang melakukan alih daya.	P Level 1 akt 3	Diskominfo Klungkung belum memiliki inventaris proses bisnis yang terdokumentasi secara menyeluruh. Hasil FGD menunjukkan bahwa pemetaan hubungan antara proses bisnis dan ketergantungan terhadap sistem I&T belum dilakukan. Namun, pada hasil studi dokumentasi ditemukan bukti berupa catatan infrastruktur dan aset TI yang memuat rincian perangkat dan sumber daya yang digunakan oleh tiap bidang. Masing-masing bidang memiliki daftar aset sendiri, namun belum dikonsolidasikan menjadi inventaris bisnis-TI terintegrasi. Penanggung jawab pemeliharaan data inventaris berada pada setiap bidang sesuai fungsi kerja masing-masing. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada aturan atau pedoman formal tentang inventaris proses bisnis dan ketergantungan I&T; <i>Processes</i>: pencatatan hanya dilakukan sebatas daftar aset tanpa analisis dependensi proses bisnis; <i>Organizational Structures</i>: tanggung jawab inventaris dibagi ke tiap bidang tanpa

No	Aktivitas	Nilai	Alasan / Justifikasi
			koordinasi lintas unit; <i>Information Flows & Items</i>: terdapat bukti catatan infrastruktur valid sebagai dokumen parsial inventaris; <i>Culture & Behavior</i>: kesadaran pentingnya inventaris sudah ada namun belum sistematis; <i>Services & Infrastructure</i>: data aset dikelola manual tanpa sistem inventarisasi terpusat. Aktivitas ini dinilai <i>Partially Achieved</i> (P) karena sudah ada catatan infrastruktur yang valid, namun belum mencakup proses bisnis dan hubungan dependensi layanan I&T.
18	Menentukan dan menyetujui layanan I&T dan sumber daya infrastruktur I&T mana yang penting untuk mempertahankan operasi proses bisnis. Menganalisis ketergantungan dan mengidentifikasi titik lemah.	N Level 1 akt 4	Organisasi belum memiliki metode maupun dokumen resmi yang menetapkan layanan dan infrastruktur I&T mana yang dianggap paling kritis bagi kelangsungan operasi publik. Tidak ditemukan daftar formal layanan penting, <i>Business Continuity Plan</i> (BCP), atau analisis ketergantungan sistem. Pimpinan dan bidang I&T belum pernah melakukan penilaian terhadap titik lemah (single point of failure) dari layanan digital. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada kebijakan formal penetapan layanan kritis; <i>Processes</i>: tidak ada proses identifikasi atau analisis dependensi; <i>Organizational Structures</i>: belum ada unit khusus yang bertugas menilai layanan penting; <i>Information Flows & Items</i>: tidak ditemukan laporan atau daftar layanan esensial; <i>Culture & Behavior</i>: kesadaran

No	Aktivitas	Nilai	Alasan / Justifikasi
			terhadap pentingnya layanan kritis masih rendah; <i>Services & Infrastructure</i>: tidak ada sistem BCP/DRP untuk menjaga layanan kritis. Aktivitas ini dinilai <i>Not Achieved</i> (N) karena tidak ada bukti penetapan, dokumentasi, atau analisis layanan I&T esensial.
19	Mengumpulkan skenario risiko saat ini berdasarkan kategori, lini bisnis, dan area fungsional.	L Level 1 akt 5	Diskominfo telah memiliki skenario risiko I&T yang secara sederhana dikategorikan dalam <i>Risk Register</i> 2025, terutama di bidang operasional layanan TTE. Meskipun taksonomi risiko belum formal, klasifikasi “operasional” sudah digunakan secara konsisten antarbidang. Dokumen <i>Risk Register</i> juga menunjukkan penggabungan risiko lintas fungsi (Telematika, Komunikasi, Statistik dan Persandian), yang disahkan oleh Kepala Dinas. Namun, belum ada laporan konsolidasi terpisah atau analisis mendalam per kategori. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada pedoman formal tentang kategorisasi risiko; <i>Processes</i>: pengelompokan risiko dilakukan sederhana melalui form register; <i>Organizational Structures</i>: agregasi disahkan pimpinan namun tanpa komite khusus; <i>Information Flows & Items</i>: laporan evaluasi risiko semesteran mencakup data lintas bidang; <i>Culture & Behavior</i>: staf mengikuti pola pencatatan seragam walau tanpa panduan

No	Aktivitas	Nilai	Alasan / Justifikasi
			tertulis; <i>Services & Infrastructure</i> : pengelolaan data risiko masih manual (Excel). Aktivitas ini dinilai <i>Largely Achieved</i> (L) karena pengelompokan dan konsolidasi lintas fungsi sudah berjalan dengan konsisten walau belum terdokumentasi formal.
20	Secara berkala menangkap semua informasi profil risiko dan menggabungkannya menjadi profil risiko agregat.	N Level 3 akt 9	Diskominfo belum memiliki proses formal atau sistem yang digunakan untuk menyatukan seluruh data risiko menjadi profil risiko agregat organisasi. Tidak ada aplikasi atau mekanisme khusus untuk konsolidasi, dan hasil monitoring tidak disusun dalam bentuk profil terkini yang memperlihatkan tren risiko. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i> : tidak ada pedoman pembentukan profil risiko agregat; <i>Processes</i> : tidak dilakukan konsolidasi risiko lintas unit secara periodik; <i>Organizational Structures</i> : belum ada peran yang ditunjuk untuk mengelola profil agregat; <i>Information Flows & Items</i> : tidak ada laporan risk profile terintegrasi; <i>Culture & Behavior</i> : kesadaran pelaporan risiko masih sektoral per bidang; <i>Services & Infrastructure</i> : tidak tersedia sistem GRC atau tools konsolidasi risiko. Aktivitas ini dinilai <i>Not Achieved</i> (N) karena profil risiko agregat belum pernah dibuat.
21	Menangkap informasi	N	Organisasi belum memiliki pedoman

No	Aktivitas	Nilai	Alasan / Justifikasi
	tentang status rencana tindakan risiko untuk dimasukkan dalam profil risiko I&T perusahaan.	Level 3 akt 10	penyusunan <i>action plan</i> resmi untuk tiap mitigasi risiko. Status pelaksanaan mitigasi juga belum dipantau atau dilaporkan secara teratur. Tidak ada bukti laporan progres rencana tindakan, dan belum jelas siapa yang bertanggung jawab dalam pelaporannya. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: tidak ada kebijakan penyusunan dan pemantauan rencana aksi risiko; <i>Processes</i>: tidak dilakukan monitoring terhadap pelaksanaan mitigasi; <i>Organizational Structures</i>: belum ditetapkan pemilik risiko secara operasional; <i>Information Flows & Items</i>: tidak ditemukan laporan progres mitigasi; <i>Culture & Behavior</i>: pemantauan dilakukan informal tanpa catatan formal; <i>Services & Infrastructure</i>: tidak ada sistem pelacakan status mitigasi. Aktivitas ini dinilai <i>Not Achieved</i> (N) karena <i>action plan</i> tidak tersedia dan pelaporannya tidak dilakukan.
22	Berdasarkan semua data profil risiko, tentukan serangkaian indikator risiko yang memungkinkan identifikasi dan pemantauan cepat risiko terkini dan tren risiko.	N Level 4 akt 6	Diskominfo Klungkung belum memiliki indikator risiko utama (<i>Key Risk Indicator/KRI</i>) yang digunakan untuk memantau tren risiko I&T. Tidak ditemukan dokumen yang mendefinisikan KRI atau menjelaskan cara penetapannya dari data profil risiko. KRI tidak pernah dibahas dalam rapat pimpinan, dan tidak ada pihak yang menyetujui atau meninjau indikator tersebut.

