Yth.
1. Direksi Bank Umum Konvensional; dan
2. Direksi Bank Umum Syariah,

di tempat.

SALINAN
SURAT EDARAN OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 24/SEOJK.03/2023
TENTANG
PENILAIAN TINGKAT MATURITAS DIGITAL BANK UMUM

Sehubungan dengan berlakunya Peraturan Otoritas Jasa Keuangan Nomor 11/POJK.03/2022 tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum (Lembaran Negara Republik Indonesia Tahun 2022 Nomor 5/OJK, Tambahan Lembaran Negara Republik Indonesia Nomor 5/OJK) yang selanjutnya disebut sebagai POJK PTI, perlu untuk mengatur ketentuan pelaksanaan mengenai penilaian tingkat maturitas digital bank umum dalam Surat Edaran Otoritas Jasa Keuangan sebagai berikut:

I. KETENTUAN UMUM

1. Latar Belakang

Perkembangan Teknologi Informasi yang selanjutnya disingkat TI secara cepat telah mengubah proses bisnis serta model layanan yang disediakan oleh Bank kepada konsumen. Perubahan lanskap perbankan didorong oleh perubahan perilaku ekonomi masyarakat yang semakin ke arah digital, sehingga transformasi digital merupakan salah satu langkah yang dilakukan oleh Bank untuk dapat menyediakan produk dan layanan sesuai dengan kebutuhan konsumen. Tuntutan konsumen terhadap layanan berbasis digital yang lengkap dan aman menyebabkan tingginya ketergantungan Bank terhadap penggunaan TI dalam seluruh aktivitas operasionalnya. Transformasi digital dapat secara maksimal memberikan manfaat jika adopsi TI sesuai dengan kebutuhan proses bisnis Bank. Selain membawa peluang, tentunya transformasi digital juga memiliki tantangan diantaranya kebocoran data, investasi teknologi yang tidak sesuai dengan strategi bisnis, penyalahgunaan teknologi, serangan siber, tingginya ketergantungan terhadap pihak penyedia jasa TI, literasi keuangan digital yang masih rendah dan infrastruktur TI yang belum merata di Indonesia. Kesuksesan transformasi digital perbankan salah satunya bergantung dari kombinasi 3 (tiga) unsur, yaitu sumber daya manusia pada perbankan, proses dalam implementasi strategi untuk melakukan transformasi bisnis, serta teknologi yang menciptakan nilai tambah bagi Bank dan konsumen. Peningkatan kematangan dalam penyelenggaraan TI merupakan suatu konsekuensi yang perlu dilakukan oleh Bank ketika melakukan transformasi digital. Salah satu upaya yang dapat dilakukan oleh Bank untuk meningkatkan kematangan dalam penyelenggaraan TI

adalah melalui penerapan tata kelola dan manajemen risiko TI secara memadai. Selanjutnya untuk mengetahui tingkat kematangan tersebut, diperlukan suatu panduan berupa penilaian tingkat maturitas digital yang dapat digunakan oleh Bank dan Otoritas Jasa Keuangan untuk mengukur kualitas penyelenggaraan TI Bank.

2. Tingkat maturitas digital merupakan kondisi yang mencerminkan pemenuhan terhadap seluruh aspek dalam penyelenggaraan TI sesuai dengan POJK PTI serta kesiapan Bank dalam mendukung transformasi digital.
3. Penilaian tingkat maturitas digital merupakan panduan untuk menentukan, menilai, dan mengevaluasi tingkat digitalisasi Bank, sehingga dapat diketahui kondisi digitalisasi Bank. Panduan tersebut juga dapat digunakan sebagai alat monitoring bagi Bank dan Otoritas Jasa Keuangan terhadap perkembangan transformasi digital yang dilakukan oleh Bank.
4. Penilaian tingkat maturitas digital Bank dapat menjadi salah satu acuan bagi Bank untuk mengetahui keandalan infrastruktur TI serta manajemen pengelolaan infrastruktur TI, sehingga dapat digunakan oleh Bank sebagai dasar pertimbangan untuk pengembangan produk dan layanan yang lebih komprehensif bagi konsumen.

II. PENILAIAN SENDIRI TINGKAT MATURITAS DIGITAL BANK

1. Untuk melaksanakan Pasal 66 POJK PTI, Bank melakukan penilaian sendiri atas tingkat maturitas digital Bank secara berkala, paling sedikit 1 (satu) kali dalam 1 (satu) tahun dengan mempertimbangkan adanya perubahan kondisi intern dan ekstern Bank. Contoh perubahan kondisi intern yaitu perubahan sasaran dan strategi bisnis Bank. Contoh perubahan kondisi ekstern yaitu perkembangan Tl. Tingkat maturitas digital Bank mempertimbangkan seluruh aspek dalam penyelenggaraan TI. Dalam hal teridentifikasi terdapat area yang memiliki kelemahan dan memerlukan perbaikan, hal tersebut dapat menjadi masukan untuk meningkatkan maturitas digital dalam penyelenggaraan TI Bank.
2. Tata Cara Penilaian Sendiri Tingkat Maturitas Digital Bank
   a. Penilaian tingkat maturitas digital Bank mencakup penilaian terhadap aspek sebagai berikut:
      1) tata kelola, yang meliputi tatanan institusi dan tata kelola TI;
      2) arsitektur, yang meliputi arsitektur TI;
      3) manajemen risiko, yang meliputi manajemen risiko TI;
      4) ketahanan dan keamanan siber, sesuai dengan peringkat tingkat maturitas keamanan siber dengan mengacu pada ketentuan Otoritas Jasa Keuangan mengenai ketahanan dan keamanan siber bagi bank umum;
      5) teknologi, yang meliputi adopsi TI secara bertanggung jawab dan penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI Bank;
      6) data, yang meliputi tata kelola data, pelindungan data pribadi, dan transfer data;
      7) kolaborasi, yang meliputi kerja sama kemitraan dan penyediaan jasa TI oleh Bank; dan

8) pelindungan konsumen, yang meliputi pemenuhan aspek pelayanan dan pelindungan konsumen.

b. Dalam melakukan penilaian atas tingkat maturitas digital Bank sebagaimana dimaksud pada huruf a, Bank melakukan analisis terhadap penerapan kontrol atas aspek maturitas digital Bank sebagaimana tercantum dalam Lampiran I yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

c. Dalam melakukan penilaian tingkat maturitas digital Bank, Bank menggunakan format kertas kerja penilaian kualitas penerapan aspek maturitas digital Bank sebagaimana tercantum dalam Lampiran II yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

d. Penetapan tingkat kualitas penerapan aspek maturitas digital Bank dikategorikan ke dalam Peringkat 1 (*strong*), Peringkat 2 (*satisfactory*), Peringkat 3 (*fair*), Peringkat 4 (*marginal*), dan Peringkat 5 (*unsatisfactory*), dilakukan dengan mengacu pada definisi peringkat pada matriks penetapan kualitas penerapan aspek maturitas digital Bank sebagaimana tercantum dalam Lampiran III Bagian A yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

e. Penetapan tingkat maturitas digital Bank dikategorikan ke dalam 5 (lima) tingkat, yaitu Tingkat 1, Tingkat 2, Tingkat 3, Tingkat 4, dan Tingkat 5, dilakukan dengan mengacu pada definisi peringkat pada matriks penetapan tingkat maturitas digital Bank sebagaimana tercantum dalam Lampiran III Bagian B yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.