No	Aktivitas	Nilai	Alasan / Justifikasi
			Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada definisi maupun kebijakan tentang KRI; <i>Processes</i>: tidak ada proses penetapan dan pengukuran indikator risiko; <i>Organizational Structures</i>: belum ada struktur pengelola KRI; <i>Information Flows & Items</i>: laporan risiko I&T tidak mencantumkan indikator numerik; <i>Culture & Behavior</i>: kesadaran terhadap pemantauan kuantitatif risiko belum terbentuk; <i>Services & Infrastructure</i>: tidak ada tools monitoring indikator risiko. Aktivitas ini dinilai <i>Not Achieved</i> (N) karena KRI belum ditetapkan, diukur, maupun digunakan.
23	Menangkap informasi tentang peristiwa risiko I&T yang telah terwujud untuk dimasukkan dalam profil risiko I&T perusahaan.	F Level 4 akt 7	Diskominfo Klungkung telah memiliki catatan formal terkait peristiwa risiko I&T yang terjadi, ditunjukkan oleh Laporan Monitoring Web Terdampak Serangan Cyber Mei 2025. Dokumen tersebut memuat kronologi, jenis serangan, waktu kejadian, dampak terhadap layanan, dan tindakan penanganan yang diambil. Hal ini menunjukkan bahwa organisasi telah menerapkan mekanisme dokumentasi insiden secara sistematis. Pengumpulan data insiden dilakukan secara manual melalui laporan teknis internal yang disusun oleh Bidang Telematika, kemudian dilaporkan kepada Kepala Dinas sebagai bagian dari proses pengawasan formal. Mekanisme ini

No	Aktivitas	Nilai	Alasan / Justifikasi
			menunjukkan adanya alur komunikasi dan pelaporan yang jelas antara unit operasional dan pimpinan. Dari sisi struktur organisasi, Bidang Telematika bertanggung jawab penuh dalam pelaporan insiden, sebagaimana tercermin dari dokumen laporan resmi dan praktik pelaporan langsung ke pimpinan. Proses ini juga menunjukkan adanya pembagian tanggung jawab yang telah berjalan dengan baik, meskipun belum diformalkan dalam SOP. Bukti dari laporan insiden tersebut juga menunjukkan bahwa tindakan korektif dilakukan segera setelah insiden, seperti isolasi server dan perbaikan sistem, menunjukkan bahwa organisasi telah melakukan respons dan tindak lanjut terhadap insiden yang terjadi. Dokumentasi ini menjadi bagian dari sumber data penting bagi pembaruan profil risiko dan evaluasi mitigasi pada periode berikutnya. Komponen COBIT 2019 yang terpenuhi: <i>Policies, Principles & Frameworks</i>: adanya kebijakan implisit terkait pelaporan insiden dan dokumentasi formal serangan siber; <i>Processes</i>: prosedur pencatatan dan pelaporan insiden dilakukan secara konsisten melalui mekanisme manual yang terkoordinasi; <i>Organizational Structures</i>: Bidang Telematika berperan sebagai pelaksana utama dan pelapor kepada pimpinan; <i>Information Items</i>: laporan insiden formal berisi rincian

No	Aktivitas	Nilai	Alasan / Justifikasi
			kejadian, dampak, dan tindakan korektif; <i>Information Flows</i>: alur pelaporan berjalan dari staf teknis ke Kepala Dinas sebagai pengambil Keputusan; <i>Culture & Behavior</i>: staf menunjukkan kesiapsiagaan dan tanggung jawab dalam mendokumentasikan serta menindaklanjuti insiden. Seluruh unsur pelaksanaan aktivitas ini telah terpenuhi dan selaras dengan prinsip COBIT 2019 untuk proses manajemen insiden dan pelaporan risiko. Oleh karena itu, aktivitas ini dinilai <i>Fully Achieved</i> (F).
24	Melaporkan hasil analisis risiko kepada semua pemangku kepentingan yang terpengaruh dalam bentuk dan format yang berguna untuk mendukung keputusan perusahaan. Jika memungkinkan, sertakan probabilitas dan rentang kerugian atau keuntungan beserta tingkat keyakinan, untuk memungkinkan manajemen menyeimbangkan risiko-imbal hasil.	F Level 3 akt 11	Diskominfo Klungkung telah melaporkan hasil analisis risiko kepada pemangku kepentingan internal melalui Laporan Evaluasi Risiko Semester I 2025. Laporan tersebut berisi tingkat risiko, rencana mitigasi, dan status pengendalian, serta ditandatangani oleh Kepala Dinas. Kolom “Kemungkinan” dan “Dampak” pada <i>Risk Register</i> Form 9 berfungsi menggambarkan probabilitas dan tingkat kerugian, meski tidak dalam bentuk kuantitatif. Laporan disusun oleh bidang terkait dan diverifikasi oleh pimpinan sebelum distribusi. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada kebijakan baku format pelaporan risiko; <i>Processes</i>: penyampaian laporan dilakukan rutin setiap semester; <i>Organizational Structures</i>: bidang penyusun

No	Aktivitas	Nilai	Alasan / Justifikasi
			dan pimpinan sebagai pihak verifikator; <i>Information Flows & Items</i>: laporan evaluasi risiko dan <i>risk register</i> sebagai media komunikasi formal; <i>Culture & Behavior</i>: terdapat praktik pelaporan risiko yang dilakukan secara berkala kepada pihak terkait; <i>Services & Infrastructure</i>: belum ada dashboard atau sistem pelaporan digital. Aktivitas ini dinilai <i>Fully Achieved</i> (F) karena seluruh komponen pelaporan risiko telah terpenuhi dan selaras dengan praktik pengelolaan risiko berdasarkan COBIT 2019.
25	Memberikan para pengambil keputusan pemahaman tentang skenario terburuk dan paling mungkin, paparan kerugian terkait I&T, serta reputasi signifikan, pertimbangan hukum dan peraturan, atau kategori dampak lainnya sesuai taksonomi risiko.	L Level 3 akt 12	Pimpinan memperoleh pemahaman tentang skenario risiko melalui Laporan Evaluasi Risiko Semester I 2025, yang menyoroti risiko I&Tngkat “Tinggi” sebagai skenario terburuk yang harus segera dimitigasi. Aspek regulasi dan reputasi dicantumkan dalam kategori dampak, walaupun tidak dijabarkan secara rinci. Komunikasi antara bidang teknis dan non-teknis dilakukan secara kolaboratif untuk memastikan pimpinan memahami risiko dalam bahasa operasional, bukan hanya teknis. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: pelaporan risiko sudah menyebut regulasi, namun belum mengatur skenario detail; <i>Processes</i>: briefing risiko dilakukan melalui laporan evaluasi rutin; <i>Organizational Structures</i>: pimpinan sebagai