3. Bank dapat melakukan penilaian tingkat maturitas digital Bank secara mandiri dan/atau menggunakan pihak ketiga. Dalam hal penilaian tingkat maturitas digital dilakukan oleh:
   a. Bank secara mandiri maka penilaian dilakukan oleh pihak independen di intern Bank yang memiliki kompetensi relevan, yaitu pihak berbeda dengan yang melakukan operasional, untuk menghindari benturan kepentingan;
   b. pihak ketiga, Bank harus:
      1) memastikan pihak ketiga memiliki kompetensi yang memadai sesuai dengan kebutuhan penilaian, antara lain dengan adanya sertifikasi dan/atau pengakuan dari lembaga yang berwenang di Indonesia atau di luar negeri, atau pengalaman yang relevan; dan
      2) bertanggung jawab atas pelaksanaan penilaian tingkat maturitas digital.
4. Bank memiliki kebijakan dan prosedur intern dalam melakukan penilaian yang memuat paling sedikit mengenai pihak yang melakukan penilaian dan pihak yang melakukan reviu atas penilaian yang disesuaikan dengan organisasi dan kompleksitas Bank.
5. Otoritas Jasa Keuangan melakukan penelaahan atas hasil penilaian sendiri tingkat maturitas digital sebagaimana dimaksud pada angka 1. Dalam hal berdasarkan penelaahan Otoritas Jasa Keuangan menunjukkan bahwa hasil penilaian tingkat maturitas digital tidak mencerminkan kondisi Bank yang sebenarnya, Otoritas Jasa Keuangan dapat menyesuaikan hasil penilaian tingkat maturitas digital.

III. PELAPORAN

1. Bank menyampaikan laporan hasil penilaian sendiri atas tingkat maturitas digital Bank sebagai bagian dari laporan kondisi terkini penyelenggaraan TI Bank sebagaimana dimaksud dalam POJK PTI.
2. Hasil penilaian tingkat maturitas digital Bank sebagaimana dimaksud pada Romawi II angka 2.e. disampaikan kepada Otoritas Jasa Keuangan sebagai bagian dari laporan kondisi terkini penyelenggaraan TI Bank, yaitu paling lama 15 (lima belas) hari kerja setelah akhir tahun pelaporan dengan menggunakan format sebagaimana tercantum dalam Lampiran IV yang merupakan bagian tidak terpisahkan dari Surat Edaran Otoritas Jasa Keuangan ini.
3. Penilaian tingkat maturitas digital Bank pertama kali dilakukan oleh Bank untuk posisi akhir bulan Desember 2023 dan hasil penilaian dimaksud disampaikan kepada Otoritas Jasa Keuangan paling lambat pada akhir bulan Juni 2024. Untuk penilaian tahun berikutnya disampaikan sesuai dengan tenggat waktu sebagaimana dimaksud pada angka 2.

IV. PENUTUP

Ketentuan dalam Surat Edaran Otoritas Jasa Keuangan ini mulai berlaku pada tanggal ditetapkan.

Ditetapkan di Jakarta
pada tanggal 14 Desember 2023

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Mufli Asmawidjaja

LAMPIRAN I
SURAT EDARAN OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 24/SEOJK.03/2023
TENTANG
PENILAIAN TINGKAT MATURITAS DIGITAL BANK UMUM

Penilaian Kualitas Kontrol atas Aspek Maturitas Digital Bank

Matriks Kontrol atas Aspek Maturitas Digital Bank

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
1.	Tata Kelola	1.a. Tatanan Institusi	1.a.1. Bank memiliki permodalan yang memadai untuk mendukung rencana pengembangan TI.	a. Bank memiliki kecukupan serta dukungan permodalan yang memadai untuk mendukung rencana pengembangan TI. b. Terdapat dokumen pendukung yang menunjukkan komitmen dari pemegang saham untuk mendukung permodalan Bank dalam pengembangan TI, antara lain laporan rapat umum pemegang saham, rencana strategis TI (RSTI), rencana korporasi maupun rencana bisnis Bank yang memuat alokasi anggaran untuk pengembangan TI.
			1.a.2. Bank mengelola portofolio investasi TI secara memadai.	a. Bank melakukan analisis kelayakan rencana investasi yang akan didanai, memuat antara lain keselarasan rencana investasi TI dengan strategi Bank, keuntungan dan risiko bagi Bank, ketersediaan sumber pendanaan, perhitungan ekspektasi tingkat pengembalian investasi, serta dampak penambahan investasi terhadap portofolio investasi Bank secara keseluruhan. b. Bank menetapkan prioritas alokasi sumber dana pada investasi TI yang bernilai tinggi. c. Bank memantau kinerja portofolio investasi, seperti tren tingkat pengembalian investasi, deviasi anggaran, dan realisasi investasi.
			1.a.3. Bank melakukan pengelolaan biaya terkait TI secara efektif.	Bank melakukan pengelolaan biaya secara efektif antara lain:

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				a. melakukan pemantauan deviasi anggaran, proyeksi biaya, dan realisasi biaya, termasuk analisis biaya dan manfaat; dan b. melakukan pemantauan penggunaan anggaran sesuai dengan manfaat yang diterima, termasuk jika penyelenggaraan TI disediakan oleh pihak penyedia jasa TI.
			1.a.4. Direksi dan Dewan Komisaris memiliki komitmen untuk menerapkan kepemimpinan yang berorientasi digital (*digital leadership*).	Bank memiliki komitmen untuk mengembangkan kepemimpinan yang berorientasi digital bagi Direksi, Dewan Komisaris, dan jajaran manajemen antara lain dengan menyediakan program pelatihan bagi Direksi, Dewan Komisaris, dan jajaran manajemen terkait pengembangan kepemimpinan yang berorientasi digital. Kepemimpinan yang berorientasi digital yaitu kepemimpinan strategis yang dapat memanfaatkan aset digital Bank untuk mencapai tujuan organisasi.
			1.a.5. Bank memiliki desain organisasi yang mendukung transformasi digital.	Bank memiliki desain organisasi yang memungkinkan Bank dapat melakukan pekerjaan yang mendukung transformasi digital, antara lain memuat aspek sebagai berikut: a. Bank memiliki struktur organisasi yang kolaboratif, sehingga memungkinkan interaksi yang lebih luas antar unit kerja agar proses bisnis Bank berjalan lebih adaptif; b. melaksanakan kewenangan yang terdesentralisasi di unit kerja sehingga pengambilan keputusan dapat dilakukan dengan lebih cepat; dan