No	Aktivitas	Nilai	Alasan / Justifikasi
			penerima dan penilai utama risiko; <i>Information Flows & Items</i>: laporan risiko semesteran berfungsi sebagai media komunikasi utama; <i>Culture & Behavior</i>: terdapat budaya kolaboratif antara teknis dan manajerial; <i>Services & Infrastructure</i>: penyampaian dilakukan manual melalui dokumen. Aktivitas ini dinilai <i>Largely Achieved</i> (L) karena briefing risiko sudah rutin dan dipahami pimpinan, namun belum dilengkapi analisis formal skenario terburuk dan terbaik.
26	Melaporkan profil risiko terkini kepada semua pemangku kepentingan. Sertakan informasi tentang efektivitas proses manajemen risiko, efektivitas pengendalian, kesenjangan, inkonsistensi, redundansi, status perbaikan, dan dampaknya terhadap profil risiko.	N Level 3 akt 13	Diskominfo Klungkung belum memiliki mekanisme pelaporan profil risiko terkini yang dilakukan secara rutin kepada seluruh pemangku kepentingan. Tidak ditemukan bukti laporan yang mencakup informasi efektivitas kontrol, kesenjangan, status remediasi, atau dampak terhadap profil risiko secara menyeluruh. Profil risiko saat ini hanya tersirat melalui Laporan Evaluasi Risiko Semester I 2025, tanpa pembaruan formal dalam bentuk laporan agregat risiko. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada pedoman formal tentang pelaporan profil risiko terkini; <i>Processes</i>: belum ada siklus pelaporan profil risiko yang rutin; <i>Organizational Structures</i>: belum ada pihak resmi yang ditunjuk sebagai penanggung jawab pelaporan profil risiko; <i>Information Items</i>: tidak ditemukan dokumen

No	Aktivitas	Nilai	Alasan / Justifikasi
			profil risiko lengkap yang memuat efektivitas kontrol dan kesenjangan; <i>Information Flows</i>: distribusi laporan risiko terbatas ke pimpinan internal; <i>Culture & Behavior</i>: budaya pelaporan risiko masih administratif dan belum analitis. Aktivitas ini dinilai <i>Not Achieved</i> (N) karena pelaporan profil risiko belum dilakukan secara menyeluruh dan tidak melibatkan seluruh stakeholder.
27	Secara berkala, untuk area dengan risiko relatif dan paritas kapasitas risiko, mengidentifikasi peluang terkait I&T yang akan memungkinkan penerimaan risiko lebih besar dan peningkatan pertumbuhan dan laba.	P Level 3 akt 14	Meskipun organisasi belum secara formal menjalankan analisis peluang risiko, Laporan Evaluasi Renja TW II 2025 menunjukkan bahwa pengembangan inovasi aplikasi pelayanan digital diidentifikasi sebagai peluang yang muncul dari kondisi risiko rendah. Evaluasi peluang dilakukan secara kualitatif, mempertimbangkan kemampuan sumber daya dan risiko teknis. Hasil Survei Kepuasan Masyarakat (SKM) juga menunjukkan peningkatan layanan digital, mencerminkan pemanfaatan peluang dari kondisi risiko terkendali. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada pedoman formal evaluasi peluang I&T berbasis risiko; <i>Processes</i>: analisis peluang dilakukan tidak terstruktur namun mulai diterapkan melalui Renja; <i>Organizational Structures</i>: penilaian peluang dilakukan oleh pimpinan dan bidang perencanaan; <i>Information Items</i>: laporan Renja

No	Aktivitas	Nilai	Alasan / Justifikasi
			dan SKM menjadi bukti implementasi peluang digital; <i>Information Flows</i>: hasil analisis peluang disampaikan melalui forum OPD dan laporan Renja; <i>Culture & Behavior</i>: pimpinan mulai proaktif melihat risiko rendah sebagai peluang inovasi. Aktivitas ini dinilai <i>Partially Achieved</i> (P) karena peluang I&T telah dimanfaatkan meski belum ada prosedur formal untuk mengelolanya.
28	Meninjau hasil penilaian pihak ketiga yang objektif dan tinjauan audit internal serta jaminan kualitas. Sertakan hasil tersebut dalam profil risiko. Tinjau kesenjangan yang teridentifikasi dan paparan kerugian terkait I&T untuk menentukan perlunya analisis risiko tambahan.	N Level 4 akt 8	Tidak ditemukan bukti bahwa hasil audit eksternal, asesmen pihak ketiga, atau audit internal dimasukkan dalam profil risiko. Kesenjangan dari hasil audit belum ditindaklanjuti secara formal dalam <i>Risk Register</i> atau rencana perbaikan risiko. Proses evaluasi risiko masih terbatas pada analisis internal Bidang Telematika. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada kebijakan yang mengatur integrasi hasil audit ke profil risiko; <i>Processes</i>: tidak ada proses tindak lanjut hasil audit pihak ketiga; <i>Organizational Structures</i>: belum ada koordinasi antara auditor internal dan pengelola risiko; <i>Information Items</i>: tidak ditemukan laporan tindak lanjut hasil audit yang dikaitkan dengan risiko I&T; <i>Information Flows</i>: hasil audit tidak disalurkan dalam siklus manajemen risiko; <i>Culture & Behavior</i>: masih mengandalkan

No	Aktivitas	Nilai	Alasan / Justifikasi
			evaluasi internal tanpa validasi eksternal. Aktivitas ini dinilai <i>Not Achieved</i> (N) karena integrasi hasil audit ke manajemen risiko belum dilakukan.
29	Memelihara inventaris aktivitas pengendalian yang ada untuk mengurangi risiko dan yang memungkinkan risiko ditangani sesuai dengan selera dan toleransi risiko. Mengklasifikasikan aktivitas pengendalian dan memetakannya ke skenario risiko I&T tertentu dan agregasi skenario risiko I&T.	N Level 1 akt 6	Diskominfo Klungkung belum memiliki daftar resmi atau katalog aktivitas pengendalian (<i>control inventory</i>) yang dipetakan ke skenario risiko tertentu. Tidak ditemukan dokumen yang mengklasifikasikan kontrol atau menjelaskan siapa yang bertanggung jawab memperbaruinya. Pengendalian masih tercantum per risiko di <i>Risk Register</i> Form 9, namun belum dipetakan atau dikelola secara terpusat. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: tidak ada pedoman penyusunan inventaris kontrol; <i>Processes</i>: pengendalian dimasukkan per risiko tanpa konsolidasi; <i>Organizational Structures</i>: tidak ada penanggung jawab khusus pembaruan kontrol; <i>Information Items</i>: data kontrol tersebar di <i>Risk Register</i>, belum jadi katalog tersendiri; <i>Information Flows</i>: komunikasi kontrol hanya melalui laporan evaluasi risiko; <i>Culture & Behavior</i>: kesadaran dokumentasi kontrol masih rendah. Aktivitas ini dinilai <i>Not Achieved</i> (N) karena belum ada inventaris pengendalian formal dan terintegrasi.
30	Menentukan apakah setiap	N	Belum ada bukti bahwa tiap bidang di