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				c. pemanfaatan TI yang mendukung kolaborasi, komunikasi, dan konektivitas untuk menyelesaikan pekerjaan pada Bank.
			1.a.6. Bank memiliki program pengembangan budaya digital dan menerapkan budaya digital untuk mendukung transformasi digital.	a. Terdapat informasi yang menunjukkan komitmen Direksi dan Dewan Komisaris untuk mengembangkan budaya digital pada laporan tahunan dan rencana bisnis Bank. b. Bank memiliki pengembangan budaya digital antara lain kolaborasi, *data driven*, berfokus pada pelanggan (*customer centric*), inovasi digital, serta integrasi teknologi digital dalam semua proses bisnis. c. Bank melakukan evaluasi program pengembangan budaya digital.
			1.a.7. Bank melakukan pengembangan talenta digital.	a. Bank memiliki kebijakan terkait pengembangan talenta digital secara terstruktur dan memadai mulai dari proses rekrutmen, perencanaan, evaluasi, dan pengembangan. b. Bank melakukan pengembangan talenta digital melalui rekrutmen atau pelatihan/sertifikasi, antara lain pada jenis keahlian terkait: 1) perkembangan teknologi terkini, antara lain *machine learning*, *blockchain*, *cloud integration, biometrics*, dan *experience design*; 2) *digital business* dan *marketing*; 3) *cybersecurity* dan *data privacy;* dan 4) *customer engagement.* c. Bank melakukan evaluasi terhadap program pengembangan talenta digital secara berkala.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				d. Bank memastikan keberlanjutan atas program pengembangan talenta digital.
		1.b. Tata Kelola TI	1.b.1. Bank memastikan pengaturan dan pengelolaan tata kelola TI telah memadai.	Bank menyelaraskan tata kelola TI sesuai dengan prinsip tata kelola TI yang baik, melalui: a. penetapan struktur, proses, dan praktik tata kelola TI yang selaras dengan prinsip tata kelola Bank; dan b. penetapan mekanisme koordinasi dan pelaporan terkait tata kelola TI untuk pengawasan dan pengambilan keputusan.
			1.b.2. Bank mengoptimalkan nilai bisnis dari investasi dalam proses bisnis, layanan dan aset TI.	a. Bank menyusun target investasi TI yang selaras dengan aspek berikut: 1) strategi bisnis Bank; 2) analisis biaya dan tingkat pengembalian investasi; dan 3) tingkat risiko dan jenis manfaat yang akan diperoleh. b. Bank memantau kesesuaian investasi TI dengan keuntungan yang diharapkan. Hal yang perlu diperhatikan Bank dalam melakukan pemantauan, yaitu: 1) jumlah peluang pendapatan bisnis baru yang direalisasikan sebagai akibat langsung dari investasi TI; 2) tujuan strategis Bank yang dicapai sebagai hasil dari inisiatif TI; dan 3) tingkat kepuasan pemangku kepentingan terhadap inisiatif TI.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			1.b.3. Bank memastikan risiko terkait penggunaan TI telah diidentifikasi dan dikelola secara memadai.	a. Bank mengidentifikasi dan mengevaluasi risiko penggunaan TI serta memastikan bahwa risiko penggunaan TI tidak melebihi toleransi risiko Bank. b. Bank menerapkan praktik manajemen risiko terhadap penggunaan TI, yaitu: 1) Bank memiliki strategi pengelolaan risiko TI yang terintegrasi dalam praktik manajemen risiko Bank secara keseluruhan; dan 2) Bank memiliki mekanisme atau proses untuk identifikasi, monitor, mitigasi, dan pelaporan risiko.
			1.b.4. Bank memastikan sumber daya terkait TI, meliputi Sumber Daya Manusia (SDM), proses, dan teknologi tersedia untuk mendukung Bank secara efektif dan dengan biaya optimal.	a. Bank mengidentifikasi dan mengevaluasi kebutuhan sumber daya terkait TI minimal 1 (satu) tahun sekali yang mencakup kebutuhan pendanaan, SDM, strategi, dan pengembangan kapabilitas yang diperlukan. b. Bank memonitor pengelolaan sumber daya telah dijalankan secara optimal. Hal yang perlu diperhatikan Bank yaitu: 1) Bank memiliki mekanisme atau proses untuk identifikasi, respon atau mitigasi dan pelaporan suatu permasalahan; 2) tingkat umpan balik (*feedback*) pemangku kepentingan tentang optimalisasi sumber daya; 3) jumlah manfaat yang dicapai melalui optimalisasi pemanfaatan sumber daya, misalnya penghematan biaya; 4) jumlah target kinerja pengelolaan sumber daya yang direalisasikan; dan

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				5) jumlah proyek dan program dengan status berisiko sedang atau tinggi karena masalah pengelolaan sumber daya.
			1.b.5. Bank mengidentifikasi, mengevaluasi, dan melibatkan seluruh pemangku kepentingan dalam tata kelola TI.	a. Bank melakukan identifikasi dan evaluasi terhadap pemangku kepentingan yang terlibat dalam tata kelola TI dan kebutuhan terkait komunikasi maupun pelaporan kepada pemangku kepentingan yang relevan. b. Bank memastikan keterlibatan pemangku kepentingan dan efektivitas komunikasi dengan pemangku kepentingan. Hal yang perlu diperhatikan Bank dalam memastikan keterlibatan pemangku kepentingan yaitu: 1) tingkat keterlibatan pemangku kepentingan dengan TI Bank; 2) tingkat kepuasan pemangku kepentingan dengan strategi komunikasi dan pelaporan; 3) persentase laporan yang tidak akurat; dan 4) persentase laporan yang disampaikan tepat waktu.
			1.b.6. Sistem manajemen TI Bank dirancang secara memadai.	a. Bank merancang sistem manajemen TI sesuai dengan kebutuhan Bank. Hal yang perlu diperhatikan Bank dalam merancang sistem manajemen TI, yaitu: 1) visi dan misi Bank; 2) strategi Bisnis Bank; 3) tantangan yang dihadapi Bank; 4) lingkungan internal Bank, termasuk budaya, toleransi risiko, keamanan dan kebijakan privasi, nilai etika, kode etik, dan akuntabilitas; dan

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				5) standar maupun regulasi terkait. b. Bank mengkomunikasikan tujuan dan arah penggunaan TI ke seluruh pegawai. Hal yang perlu diperhatikan Bank yaitu memastikan informasi yang dikomunikasikan mencakup misi, tujuan layanan, dan pengendalian internal. c. Bank menetapkan struktur organisasi sesuai dengan desain sistem manajemen, antara lain adanya komite pengarah TI. d. Bank menetapkan peran dan tanggung jawab untuk pengelolaan TI Bank termasuk limit, tanggung jawab, dan akuntabilitas. e. Bank mengoptimalkan penempatan fungsi TI dalam struktur organisasi. Penempatan fungsi TI dalam organisasi, baik terpusat, terdesentralisasi, maupun kombinasi, mencerminkan kepentingan strategis dan ketergantungan operasional TI dalam Bank, model operasional Bank dan strategi penempatan sumber daya pada fungsi TI. f. Bank menentukan kepemilikan data dan informasi, serta sistem informasi. g. Bank menentukan standar kompetensi yang diperlukan untuk mencapai tujuan bisnis bank yang relevan. h. Bank menetapkan dan mengkomunikasikan kebijakan dan prosedur kontrol TI pada area utama seperti kualitas, keamanan, privasi, kontrol internal, penggunaan aset TI, etika, dan hak kekayaan intelektual.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				i. Bank menetapkan dan mengimplementasikan infrastruktur, layanan, dan aplikasi untuk mendukung tata kelola dan sistem manajemen.
			1.b.7. Bank memastikan bahwa setiap inisiatif digitalisasi atau transformasi digital yang dimuat dalam RSTI Bank telah sesuai dengan arah dan strategi Bank.	a. Bank memahami lingkungan bisnis dan arah pengembangan Bank ke depan. Yang dimaksud lingkungan bisnis yaitu faktor penentu perubahan industri, regulasi terkait, tingkat persaingan, model operasional saat ini, dan target tingkat maturitas digitalisasi. b. Bank menilai kemampuan, kinerja, dan tingkat maturitas digitalisasi Bank saat ini. c. Bank menentukan target kapabilitas digital berdasarkan hasil pemahaman lingkungan bisnis dan arah pengembangan Bank ke depan. Target kapabilitas digital dapat mencakup produk dan layanan serta kapabilitas digital yang diperlukan untuk menghasilkan produk dan layanan tersebut. d. Bank melakukan analisis kesenjangan antara lingkungan TI saat ini dan target ke depan, yang dapat dituangkan pada penilaian tingkat kesehatan Bank setelah dikomunikasikan kepada OJK terlebih dahulu. e. Bank menetapkan rencana strategis dan peta jalan transformasi yang akan dilakukan. Rencana tersebut tercantum pada RSTI. f. Bank mengkomunikasikan strategi dan arah pengembangan TI kepada seluruh pengampu kepentingan dan satuan kerja pengguna TI.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			1.b.8. Pengelolaan hubungan dengan pemangku kepentingan bisnis dengan cara yang formal dan transparan.	a. Bank memahami isu bisnis, tujuan dan ekspektasi atas TI yang dipergunakan Bank. b. Bank telah menjaga hubungan bisnis yang baik antara organisasi TI dan unit bisnis, antara lain peran dan tanggung jawab hubungan telah ditentukan, ditetapkan, dan dikomunikasikan secara memadai. c. Bank telah melakukan komunikasi melalui sistem internal yang transparan dengan semua pemangku kepentingan yang relevan dan mengoordinasikan layanan TI yang diberikan kepada unit bisnis. d. Bank secara berkesinambungan memperbaiki dan mengembangkan layanan TI yang diperlukan oleh organisasi agar tetap relevan dengan perkembangan bisnis Bank dan teknologi.
			1.b.9. Bank mengelola layanan TI secara memadai bagi pihak internal dan eksternal.	a. Bank menganalisis layanan TI saat ini untuk mengidentifikasi kinerja layanan terhadap aktivitas bisnis yang didukung oleh layanan tersebut serta analisis kebutuhan untuk mengembangkan layanan TI. Bank menganalisis persyaratan bisnis dan sejauh mana tingkat dan layanan yang mendukung TI, mendukung proses bisnis yang dapat dilakukan antara lain melalui analisis: 1) jumlah aktivitas bisnis yang tidak didukung oleh layanan TI; dan 2) jumlah layanan usang yang telah teridentifikasi.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				b. Bank menganalisis layanan TI saat ini untuk mengidentifikasi kinerja layanan terhadap aktivitas bisnis mitra terkait penyediaan jasa TI. c. Bank memiliki dan mengelola katalog layanan TI serta melakukan publikasi layanan aktif, yang mencakup: 1) perbandingan layanan dan paket layanan TI langsung yang ditawarkan dengan portofolio; dan 2) waktu sejak pembaruan portofolio layanan terakhir. d. Bank memantau tingkat layanan TI, mengamati tren layanan TI, dan menetapkan langkah tindak lanjut atas penurunan kinerja layanan TI. Hal yang perlu diperhatikan dalam memantau tingkat layanan TI yaitu: 1) tingkat beratnya pelanggaran layanan; 2) persentase nasabah yang puas terhadap layanan; dan 3) persentase target layanan terpenuhi.
			1.b.10. Bank menerapkan praktik dan standar pengendalian kualitas dalam semua proses dan prosedur.	a. Bank mengembangkan manajemen mutu yang dijadikan standar dan pendekatan untuk sistem manajemen informasi. b. Bank mengetahui kebutuhan pemangku kepentingan dan memastikan kebutuhan tersebut telah terintegrasi pada praktik manajemen kualitas. c. Bank mengelola standar, praktik, dan prosedur kualitas serta mengintegrasikan manajemen kualitas ke dalam semua proses.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				d. Bank melakukan pemantauan, pengendalian, dan evaluasi terhadap kualitas proses dan layanan secara berkesinambungan sesuai standar manajemen kualitas.
			1.b.11. Sistem manajemen keamanan informasi sudah didefinisikan, dioperasikan, dan dipantau.	a. Bank membangun dan memelihara sistem manajemen keamanan informasi yang menyediakan pendekatan standar, formal, dan berkelanjutan untuk manajemen keamanan informasi, memungkinkan teknologi yang aman, dan proses bisnis yang selaras dengan kebutuhan bisnis. b. Bank menetapkan dan mengelola rencana penanganan risiko keamanan informasi dan data pribadi. c. Bank memantau dan meninjau sistem manajemen keamanan informasi secara berkala yang memperhitungkan paling sedikit: 1) frekuensi tinjauan keamanan terjadwal; 2) jumlah temuan dalam tinjauan keamanan yang dijadwalkan secara teratur; 3) tingkat kepuasan pemangku kepentingan dengan rencana keamanan; dan 4) jumlah insiden terkait keamanan yang disebabkan oleh kegagalan untuk mematuhi rencana keamanan.
			1.b.12. Aktivitas pengembangan, akuisisi, dan implementasi solusi/adopsi TI dan integrasinya dalam proses bisnis telah memadai.	a. Bank mengelola seluruh proyek yang diinisiasi secara terkoordinasi dengan menggunakan pendekatan *project management tools*. b. Bank mengelola seluruh program dari portofolio investasi terkait TI sesuai dengan strategi Bank secara terkoordinasi.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				c. Bank melakukan identifikasi solusi dan analisis persyaratan sebelum akuisisi atau pengembangan untuk memastikan bahwa solusi tersebut selaras dengan sasaran strategis Bank yang mencakup proses bisnis, aplikasi, informasi/data, infrastruktur, dan layanan. d. Bank merancang solusi TI, proses bisnis, dan alur kerja sesuai dengan persyaratan Bank membangun solusi TI yang mencakup tahap mengelola persiapan pengujian, pengujian, mengelola persyaratan, dan pemeliharaan proses bisnis, aplikasi, informasi/data, infrastruktur, dan layanan. e. Bank menyeimbangkan kebutuhan saat ini dan masa depan untuk ketersediaan, kinerja, dan kapasitas penyediaan layanan, termasuk menilai kemampuan saat ini, memprediksi kebutuhan masa depan berdasarkan kebutuhan bisnis, analisis dampak bisnis, dan penilaian risiko untuk merencanakan dan mengimplementasikan tindakan untuk memenuhi persyaratan yang diidentifikasi. f. Bank melakukan berbagai upaya untuk memaksimalkan keberhasilan perubahan bisnis akibat solusi TI seperti mempersiapkan dan memperoleh komitmen dari seluruh pemangku kepentingan yang terdampak perubahan atas solusi TI. g. Bank mengelola perubahan terkait TI, antara lain perubahan standar dan pemeliharaan yang berkaitan dengan proses bisnis, aplikasi, dan infrastruktur, yang mencakup evaluasi dampak

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				perubahan, prioritisasi dan otorisasi permintaan perubahan, monitoring status perubahan, pelaporan, penutupan, dan dokumentasi. h. Bank melakukan perencanaan implementasi, konversi sistem dan data, *acceptance testing*, komunikasi, persiapan rilis, promosi ke produksi proses bisnis/layanan TI baru atau yang diubah, dukungan produksi awal, dan kajian pascaimplementasi (*post implementation review*). i. Bank menjaga ketersediaan informasi yang relevan, terkini, tervalidasi, dan andal untuk mendukung proses dan memfasilitasi pengambilan keputusan terkait tata kelola dan manajemen TI Bank. j. Bank mengelola aset TI di sepanjang siklus hidup TI untuk memastikan bahwa penggunaannya memberikan nilai dengan biaya optimal, aset tetap beroperasi sesuai dengan tujuan, dan diperhitungkan serta dilindungi secara fisik. k. Bank menyusun dan mengelola model deskripsi dan hubungan (*configuration model*) layanan, aset, infrastuktur dan kapabilitas TI yang dibutuhkan untuk mendukung layanan TI.
			1.b.13. Aktivitas operasional layanan dan dukungan TI yang memadai.	a. Bank menerapkan prosedur operasional secara andal dan konsisten dalam memberikan layanan TI, baik layanan TI internal, layanan TI kepada pihak eksternal, infrastuktur TI, dan