No	Aktivitas	Nilai	Alasan / Justifikasi
	entitas organisasi memantau risiko dan menerima akuntabilitas untuk beroperasi dalam tingkat toleransi individu dan portofolionya.	Level 3 akt 15	Diskominfo Klungkung memiliki tanggung jawab formal untuk memantau risiko dan memastikan operasi dalam batas toleransi masing-masing. Tidak ditemukan laporan risiko per unit atau mekanisme verifikasi kesesuaian toleransi. Pemantauan risiko masih bersifat terpusat di bidang perencanaan atau manajemen risiko. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada kebijakan pembagian akuntabilitas risiko per unit; <i>Processes</i>: tidak ada mekanisme penilaian kinerja risiko unit; <i>Organizational Structures</i>: belum ditetapkan <i>risk owner</i> per bidang secara formal; <i>Information Items</i>: laporan risiko masih bersifat agregat, bukan per unit; <i>Information Flows</i>: pelaporan risiko masih satu arah dari Bidang Telematika ke pimpinan; <i>Culture & Behavior</i>: budaya akuntabilitas risiko belum tumbuh di tingkat bidang. Aktivitas ini dinilai <i>Not Achieved</i> (N) karena akuntabilitas risiko belum diterapkan di seluruh unit organisasi.
31	Menentukan serangkaian proposal proyek yang seimbang yang dirancang untuk mengurangi risiko dan/atau proyek yang memungkinkan peluang perusahaan strategis, dengan mempertimbangkan biaya,	N Level 3 akt 16	Organisasi belum memiliki prosedur formal dalam menilai proyek mitigasi risiko dibanding proyek peluang. Tidak ditemukan pedoman seleksi atau analisis biaya–manfaat proyek. Keputusan proyek lebih didasarkan pada prioritas anggaran dan arahan pimpinan, bukan pertimbangan profil risiko. Komponen COBIT 2019 yang terpenuhi:

No	Aktivitas	Nilai	Alasan / Justifikasi
	manfaat, dampak pada profil risiko dan peraturan saat ini.		<i>Policies</i>: belum ada pedoman seleksi proyek berbasis risiko; <i>Processes</i>: tidak ada proses analisis biaya–manfaat proyek risiko; <i>Organizational Structures</i>: keputusan proyek diambil langsung oleh pimpinan; <i>Information Items</i>: tidak ditemukan dokumen business case atau analisis risiko proyek; <i>Information Flows</i>: pengambilan keputusan proyek tidak berbasis data risiko; <i>Culture & Behavior</i>: pendekatan masih administratif, bukan berbasis risiko strategis. Aktivitas ini dinilai <i>Not Achieved</i> (N) karena proyek mitigasi belum ditentukan melalui analisis risiko dan peluang.
32	Menyiapkan, memelihara, dan menguji rencana yang mendokumentasikan langkah-langkah spesifik yang harus diambil ketika suatu peristiwa risiko dapat menyebabkan insiden operasional atau pengembangan yang signifikan dengan dampak bisnis yang serius. Pastikan bahwa rencana tersebut mencakup jalur eskalasi di seluruh perusahaan.	P Level 3 akt 17	Diskominfo Klungkung belum memiliki dokumen formal BCP atau DRP, namun rencana tanggap risiko diadaptasi dari format <i>Risk Register</i> dan laporan insiden. Penyusunan melibatkan Kepala Bidang, JF Perencana, dan Tim Telematika, namun tidak ada SOP atau mekanisme uji coba formal. Terdapat bukti sistem backup dan server cadangan yang digunakan saat insiden web Mei 2025, menunjukkan kesiapan infrastruktur dasar meski tanpa dokumen formal. Belum ditemukan bukti adanya simulasi atau drill, dan budaya kesiapsiagaan masih bersifat reaktif. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada kebijakan formal penyusunan DRP/BCP; <i>Processes</i>: rencana

No	Aktivitas	Nilai	Alasan / Justifikasi
			tanggap insiden disusun informal tanpa prosedur uji coba; <i>Organizational Structures</i>: tim Telematika dan bidang perencana terlibat dalam penyusunan; <i>Information Items: Risk Register</i> dan laporan insiden sebagai referensi teknis; <i>Culture & Behavior</i>: kesiapsiagaan masih rendah dan belum terbentuk budaya latihan rutin; <i>Services & Infrastructure</i>: terdapat server backup dan sistem cadangan lokal. Aktivitas ini dinilai <i>Partially Achieved</i> (P) karena ada infrastruktur tanggap insiden, tetapi belum ada rencana formal dan uji coba.
33	Menerapkan rencana respons yang tepat untuk meminimalkan dampak saat insiden risiko terjadi.	L Level 3 akt 18	Rencana respons risiko telah diterapkan saat insiden serangan siber Mei 2025, di mana server diisolasi dan sistem diperbaiki secara cepat. Keputusan utama diambil oleh Kepala Dinas, dengan pelaksanaan oleh Bidang Telematika dan tim teknis. Koordinasi dilakukan melalui rapat tanggap darurat internal. Sarana pendukung seperti firewall dan monitoring server digunakan secara aktif, meski belum ada fasilitas ruang kendali. Evaluasi pasca-insiden belum terdokumentasi formal. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada pedoman tertulis pelaksanaan rencana respons; <i>Processes</i>: pelaksanaan dilakukan reaktif berdasarkan pengalaman teknis; <i>Organizational</i>

No	Aktivitas	Nilai	Alasan / Justifikasi
			<i>Structures</i>: Kepala Dinas dan Bidang Telematika berperan sentral dalam keputusan; <i>Information Items</i>: laporan insiden sebagai bukti penerapan tindakan; <i>Culture & Behavior</i>: staf tenang dan kooperatif selama penanganan insiden; <i>Services & Infrastructure</i>: sistem firewall dan monitoring digunakan sebagai dukungan teknis. Aktivitas ini dinilai <i>Largely Achieved</i> (L) karena penerapan rencana respons nyata sudah dilakukan dengan bukti insiden valid, meski belum sistematis.
34	Mengategorikan insiden dan bandingkan paparan kerugian terkait I&T terhadap ambang batas toleransi risiko. Komunikasikan dampak bisnis kepada para pengambil keputusan sebagai bagian dari pelaporan dan perbarui profil risiko.	L Level 4 akt 9	Organisasi belum memiliki SOP formal kategorisasi insiden berdasarkan tingkat keparahan. Namun, Laporan Evaluasi Risiko Semester I 2025 membandingkan insiden terhadap matriks risiko (tinggi, sedang, rendah) yang merepresentasikan toleransi. Validasi tingkat risiko dilakukan oleh Kepala Dinas, dan hasilnya dicatat dalam <i>Risk Register</i>. Dampak bisnis dilaporkan melalui rapat pimpinan dan laporan resmi. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada SOP kategorisasi insiden; <i>Processes</i>: penilaian dilakukan menggunakan matriks risiko sederhana; <i>Organizational Structures</i>: Kepala Dinas berwenang memvalidasi tingkat risiko; <i>Information Items</i>: laporan insiden dan <i>Risk Register</i> menjadi bukti dokumentasi;