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				fasilitas terkait seperti peralatan daya dan komunikasi. b. Bank memberikan respons yang tepat waktu dan efektif terhadap permintaan pengguna dan resolusi atas semua jenis insiden TI. c. Bank melakukan upaya identifikasi dan klasifikasi masalah serta akar penyebab dari insiden atau permasalahan yang muncul, termasuk menyusun klasifikasi masalah, kategorisasi dan prioritas, mencakup hal sebagai berikut: 1) persentase insiden besar yang masalahnya dicatat; 2) persentase insiden yang diselesaikan sesuai dengan jaminan tingkat layanan atau *service level agreement* (SLA) yang disepakati; dan 3) persentase masalah yang diidentifikasi dengan tepat, termasuk klasifikasi, kategorisasi, dan prioritas.
			1.b.14. Bank menetapkan rencana dan memastikan keberlangsungan rencana pemeliharaan untuk memungkinkan bisnis dan organisasi TI merespons insiden dan beradaptasi dengan cepat terhadap gangguan.	a. Bank menetapkan kebijakan, tujuan, dan ruang lingkup kelangsungan bisnis. b. Bank telah melakukan *Business Impact Analysis* (BIA), termasuk: 1) total waktu henti akibat insiden atau gangguan besar; dan 2) persentase pemangku kepentingan utama yang terlibat dalam analisis dampak bisnis yang mengevaluasi dampak gangguan dari waktu ke waktu terhadap fungsi bisnis

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				penting dan dampak gangguan terhadap Bank. c. Bank telah mengevaluasi berbagai pilihan strategi ketahanan bisnis guna memastikan kelangsungan bisnis disaat terjadi insiden TI. d. Bank telah mengembangkan dan mengimplementasikan *Business Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP) berdasarkan pilihan strategi. e. Bank memastikan uji coba BCP dan DRP dilakukan secara berkala dan telah memenuhi kebutuhan bisnis sesuai BIA. f. Bank telah melakukan tinjauan atas kecukupan BCP dan DRP pasca hasil uji coba dan pasca insiden/disrupsi.
			1.b.15. Pelindungan terhadap informasi Bank berdasarkan tingkat risiko keamanan informasi yang dapat diterima oleh Bank sesuai kebijakan keamanan, melakukan penerapan dan pemeliharaan peran keamanan informasi dan hak akses, serta melakukan pemantauan keamanan terhadap informasi Bank.	a. Bank mengelola keamanan pada level sistem aplikasi. b. Bank mengelola keamanan jaringan dan konektivitas. c. Bank mengelola keamanan *endpoint*, seperti pada laptop, *desktop*, *server*, perangkat jaringan atau perangkat aplikasi. d. Bank mengelola identitas pengguna dan *logical access*. e. Bank mengelola *physical access* ke aset TI. f. Bank mengelola *output devices* seperti *printer* dan *security tokens*. g. Bank mengelola kerentanan dan memantau infrastruktur untuk kejadian terkait keamanan.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			1.b.16. Aktivitas pemantauan kinerja layanan TI yang memadai.	a. Bank melakukan evaluasi kesesuaian TI dengan target kinerja yang disepakati minimal 1 (satu) kali dalam setahun. b. Bank memiliki mekanisme untuk melakukan evaluasi atas kecukupan kontrol internal. c. Bank mengevaluasi bahwa proses bisnis yang didukung TI patuh terhadap persyaratan perjanjian dan ketentuan peraturan perundang-undangan. d. Bank melakukan pemeriksaan independen terkait TI terhadap kepatuhan atas persyaratan internal, ketentuan peraturan perundang-undangan, dan tujuan strategis.
2.	Arsitektur	2.a. Arsitektur TI	2.a.1. Direksi memastikan arsitektur TI disusun selaras dengan strategi bisnis dan sesuai dengan kebutuhan bisnis Bank.	
			2.a.2. Direksi dan Komite Pengarah TI terlibat secara aktif dalam penyusunan arsitektur TI.	Direksi dan Komite Pengarah TI terlibat secara aktif dalam proses penyusunan arsitektur TI sesuai kewenangannya. Keterlibatan Direksi dan Komite Pengarah TI dilihat dari adanya rapat rutin sesuai kebutuhan Bank untuk pembahasan terkait penyusunan arsitektur TI termasuk perubahannya, apabila ada.
			2.a.3. Pengelolaan arsitektur TI yang memadai oleh Bank.	a. Arsitektur TI Bank disusun dengan mempertimbangkan faktor paling sedikit: 1) visi dan misi Bank; 2) rencana korporasi Bank; 3) proses dan kapabilitas bisnis Bank; 4) tata kelola TI Bank;

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				5) prinsip pengelolaan data, aplikasi, dan teknologi Bank; 6) ukuran dan kompleksitas bisnis Bank; 7) kemampuan permodalan Bank; 8) standar yang berlaku secara nasional maupun internasional; dan 9) ketentuan peraturan perundang-undangan. b. Arsitektur TI Bank mempertimbangkan kebijakan keamanan TI; c. Arsitektur TI Bank dievaluasi secara berkala untuk memastikan kesesuaian dengan kondisi terkini.
			2.a.4. Penyusunan arsitektur TI melibatkan partisipasi dari pemangku kepentingan (*stakeholders*) terkait.	
			2.a.5. Bank memiliki mekanisme permintaan dan pemberian informasi terkait arsitektur TI.	Bank memiliki mekanisme persetujuan, tata cara pemberian informasi, dan media komunikasi kepada pemangku kepentingan.
			2.a.6. Pelaksanaan strategi investasi TI, akuisisi TI, dan pengambilan keputusan bisnis TI selaras dengan arsitektur TI Bank serta RSTI.	a. Investasi TI dan akusisi TI Bank selaras dengan arsitektur TI Bank serta RSTI. b. Arsitektur TI Bank menjadi salah satu referensi dalam pengambilan keputusan bisnis terkait TI.
3.	Manajemen Risiko	3.a. Manajemen Risiko TI	3.a.1. Bank melakukan identifikasi risiko terkait penyelenggaraan TI secara memadai.	a. Bank melakukan identifikasi dan penilaian risiko TI dengan terlebih dahulu memastikan adanya *risk awareness* di seluruh lini Bank, yaitu: 1) *risk awareness* dari Direksi dan pejabat eksekutif;

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				2) pemahaman yang jelas mengenai *risk appetite* dari Bank; 3) pemahaman terhadap ketentuan peraturan perundang-undangan terkait TI; dan 4) transparansi dan integrasi terkait tanggung jawab mengenai risiko yang signifikan dari setiap aspek terkait penyelenggaraan TI. b. Bank memiliki pendekatan manajemen risiko yang terpadu atau terintegrasi untuk dapat melakukan identifikasi risiko terkait penyelenggaraan TI yang utama antara lain risiko operasional, risiko kepatuhan, risiko hukum, risiko reputasi, dan risiko stratejik. c. Bank melakukan identifikasi terhadap aset dan infrastruktur informasi vital, berikut risiko yang menyertainya. d. Risiko untuk aspek penyelenggaraan TI pada risiko operasional harus dikaji ulang bersamaan dengan risiko lain yang dimiliki Bank untuk menentukan profil risiko Bank secara keseluruhan.
			3.a.2. Bank melakukan pengukuran risiko terkait penyelenggaraan TI secara memadai.	a. Penilaian risiko untuk aspek TI pada risiko operasional oleh Bank harus dilakukan secara berkesinambungan sebagai suatu siklus dan paling sedikit memuat 4 (empat) langkah penting berikut: 1) melakukan pengumpulan data atau dokumen atas aktivitas terkait TI yang berpotensi menimbulkan atau meningkatkan risiko, baik dari kegiatan