No	Aktivitas	Nilai	Alasan / Justifikasi
			<i>Information Flows</i>: komunikasi hasil penilaian dilakukan melalui rapat dan laporan resmi; <i>Culture & Behavior</i>: pimpinan dan staf terbuka membahas insiden besar untuk pembelajaran. Aktivitas ini dinilai <i>Largely Achieved</i> (L) karena proses pembandingan insiden terhadap toleransi risiko sudah dilakukan walau belum formal.
35	Memeriksa kejadian/kerugian buruk di masa lalu dan kesempatan yang hilang, serta menentukan akar penyebabnya.	L Level 4 akt 10	Diskominfo Klungkung memiliki catatan resmi insiden masa lalu, seperti serangan siber Mei 2025. Analisis akar penyebab dilakukan secara deskriptif dengan menyoroti faktor internal seperti kesalahan konfigurasi dan keterbatasan SDM, tanpa metode formal seperti 5-Why. Evaluasi dilakukan oleh Bidang Persandian dan Tim TI secara kolaboratif. Faktor eksternal seperti regulasi BSSN juga dipertimbangkan. Organisasi menunjukkan budaya terbuka dan pembelajaran positif, serta hasil evaluasi digunakan untuk memperkuat kontrol keamanan jaringan. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada SOP formal analisis pasca-insiden; <i>Processes</i>: analisis dilakukan deskriptif, bukan metodologis; <i>Organizational Structures</i>: tim TI, persandian, dan pimpinan terlibat; <i>Information Items</i>: laporan insiden dan evaluasi risiko sebagai bukti; <i>Culture &</i>

No	Aktivitas	Nilai	Alasan / Justifikasi
			<i>Behavior</i>: budaya terbuka mencari solusi, bukan menyalahkan; <i>Information Flows</i>: hasil analisis digunakan dalam laporan risiko berikutnya. Aktivitas ini dinilai <i>Largely Achieved</i> (L) karena analisis akar penyebab sudah dilakukan walau belum memakai metode baku.
36	Mengomunikasikan akar permasalahan, persyaratan respons risiko tambahan, dan perbaikan proses kepada para pengambil keputusan yang tepat. Pastikan bahwa penyebab, persyaratan respons, dan perbaikan proses disertakan dalam proses tata kelola risiko.	P Level 5 akt 2	Diskominfo Klungkung belum secara rutin mengomunikasikan hasil analisis akar penyebab dan rekomendasi perbaikan kepada pimpinan atau pengambil keputusan. Mekanisme komunikasi dilakukan secara informal melalui telaah staf dan laporan evaluasi risiko, namun belum didukung oleh kebijakan formal atau struktur tanggung jawab yang jelas. Meskipun demikian, pimpinan menunjukkan budaya terbuka dan proaktif dalam menerima rekomendasi serta menindaklanjutinya pada pembaruan <i>Risk Register</i>. Komponen COBIT 2019 yang terpenuhi: <i>Policies</i>: belum ada kebijakan formal eskalasi hasil investigasi; <i>Processes</i>: komunikasi hasil analisis dilakukan secara terbatas melalui laporan evaluasi; <i>Organizational Structures</i>: tidak ada penanggung jawab khusus komunikasi perbaikan; <i>Information Items</i>: laporan evaluasi risiko menjadi media penyampaian utama; <i>Culture & Behavior</i>: pimpinan

No	Aktivitas	Nilai	Alasan / Justifikasi
			proaktif dan terbuka terhadap perbaikan; <i>Information Flows</i>: komunikasi belum rutin lintas unit. Aktivitas ini dinilai <i>Partially Achieved</i> (P) karena komunikasi hasil analisis dan tindak lanjut sudah ada namun belum dilakukan secara rutin dan formal sesuai prinsip tata kelola COBIT 2019.



Lampiran 10. Hasil Olah Data COBIT 2019 Capability Level Assessment Tool

Assessment of Capability Level COBIT 2019 Governance and Management Objectives

Process Name: EDM03	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Rating by performed activity	FALSE if Process Capability is Level 1 or Higher	L	L	L	L	N/A
	FALSE	Largely Achieved	Largely Achieved	Largely Achieved	Largely Achieved	N/A
Capability Level Achieved			2 (Managed)			

N - 0%-15%	P - >15%-50%	L - >50%-85%	F - >85%-100%
------------	--------------	--------------	---------------

N – Not Achieved
P – Partially Achieved
L – Largely Achieved
F – Fully Achieved

Rating	Not achieved (0% -15%)	Partially Achieved (>15% -50%)	Largely Achieved (>50% - 85%)	Fully Achieved (>85% -100%)
Score (%)	0	33	67	100
Baseline (%)	7,5	33	68	93

EDM03	Ensured Risk Optimization									
	Purpose	Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.								
Process Capability Level	Assess of how well a process is implemented and performing	Activity	Ordinal Scale (ISO/IEC 33020:2019)				Score	CAPABILITY LEVEL		
			Overall assessment of the process					2		
Level 0	The process lacks basic capability and reflects an incomplete approach to address the governance and management purpose; it may or may not be meeting the intent of any process practices	At this level, there is little or no evidence of any achievement of the process purpose.								
Level 1	The process more or less achieves its purpose through the application of an incomplete set of activities that can be characterized as initial or intuitive—not very organized.	To what extent are the following activities performed? 1. Understand the organization and its context related to I&T risk. 2. Determine the risk appetite of the organization, i.e., the level of I&T-related risk that the enterprise is willing to take in its pursuit of enterprise objectives.	Not achieved (0% -15%)	Partially Achieved (>15% - 50%)	Largely Achieved (>50% - 85%)	Fully Achieved (>85% - 100%)	Score (%)	Average score (%)	Achievement of Capability Level 1	
						X	100			
					X		67			L

	All activities of the process practice are performed but not achieved or partially achieved the process purpose.	3. Determine risk tolerance levels against the risk appetite, i.e., temporarily acceptable deviations from the risk appetite.		X			33	67				L	
		4. Determine the extent of alignment of the I&T risk strategy to the enterprise risk strategy and ensure the risk appetite is below the organization's risk capacity.				X	67						
		5. Direct the translation and integration of the I&T risk strategy into risk management practices and operational activities.					100						
		6. Direct the development of risk communication plans (covering all levels of the enterprise).		X			33						
		7. Direct implementation of the appropriate mechanisms to respond quickly to changing risk and report immediately to appropriate levels of management, supported by agreed principles of escalation (what to report, when, where and how).				X	67						
		8. Direct that risk, opportunities, issues and concerns may be identified and reported by anyone to the appropriate party at any time. Risk should be managed in accordance with published policies and procedures and escalated to the relevant decision makers.		X			33						
		9. Report any risk management issues to the board or executive committee.				X	100						
Level 2	The process achieves its purpose through the application of a basic, yet complete, set of activities that can be characterized as performed.	To what extent are the following activities performed?	Not achieved (0%-15%)	Partially Achieved (>15% - 50%)	Largely Achieved (>50% - 85%)	Fully Achieved (>85% - 100%)	Score (%)	Average score (%)	Achievement of Capability Level 2				L
		1. Understand the organization and its context related to I&T risk.				X	100	67					
		2. Determine the risk appetite of the organization, i.e., the level of I&T-related risk that the enterprise is willing to take in its pursuit of enterprise objectives.				X	67						
	All activities are performed and largely achieved or full achieved the process purpose.	3. Determine risk tolerance levels against the risk appetite, i.e., temporarily acceptable deviations from the risk appetite.		X			33						
		4. Determine the extent of alignment of the I&T risk strategy to the enterprise risk strategy and ensure the risk appetite is below the organization's risk capacity.				X	67						
		5. Direct the translation and integration of the I&T risk strategy into risk management practices and operational activities.				X	100						
		6. Direct the development of risk communication plans (covering all levels of the enterprise).		X			33						
		7. Direct implementation of the appropriate mechanisms to respond quickly to changing risk and report immediately to appropriate levels of management, supported by agreed principles of escalation (what to report, when, where and how).				X	67					L	

[illegible]

Assessment of Capability Level COBIT 2019 Governance and Management Objectives

Process Name: APO12	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Rating by performed activity	FALSE if Process Capability is Level 1 or Higher	P	P	P	P	P
Capability Level Achieved	FALSE	Partially Achieved	Partially Achieved	Partially Achieved	Partially Achieved	Partially Achieved
		1 (Performed)				

N - 0%-15%	P - >15%-50%	L - >50%-85%	F - >85%-100%
------------	--------------	--------------	---------------

N – Not Achieved
P – Partially Achieved
L – Largely Achieved
F – Fully Achieved

Rating	Not achieved (0%-15%)	Partially Achieved (>15%-50%)	Largely Achieved (>50%-85%)	Fully Achieved (>85%-100%)
Score (%)	0	33	67	100
Baseline (%)	7,5	33	68	93

APO12 Managed Risk

	Purpose	Integrate the management of I&T-related enterprise risk with overall enterprise risk management (ERM) and balance the costs and benefits of managing I&T-related enterprise risk.									
Process Capability Level	Assess of how well a process is implemented and performing	Activity	Ordinal Scale (ISO/IEC 33020:2019)				Score	CAPABILITY LEVEL			
			Overall assessment of the process					1			
Level 0	The process lacks basic capability and reflects an incomplete approach to address the governance and management purpose; it may or may not be meeting the intent of any process practices	At this level, there is little or no evidence of any achievement of the process purpose.									
Level 1	The process more or less achieves its purpose through the application of an incomplete set of activities that can be characterized as initial or intuitive—not very organized.	To what extent are the following activities performed?	Not achieved (0%-15%)	Partially Achieved (>15% -	Largely Achieved (>50% -	Fully Achieved (>85% -	Score (%)	Average score (%)	Achievement of Capability Level 1		P
		1. Establish and maintain a method for the collection, classification and analysis of I&T risk-related data.			X		67				
		2. Record relevant and significant I&T risk-related data on the enterprise's internal and external operating environment.			X		67				

	All activities of the process practice are performed but not achieved or partially achieved the process purpose.	3. Inventory business processes and document their dependency on I&T service management processes and IT infrastructure resources. Identify supporting personnel, applications, infrastructure, facilities, critical manual records, vendors, suppliers and outsourcers.		X			33		39	P		
		4. Determine and agree on which I&T services and IT infrastructure resources are essential to sustain the operation of business processes. Analyze dependencies and identify weak links.	X				0					
		5. Aggregate current risk scenarios by category, business line and functional area.			X		67					
		6. Maintain an inventory of control activities that are in place to mitigate risk and that enable risk to be taken in line with the risk appetite and tolerance. Classify control activities and map them to specific I&T risk scenarios and aggregations of I&T risk scenarios.	X				0					
Level 2	The process achieves its purpose through the application of a basic, yet complete, set of activities that can be characterized as performed.	To what extent are the following activities performed?	Not achieved (0%-15%)	Partially Achieved (>15% -	Largely Achieved (>50% -	Fully Achieved (>85%-	Score (%)	Average score (%)	Achievement of Capability Level 2		P	
	All activities are performed and largely achieved or full achieved the process purpose.	1. Establish and maintain a method for the collection, classification and analysis of I&T risk-related data.			X		67					
		2. Record relevant and significant I&T risk-related data on the enterprise's internal and external operating environment.			X		67					
		3. Inventory business processes and document their dependency on I&T service management processes and IT infrastructure resources. Identify supporting personnel, applications, infrastructure, facilities, critical manual records, vendors, suppliers and outsourcers.		X			33		39	P		
		4. Determine and agree on which I&T services and IT infrastructure resources are essential to sustain the operation of business processes. Analyze dependencies and identify weak links.	X				0					
		5. Aggregate current risk scenarios by category, business line and functional area.			X		67					
		6. Maintain an inventory of control activities that are in place to mitigate risk and that enable risk to be taken in line with the risk appetite and tolerance. Classify control activities and map them to specific I&T risk scenarios and aggregations of I&T risk scenarios.	X				0					
Level 3	The process achieves its purpose in a much more organized way using organizational assets. Processes typically are well defined.	To what extent are the following activities performed?	Not achieved (0%-15%)	Partially Achieved (>15% -	Largely Achieved (>50% -	Fully Achieved (>85%-	Score (%)	Average score (%)	Achievement of Capability Level 3		P	
		1. Adopt or define a risk taxonomy for consistent definitions of risk scenarios and impact and likelihood categories.			X		67					

All activities are performed and largely achieved or full achieved the process purpose.	2. Record data on risk events that have caused or may cause business impacts as per the impact categories defined in the risk taxonomy. Capture relevant data from related issues, incidents, problems and investigations.			X		67	33	P
	3. Define the appropriate scope of risk analysis efforts, considering all risk factors and/or the business criticality of assets.		X			33		
	4. Build and regularly update I&T risk scenarios; I&T-related loss exposures; and scenarios regarding reputational risk, including compound scenarios of cascading and/or coincidental threat types and events. Develop expectations for specific control activities and capabilities to detect.		X			33		
	5. Estimate the frequency (or likelihood) and magnitude of loss or gain associated with I&T risk scenarios. Take into account all applicable risk factors and evaluate known operational controls.	X				0		
	6. Compare current risk (I&T-related loss exposure) to risk appetite and acceptable risk tolerance. Identify unacceptable or elevated risk.	X				0		
	7. Propose risk responses for risk exceeding risk		v			33		
	8. Specify high-level requirements for projects or programs that will implement the selected risk responses. Identify requirements and expectations for appropriate key controls for risk mitigation responses.			X		67		
	9. Regularly capture all risk profile information and consolidate it into an aggregated risk profile.	X				0		
	10. Capture information on the status of the risk action plan for inclusion in the I&T risk profile of the enterprise.	X				0		
	11. Report the results of risk analysis to all affected stakeholders in terms and formats useful to support enterprise decisions. Whenever possible, include probabilities and ranges of loss or gain along with confidence levels, to enable management to balance risk-return.				X	100		
	12. Provide decision makers with an understanding of worst-case and most-probable scenarios, I&T-related loss exposures and significant reputation, legal and regulatory considerations, or any other impact category as per the risk taxonomy.			X		67		
	13. Report the current risk profile to all stakeholders. Include information on the effectiveness of the risk management process, control effectiveness, gaps, inconsistencies, redundancies, remediation status and their impacts on the risk profile.	X				0		