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				yang sedang maupun yang akan berjalan termasuk namun tidak terbatas pada: a) hasil kaji ulang rencana strategis bisnis; b) hasil uji tuntas (*due diligence*) dan pemantauan terhadap kinerja pihak penyedia jasa TI; c) hasil kaji ulang atas laporan atau keluhan yang disampaikan oleh nasabah dan/atau pengguna TI pada *call center* dan/atau *helpdesk*; d) hasil penilaian sendiri (*self assessment*) yang dilakukan seluruh satuan kerja terhadap pengendalian yang dilakukan terkait TI; dan e) temuan audit terkait penyelenggaraan dan penggunaan TI; 2) melakukan analisis risiko berkaitan dengan dampak potensial dari setiap risiko, seperti *fraud* pada pemrograman, virus komputer, kegagalan sistem, bencana alam, dan kesalahan pemilihan teknologi yang digunakan; 3) menetapkan prioritas pengendalian dan langkah mitigasi yang didasarkan pada hasil penilaian risiko Bank secara keseluruhan. Bank membuat peringkat risiko berdasarkan kemungkinan kejadian dan besarnya dampak yang dapat ditimbulkan serta mitigasi risiko yang dapat dilakukan untuk menurunkan eksposur risiko tersebut; dan

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				4) melakukan pemantauan kegiatan pengendalian dan mitigasi yang telah dilakukan atas risiko yang diidentifikasi dalam periode penilaian risiko sebelumnya, yang antara lain mencakup rencana tindak lanjut perbaikan, kejelasan akuntabilitas dan tanggung jawab, sistem pelaporan, serta pengendalian kualitas termasuk bentuk pengawasan lain atau *compensating controls*. b. Bank memperhatikan signifikansi dampak risiko yang telah diidentifikasi oleh Bank terhadap kondisi Bank dan frekuensi terjadinya risiko. c. Bank memiliki dokumentasi risiko atau yang sering disebut sebagai *risk register* yang paling sedikit memuat: 1) penetapan aset, proses, produk, atau kejadian yang mengandung risiko; 2) pengukuran atau pemeringkatan kemungkinan kejadian dan dampak (*inherent risk assessment*); dan 3) langkah penanganan terhadap risiko potensial (*potential risk treatment*), misalnya *accept, control, avoid,* atau *transfer* (ACAT). d. Dalam dokumentasi penanganan terhadap risiko potensial (*potential risk treatment*), Bank memperhatikan antara lain *risk appetite* dari manajemen, fasilitas yang dapat digunakan sebagai *preventive control* atau *corrective control*, dan kesesuaian rencana mitigasi risiko dengan kondisi keuangan Bank. Dokumentasi

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				penanganan terhadap risiko potensial perlu dikinikan secara berkala.
			3.a.3. Bank menerapkan pemantauan risiko terkait penyelenggaraan TI secara memadai.	a. Bank melakukan pemantauan risiko terkait penyelenggaraan TI dengan mengevaluasi kesesuaian, kecukupan, dan efektivitas kinerja penyelenggaraan TI. Hal yang dapat menjadi cakupan dalam evaluasi antara lain: 1) hasil audit dan kajian terkait; 2) umpan balik yang diterima; 3) kebijakan, standar, dan prosedur serta penerapannya; 4) status dari tindakan preventif maupun korektif terkait risiko yang dihadapi Bank; 5) kelemahan dan ancaman, baik yang telah ada maupun yang masih berupa potensi; 6) hasil pengukuran atas efektivitas penyelenggaraan TI; 7) tindak lanjut atas hasil evaluasi sebelumnya; 8) perubahan kondisi yang mempengaruhi penyelenggaraan TI; dan 9) rekomendasi untuk perbaikan atau penyempurnaan. b. Tindak lanjut atas hasil evaluasi dapat dituangkan dalam bentuk keputusan maupun tindakan untuk meningkatkan efektivitas penyelenggaraan TI Bank, antara lain: 1) pengkinian profil risiko, pengukuran risiko, dan rencana penanganan risiko; 2) penyempurnaan kebijakan, standar, dan prosedur di bidang TI;

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				3) pemenuhan kebutuhan SDM; 4) penetapan dan pelaksanaan tindakan preventif dan korektif berdasarkan penilaian atas ketidaksesuaian yang ada maupun yang masih bersifat potensi, dengan mempertimbangkan skala prioritas; 5) pemantauan dan evaluasi atas pelaksanaan tindakan preventif dan korektif; dan 6) pendokumentasian hasil evaluasi dan tindak lanjut harus secara memadai.
			3.a.4. Bank menerapkan pengendalian risiko penyelenggaraan TI secara memadai.	a. Bank memperhatikan praktik pengendalian risiko penyelenggaraan TI secara keseluruhan dengan memperhatikan paling sedikit: 1) hasil penilaian risiko; 2) kriteria penanganan risiko dan rekomendasi bentuk penanganan risiko; dan 3) ketentuan peraturan perundang-undangan dan persyaratan hukum atau kontrak lainnya. b. Bank melakukan pengendalian risiko penyelenggaraan TI dengan: 1) menerapkan kebijakan, standar, dan prosedur, serta struktur organisasi termasuk alur kerja; 2) menerapkan pengendalian intern yang efektif yang dapat memitigasi risiko dalam proses TI; 3) menerapkan identifikasi persyaratan spesifik pengendalian intern yang

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				diperlukan dalam setiap kebijakan dan prosedur yang diterapkan; 4) menetapkan kebijakan, standar, dan prosedur sistem pengelolaan pengamanan informasi yang diperlukan Bank untuk melakukan pengamanan aset terkait penyelenggaraan TI termasuk data atau informasi; 5) melakukan evaluasi hasil kaji ulang dan pengujian atas DRP untuk setiap bagian operasional yang kritis; 6) menetapkan kebijakan dan prosedur mengenai penggunaan pihak penyedia jasa TI; 7) melakukan evaluasi terkait kemampuan penyedia jasa TI untuk menjaga tingkat keamanan paling sedikit sama atau lebih ketat dari yang diterapkan oleh pihak intern Bank baik dari sisi kerahasiaan, integritas data, dan ketersediaan informasi; 8) menggunakan asuransi sebagai upaya untuk melengkapi mitigasi potensi kerugian dalam penyelenggaraan TI; dan 9) melakukan kaji ulang secara berkala atas kebutuhan, cakupan, dan nilai asuransi yang ditutup.
			3.a.5. Bank memiliki sistem informasi manajemen risiko terkait penyelenggaraan TI yang memadai disampaikan secara rutin kepada Direksi.	a. Direksi memberikan arahan strategis atas ketersediaan sistem informasi manajemen risiko terkait penyelenggaraan TI yang dapat menghasilkan informasi yang diperlukan dalam

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				rangka mendukung peran dan fungsi manajemen secara efektif. b. Bank memastikan sistem informasi manajemen risiko terkait penyelenggaraan TI dapat: 1) memfasilitasi pengelolaan operasional bisnis Bank termasuk pelayanan kepada nasabah; 2) melakukan pencatatan dan mengumpulkan informasi secara objektif; 3) mendistribusikan data atau informasi ke berbagai satuan kerja yang sesuai, baik dari sisi jenis informasi, kualitas dan kuantitas informasi, maupun frekuensi dan waktu pengiriman laporan yang dibutuhkan; 4) meningkatkan efektivitas dan efisiensi komunikasi di Bank; 5) membantu Bank meningkatkan kepatuhan terhadap ketentuan peraturan perundang-undangan; dan 6) mendukung proses penilaian kinerja seluruh satuan kerja. c. Satuan kerja TI menetapkan kebijakan, prosedur, dan pengendalian manajemen pangkalan data (*database*) dan pembuatan laporan.
4.	Ketahanan dan Keamanan Siber	4.a. Tingkat maturitas keamanan siber	Sesuai dengan peringkat tingkat maturitas keamanan siber dengan mengacu pada ketentuan Otoritas Jasa Keuangan mengenai ketahanan dan keamanan siber bagi bank umum.	