Level 4	The process achieves its purpose, is well defined and its performance is quantitatively measured.	14. On a periodic basis, for areas with relative risk and risk capacity parity, identify I&T-related opportunities that would allow the acceptance of greater risk and enhanced growth and return.		X			33						
		15. Determine whether each organizational entity monitors risk and accepts accountability for operating within its individual and portfolio tolerance levels.	X				0						
		16. Define a balanced set of project proposals designed to reduce risk and/or projects that enable strategic enterprise opportunities, considering costs, benefits, effect on current risk profile and regulations.	X				0						
		17. Prepare, maintain and test plans that document the specific steps to take when a risk event may cause a significant operational or development incident with serious business impact. Ensure that plans include pathways of escalation across the enterprise.		X			33						
		18. Apply the appropriate response plan to minimize the impact when risk incidents occur.			X		67						
	All activities are performed and largely achieved or full achieved the process purpose.	To what extent are the following activities performed?	Not achieved (0%-15%)	Partially Achieved (>15% -	Largely Achieved (>50% -	Fully Achieved (>85% -	Score (%)	Average score (%)	Achievement of Capability Level 4		P		
		1. Survey and analyze the historical I&T risk data and loss experience from externally available data and trends, industry peers through industry-based event logs, databases, and industry agreements for common event disclosure.			X		67	43					
		2. For similar classes of events, organize the collected data and highlight contributing factors. Determine common contributing factors across multiple events.		X			33						
		3. Determine the specific conditions that existed or were absent when risk events occurred and the way the conditions affected event frequency and loss magnitude.		X			33						
		4. Perform periodic event and risk factor analysis to identify new or emerging risk issues and to gain an understanding of the associated internal and external risk factors.			X		67						
		5. Validate the risk analysis and business impact analysis (BIA) results before using them in decision making. Confirm that the analysis aligns with enterprise requirements and verify that estimations were properly calibrated and scrutinized for bias.	X				0						
		6. Based on all risk profile data, define a set of risk indicators that allow the quick identification and monitoring of current risk and risk trends.	X				0						

		7. Capture information on I&T risk events that have materialized for inclusion in the IT risk profile of the enterprise.				X	100					
		8. Review the results of objective third-party assessments and internal audit and quality assurance reviews. Include them in the risk profile. Review identified gaps and I&T-related loss exposures to determine the need for additional risk analysis.	X				0					
		9. Categorize incidents and compare I&T-related loss exposures against risk tolerance thresholds. Communicate business impacts to decision makers as part of reporting and update the risk profile.			X		67					
		10. Examine past adverse events/losses and missed opportunities and determine root causes.			X		67					
Level 5	The process achieves its purpose, is well defined, its performance is measured to improve performance and continuous improvement is pursued.	To what extent are the following activities performed?	Not achieved (0%-15%)	Partially Achieved (>15% -	Largely Achieved (>50% -	Fully Achieved (>85% -	Score (%)	Average score (%)	Achievement of Capability Level 5			P
		1. Analyze cost/benefit of potential risk response options such as avoid, reduce/mitigate, transfer/share, and accept and exploit/seize. Confirm the optimal risk response.	X				0					
	All activities are performed and largely achieved or full achieved the process purpose.	2. Communicate root cause, additional risk response requirements and process improvements to appropriate decision makers. Ensure that the cause, response requirements and process improvement are included in risk governance processes.		X			33	17		P		



Lampiran 11. Dokumentasi Pelaksanaan FGD



Lampiran 12. Dokumentasi Permintaan Dokumen Pendukung



Lampiran 13. Form Validasi Hasil Evaluasi dan Rekomendasi

FORM VALIDASI HASIL EVALUASI DAN REKOMENDASI

Dalam Rangka Penelitian Skripsi “Pengukuran Kapabilitas Manajemen Risiko Informasi dan Teknologi (I&T) pada Dinas Komunikasi dan Informatika Kabupaten Klungkung Menggunakan *Framework* COBIT 2019”

Nama Instansi: Dinas Komunikasi dan Informatika Kabupaten Klungkung

Peneliti: Ketut Ananda Dharmawati

Tanggal Pelaksanaan: 2 Juni 2026

Metode: *Focus Group Discussion* (FGD)

A. Tujuan Validasi

Form ini digunakan untuk memperoleh tanggapan dari informan terhadap hasil evaluasi tingkat kapabilitas dan rekomendasi perbaikan pada domain EDM03 (*Ensure Risk Optimization*) dan APO12 (*Managed Risk*) berdasarkan *framework* COBIT 2019. Validasi dilakukan untuk memastikan:

1. Hasil penilaian sudah sesuai dengan kondisi faktual di instansi.
2. Rekomendasi yang diberikan relevan, realistis, dan dapat diterapkan.
3. Terdapat kesesuaian antara hasil analisis dengan konteks Manajemen Risiko I&T pada Dinas Komunikasi dan Informatika Kabupaten Klungkung.

B. Identitas Informan

1. Dr. I Wayan Sudiarsa, S.Pd., M.Si (Kepala Dinas Komunikasi dan Informatika Kabupaten Klungkung)
2. I Gusti Bagus Widya Hantersa, S.Kom (JF Pranata Komputer Ahli Muda)
3. I Made Agus Yudhiyantara, SE (Kepala Bidang Statistik dan Persandian)
4. Ida Bagus Gede Agung Darmita, S.Kom., M.Kom (JF Pranata Humas Ahli Muda)
5. I Nyoman Dharma Wijaya, SE., M.Si (JF Perencana Ahli Muda)
6. I Komang Sandiyasa, ST (JF Sandiman Ahli Muda)

C. Komponen yang Divalidasi

No	Komponen yang Divalidasi	Pernyataan Validasi	Catatan / Masukan Informan
1	Hasil Evaluasi Aktivitas Proses Domain EDM03	☒ Sesuai ☐ Perlu Revisi	—
2	Hasil Evaluasi Aktivitas Proses Domain APO12	☒ Sesuai ☐ Perlu Revisi	—
3	Penentuan Level Kapabilitas pada masing-masing domain	☒ Sesuai ☐ Perlu Revisi	—
4	Analisis <i>Gap</i> antara kondisi aktual dan target kapabilitas	☒ Sesuai ☐ Perlu Revisi	—
5	Rekomendasi Perbaikan (EDM03 dan APO12)	☒ Sesuai ☐ Perlu Revisi	—
6	Kesesuaian Rekomendasi dengan Kondisi Organisasi	☒ Sesuai ☐ Perlu Revisi	—
7	Kelayakan Implementasi Rekomendasi	☒ Layak ☐ Perlu Penyesuaian	—

D. Ringkasan Tanggapan Informan

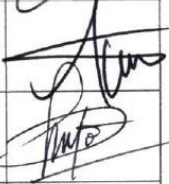
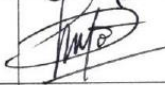
(Diisi oleh peneliti berdasarkan hasil diskusi atau catatan FGD)

No	Pokok Masukan dari Informan	Tindak Lanjut Peneliti
1	Hasil Evaluasi Domain EDM03 dan APO 12 dinilai telah sesuai dengan kondisi manajemen risiko I&T di Diskominpo Klungkung.	Hasil Evaluasi dipertahankan dalam laporan penelitian.
2	Penentuan level kapabilitas dinilai telah menggambarkan kondisi aktual organisasi berdasarkan bukti yang tersedia.	Hasil penilaian kapabilitas dipertahankan dalam laporan penelitian.