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
5.	Teknologi	5.a. Adopsi TI secara bertanggung jawab	5.a.1. Bank memiliki kebijakan terkait adopsi TI.	Kebijakan terkait proses adopsi TI Bank memuat paling sedikit: a. identifikasi kebutuhan adopsi TI; b. kajian, studi kelayakan, dan strategi adopsi TI; c. budaya kerja yang mendukung inovasi pengembangan TI; dan d. kerja sama dengan pihak ketiga dalam implementasi adopsi TI.
			5.a.2. Bank melakukan studi kelayakan untuk adopsi TI.	Studi kelayakan yang dilakukan Bank memuat paling sedikit: a. potensi dari inovasi yang dihasilkan dari penggunaan TI bagi Bank dan nasabah; b. analisis berbagai aspek terkait implementasi TI antara lain risiko inheren, kesesuaian dengan arsitektur TI, keselarasan dengan strategi bisnis Bank, dampak hukum yang ditimbulkan dari pemanfaatan teknologi, regulasi terkait pemanfaatan teknologi baru, keselarasan dengan strategi TI Bank, penerapan praktik dan standar baik secara nasional maupun internasional, serta mitigasi atas risiko yang ditimbulkan; c. metode pengukuran dan pemantauan risiko yang muncul atas adopsi TI; dan d. perencanaan implementasi adopsi TI atau inovasi yang mencakup target, kebutuhan anggaran dan analisis tingkat pengembalian investasi, jangka waktu pengembangan, dan akuntabilitas dari adopsi TI.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			5.a.3. Bank memiliki strategi implementasi TI.	Strategi implementasi TI Bank memuat paling sedikit: a. kesesuaian adopsi TI dengan rencana strategis TI; b. metode implementasi TI antara lain *big bang*, *piloting* atau paralel; dan c. penggunaan sistem pendukung atau utama.
			5.a.4. Bank melakukan evaluasi atas adopsi TI.	Evaluasi atas adopsi TI mencakup: a. Bank memantau penerapan dan penggunaan TI untuk memastikan bahwa manfaat atau hasil yang diharapkan dari penggunaan TI terealisasi sesuai perencanaan Bank; b. Bank melakukan evaluasi atas TI yang diadopsi dengan periode dan cakupan tertentu. Yang dimaksud dengan cakupan tertentu seperti *performance testing*, *backtesting*, dan *benchmarking*. c. Bank mengidentifikasi pelajaran terpetik dari adopsi TI dan merekomendasikan tindak lanjut atas hasil evaluasi.
		5.b. Penggunaan Pihak Penyedia Jasa TI dalam Penyelenggaraan TI Bank (IT *outsourcing*)	5.b.1. Bank mengelola penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI Bank secara memadai termasuk yang diselenggarakan di luar wilayah Indonesia.	Pengelolaan pihak penyedia jasa TI dalam penyelenggaraan TI Bank secara memadai mencakup: a. Bank menerapkan manajemen risiko terkait penggunaan pihak penyedia jasa TI dengan mengacu pada penerapan proses manajemen risiko dalam penyelenggaraan TI. Dalam hal Bank menempatkan sistem elektronik pada pusat data dan/atau pusat pemulihan bencana di luar wilayah Indonesia,

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				Bank mempertimbangkan risiko negara (*country risk*); b. Bank menetapkan strategi terkait penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI Bank dan strategi tersebut telah sejalan dengan strategi TI dan strategi Bank secara keseluruhan; c. Bank menetapkan kebijakan dan prosedur yang memadai terkait penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI Bank; d. Bank menetapkan wewenang dan tanggung jawab yang jelas dari Direksi, Dewan Komisaris, Komite Pengarah TI, dan pejabat tertinggi yang memimpin satuan kerja TI serta pejabat pada setiap jenjang jabatan yang terkait dengan penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI Bank; e. Bank melakukan monitoring, pengawasan, dan evaluasi atas strategi dan kebijakan penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI Bank secara berkala.
			5.b.2. Bank melakukan proses manajemen risiko atas penggunaan pihak penyedia jasa TI secara memadai.	Bank melakukan proses manajemen risiko penggunaan pihak penyedia jasa TI, meliputi: a. tanggung jawab Bank atas penerapan manajemen risiko terkait penggunaan pihak penyedia jasa TI; b. penyediaan DRP yang teruji dan memadai; dan c. penetapan dan pemantauan atas pemenuhan persyaratan keamanan data dan/atau informasi dalam kebijakan dan prosedur intern serta dalam perjanjian kerja sama.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			5.b.3. Satuan Kerja TI/ satuan kerja terkait melakukan proses pemilihan pihak penyedia jasa TI dalam menentukan perusahaan penyedia jasa TI.	Bank dalam melakukan proses pemilihan pihak penyedia jasa TI, paling sedikit memperhatikan: a. kualifikasi dan kompetensi pihak penyedia jasa TI, termasuk SDM yang dimiliki; b. analisis biaya dan manfaat dengan mengikutsertakan satuan kerja penyelenggara TI Bank; c. prinsip kehati-hatian dan manajemen risiko; dan d. prinsip hubungan kerja sama secara wajar jika pihak penyedia jasa TI merupakan pihak terkait dengan Bank.
			5.b.4. Satuan kerja yang menjalankan fungsi TI memiliki standar isi perjanjian kerja sama dengan penyedia jasa TI.	Bank dalam melakukan hubungan kerja sama dengan pihak penyedia jasa TI memiliki perjanjian kerja sama dengan pihak penyedia jasa TI, dengan memperhatikan paling sedikit: a. kualifikasi dan kompetensi SDM yang dimiliki pihak penyedia jasa TI; b. komitmen pihak penyedia jasa TI dalam menjaga kerahasiaan data dan/atau informasi Bank serta nasabah Bank; c. komitmen pihak penyedia jasa TI untuk menyampaikan hasil audit TI secara berkala yang dilakukan auditor independen atas penyediaan jasa TI kepada Bank; d. pengalihan sebagian kegiatan atau subkontrak oleh pihak penyedia jasa TI dilakukan atas persetujuan Bank yang dibuktikan dengan dokumen tertulis;