No	Pokok Masukan dari Informan	Tindak Lanjut Peneliti
3	Analisis kesenjangan dan target kapabilitas dinilai relevan dengan kebutuhan peningkatan manajemen risiko I&T organisasi.	Analisis kesenjangan dipertahankan sebagai dasar penyusunan rekomendasi.
4	Rekomendasi yang diberikan dinilai realistis dan dapat digunakan sebagai acuan peningkatan kapabilitas manajemen risiko I&T.	Rekomendasi dipertahankan dalam laporan penelitian.
5	Tidak terdapat koreksi substansial terhadap hasil evaluasi dan rekomendasi yang disampaikan peneliti.	Dilakukan penyempurnaan redaksional seperlunya pada laporan akhir penelitian.

E. Tanda Tangan Informan

Sebagai bentuk persetujuan terhadap hasil validasi dan masukan yang telah diberikan, para informan menandatangani form ini.

No	Nama Informan	Jabatan	Tanda Tangan
1	Dr. I Wayan Sudiarsa, S.Pd., M.Si	Kepala Dinas Komunikasi dan Informatika	
2	I Gusti Bagus Widya Hantersa, S.Kom	JF Pranata Komputer Ahli Muda	
3	I Made Agus Yudhiyantara, SE	Kepala Bidang Statistik dan Persandian	
4	Ida Bagus Gede Agung Darmita, S.Kom., M.Kom	JF Pranata Hubungan Masyarakat Ahli Muda	
5	I Nyoman Dharma Wijaya, SE., M.Si	JF Perencana Ahli Muda	
6	I Komang Sandiyasa, ST	JF Sandiman Ahli Muda	

Lampiran 14. Berita Acara Validasi Hasil Evaluasi dan Rekomendasi

BERITA ACARA

Validasi Hasil Evaluasi dan Rekomendasi Penelitian Skripsi

Nomor: B.500.12.6.1/0495/Diskominfo/2026

Pada hari Selasa, tanggal 2 Juni 2026, telah dilaksanakan kegiatan *Focus Group Discussion* (FGD) dalam rangka validasi hasil penelitian skripsi dengan judul “Pengukuran Kapabilitas Manajemen Risiko Informasi dan Teknologi (I&T) pada Dinas Komunikasi dan Informatika Kabupaten Klungkung Menggunakan *Framework* COBIT 2019”. FGD dilaksanakan di Dinas Komunikasi dan Informatika Kabupaten Klungkung dengan melibatkan informan yang mewakili unsur pimpinan dan bidang teknis terkait tata kelola serta manajemen risiko I&T.

Kegiatan ini bertujuan untuk:

1. Menyampaikan hasil evaluasi tingkat kapabilitas proses manajemen risiko I&T berdasarkan domain EDM03 (*Ensure Risk Optimization*) dan APO12 (*Managed Risk*) dari *framework* COBIT 2019.
2. Memperoleh tanggapan, klarifikasi, serta masukan dari pihak Dinas Komunikasi dan Informatika Kabupaten Klungkung terkait hasil analisis dan rekomendasi perbaikan yang telah disusun.
3. Memastikan bahwa hasil penelitian sesuai dengan kondisi faktual dan dapat diimplementasikan secara realistis di Dinas Komunikasi dan Informatika Kabupaten Klungkung.

Setelah dilakukan pemaparan hasil oleh peneliti dan diskusi bersama para informan, diperoleh beberapa tanggapan dan kesepakatan hasil FGD sebagai berikut:

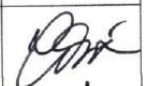
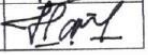
I. Pokok Pembahasan

1. Penyampaian hasil evaluasi tingkat kapabilitas domain EDM03 dan APO12.
2. Penjelasan hasil analisis kesenjangan (*gap*) antara kondisi aktual dan target kapabilitas.
3. Penyajian rekomendasi perbaikan tata kelola dan manajemen risiko I&T berdasarkan COBIT 2019.
4. Pembahasan kelayakan implementasi dan prioritas rencana perbaikan.

II. Hasil dan Kesepakatan

1. Hasil evaluasi tingkat kapabilitas domain EDM03 dan APO12 dinilai telah sesuai dengan kondisi actual manajemen risiko I&T di Dinas Komunikasi dan Informatika Kabupaten Klungkung.
2. Hasil analisis kesenjangan dan rekomendasi perbaikan dinilai relevan dengan kebutuhan peningkatan kapabilitas manajemen risiko I&T organisasi.
3. Tidak terdapat koreksi substansial terhadap hasil evaluasi yang disampaikan peneliti.
4. Informan menyetujui penggunaan hasil evaluasi dan rekomendasi sebagai bagian dari laporan penelitian skripsi.
5. Masukan yang diberikan selama diskusi digunakan sebagai bahan penyempurnaan laporan penelitian sebelum proses finalisasi.

III. Daftar Informan

No	Nama	Jabatan	Tanda Tangan
1	Dr. I Wayan Sudiarsa, S.Pd., M.Si	Kepala Dinas Komunikasi dan Informatika	
2	I Gusti Bagus Widya Hantersa, S.Kom	JF Pranata Komputer Ahli Muda	
3	I Made Agus Yudhiyantara, SE	Kepala Bidang Statistik dan Persandian	
4	Ida Bagus Gede Agung Darmita, S.Kom., M.Kom	JF Pranata Hubungan Masyarakat Ahli Muda	
5	I Nyoman Dharma Wijaya, SE., M.Si	JF Perencana Ahli Muda	
6	I Komang Sandiyasa, ST	JF Sandiman Ahli Muda	

Demikian berita acara ini dibuat dengan sebenarnya untuk digunakan sebagaimana mestinya. Berita acara ini menjadi bagian dari dokumentasi kegiatan validasi hasil penelitian dan akan dilampirkan dalam laporan akhir skripsi.

Semarapura, 2 Juni 2026

Peneliti,



Ketut Ananda Dharmawati

Mengetahui,

Kepala Dinas Komunikasi dan Informatika

Kabupaten Klungkang



Dr. I Wayan Sudiarsa, S.Pd., M.Si

NIP 19700220 199412 1 003

Lampiran 15. Riwayat Hidup



Ketut Ananda Dharmawati lahir di Kamasan pada tanggal 7 Juni 2004. Penulis merupakan putri dari pasangan (Alm.) I Wayan Resten dan Ni Wayan Wening. Penulis berkewarganegaraan Indonesia dan beragama Hindu. Pendidikan dasar ditempuh di SD Negeri 1 Kamasan dan lulus pada tahun 2016. Selanjutnya, penulis menempuh pendidikan menengah pertama di SMP Negeri 1 Semarapura dan lulus pada tahun 2019. Pendidikan menengah atas ditempuh di SMA Negeri 1 Semarapura pada peminatan Bahasa dan Budaya (IBB) dan diselesaikan pada tahun 2022. Pada tahun yang sama, penulis melanjutkan pendidikan ke jenjang Sarjana (S1) pada Program Studi Sistem Informasi, Jurusan Teknik Informatika, Fakultas Teknik dan Kejuruan, Universitas Pendidikan Ganesha.