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				e. mekanisme pelaporan kejadian kritis oleh pihak penyedia jasa TI kepada Bank; f. mekanisme penghentian perjanjian kerja sama jika terdapat penghentian perjanjian sebelum jangka waktu perjanjian berakhir; g. pemenuhan ketentuan peraturan perundang-undangan atas penyediaan jasa TI oleh pihak penyedia jasa TI; h. kesediaan pihak penyedia jasa TI untuk memenuhi kewajiban dan/atau persyaratan yang dimuat dalam perjanjian kerja sama; i. kesediaan pihak penyedia jasa TI untuk memberikan akses kepada Otoritas Jasa Keuangan dan/atau pihak lain yang berwenang untuk melakukan pemeriksaan terhadap kegiatan penyediaan jasa TI yang diberikan sesuai dengan ketentuan peraturan perundang-undangan; j. SLA; dan k. klausula yang menyatakan bahwa SLA tetap berlaku apabila terjadi perubahan kepemilikan baik pada Bank maupun penyedia jasa TI.
			5.b.5. Satuan kerja hukum atau konsultan hukum Bank meninjau ulang perjanjian kerja sama antara Bank dan pihak penyedia jasa TI sebelum ditandatangani kedua belah pihak.	Bank memiliki pegawai atau konsultan hukum yang kompeten untuk melakukan evaluasi atas perjanjian kerja sama yang terkait dengan penyediaan jasa TI.
			5.b.6. Bank melakukan koordinasi dan komunikasi yang efektif dengan pihak penyedia jasa TI mengenai aspek yang telah disepakati dalam perjanjian	a. Satuan Kerja TI atau satuan kerja terkait telah melakukan koordinasi dan komunikasi yang efektif dengan pihak penyedia jasa TI mengenai aspek yang telah disepakati dalam perjanjian

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			kerja sama untuk memastikan kedua belah pihak memiliki pemahaman yang sama dan pihak penyedia jasa TI memahami dan mematuhi hal yang diperjanjikan.	kerja sama untuk memastikan kedua belah pihak memiliki pemahaman yang sama dan pihak penyedia jasa TI memahami dan mematuhi hal yang diperjanjikan (misalnya ruang lingkup pekerjaan yang telah disepakati oleh kedua pihak telah termuat dalam *Term of Reference*/TOR). b. Bank telah melakukan alih pengetahuan (*transfer of knowledge*) terkait area pekerjaan yang dialihdayakan kepada pihak penyedia jasa TI melalui komunikasi yang efektif.
			5.b.7. Bank meninjau isi perjanjian kerja sama secara berkala untuk mengidentifikasi klausul yang perlu dinegosiasikan dan diperbaharui, disesuaikan dengan perubahan strategi bisnis Bank.	a. Terdapat dokumen tertulis atau laporan mengenai peninjauan klausul perjanjian dengan penyedia jasa TI secara berkala kepada Direksi. b. Bank melakukan koordinasi dan komunikasi yang efektif dengan pihak penyedia jasa TI mengenai penyesuaian perjanjian kerja sama untuk memastikan pemahaman kedua belah pihak atas penyesuaian klausul yang telah disepakati.
			5.b.8. Bank memiliki standar keamanan informasi yang memadai dalam kebijakan dan prosedur internal serta dalam perjanjian kerja sama dengan pihak penyedia jasa TI.	Bank memiliki standar keamanan informasi yang harus dipenuhi oleh penyedia jasa TI serta dalam perjanjian kerja sama dengan pihak penyedia jasa TI mencakup paling sedikit: a. keamanan informasi organisasi; b. pengelolaan akses; c. manajemen enkripsi dan sandi; d. keamanan jaringan dan operasi; e. aplikasi pemrograman antarmuka atau *application programming interfaces* (API);

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				f. lokasi data; g. kerahasiaan data pribadi konsumen; dan h. pemusnahan data/informasi Bank dan nasabah Bank pada saat perjanjian kerja sama berakhir.
			5.b.9. Bank memiliki prosedur pemantauan dan kontrol yang efektif untuk memantau kinerja pihak penyedia jasa TI dan mengelola risiko terkait kegiatan yang dialihdayakan, terutama jika penggunaan jasa TI yang bersifat material terkonsentrasi pada satu pihak penyedia jasa TI.	Bank dalam melakukan penilaian kinerja dan kepatuhan pihak penyedia jasa TI memperhatikan paling sedikit: a. pemantauan dan evaluasi keandalan pihak penyedia jasa TI secara berkala terkait kinerja, reputasi pihak penyedia jasa TI, dan kelangsungan penyediaan layanan; b. penerapan pengendalian TI secara memadai oleh pihak penyedia jasa TI, yang dibuktikan dengan hasil audit dan/atau penilaian yang dilakukan oleh pihak independen; dan c. pemenuhan tingkat layanan sesuai dengan SLA antara Bank dan pihak penyedia jasa TI.
			5.b.10. BCP Bank mencakup aspek terkait aktivitas penyelenggaraan jasa TI oleh pihak penyedia jasa TI dan dampaknya terhadap bisnis Bank.	a. Dalam penyusunan BCP, Bank telah memperhitungkan peran pihak peyedia jasa TI pada proses bisnis Bank serta mempertimbangkan *recovery time objectives* (RTO) dan *recovery point objectives* (RPO) pihak penyedia jasa TI. b. Bank mampu mengidentifikasi keterkaitan antar sistem dalam menjalankan proses bisnis. c. Bank melakukan pengujian BCP dengan mengikutsertakan pihak penyedia jasa TI.
			5.b.11. Bank melaksanakan audit secara berkala untuk menilai pelaksanaan	a. Rencana kerja tahunan audit intern mencakup pemeriksaan berkala terhadap proses dan

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			proses dan standar perjanjian kerja sama antara Bank dan pihak penyedia jasa TI serta dilakukan tindak lanjut atas temuan pemeriksaan.	standar perjanjian kerja sama dengan pihak penyedia jasa TI. b. Terdapat prosedur audit terhadap pihak penyedia jasa TI, baik dilakukan oleh audit intern Bank maupun pihak audit ekstern yang ditunjuk oleh Bank. c. Terdapat laporan hasil audit intern dan/atau ekstern terhadap proses dan standar perjanjian kerja sama dengan pihak penyedia jasa TI dan pelaksanaan audit telah berjalan dengan efektif dengan memperhatikan faktor sebagai berikut: 1) cakupan dan kedalaman audit telah meliputi seluruh proses dan standar perjanjian kerja sama dengan pihak penyedia jasa TI; 2) kompetensi auditor intern telah sesuai dengan kompleksitas aktivitas pihak penyedia jasa TI dalam penyelenggaraan TI Bank dan memiliki keahlian pada bidang yang diaudit; dan 3) kelengkapan dokumentasi atas cakupan, prosedur, temuan audit, dan tanggapan manajemen terhadap temuan audit. d. Satuan kerja audit intern melakukan monitoring terhadap tindak lanjut atas temuan pemeriksaan. e. Satuan kerja audit intern melakukan tindak lanjut dalam hal temuan pemeriksaan tidak ditindaklanjuti oleh manajemen.
			5.b.12. Bank memiliki rencana penghentian penggunaan pihak penyedia jasa TI	a. Bank memiliki kebijakan dan prosedur internal mengenai rencana penghentian penggunaan

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			(*exit plan*) apabila terjadi gangguan pada pihak penyedia jasa TI yang digunakan, melakukan penilaian atas keberlangsungan layanan dan data, dan melakukan pengujian/simulasi terhadap kelangsungan bisnis Bank.	pihak penyedia jasa TI dalam hal terdapat kondisi antara lain: 1) memburuknya kinerja penyelenggaraan TI oleh pihak penyedia jasa TI yang berpotensi menimbulkan dan/atau mengakibatkan dampak yang signifikan pada kegiatan usaha Bank; 2) pihak penyedia jasa TI menjadi insolven, dalam proses menuju likuidasi, atau dipailitkan oleh pengadilan; 3) terdapat pelanggaran oleh pihak penyedia jasa TI terhadap ketentuan peraturan perundang-undangan mengenai rahasia bank dan pelindungan data pribadi; 4) terdapat kondisi yang menyebabkan Bank tidak dapat menyediakan data yang diperlukan dalam rangka pengawasan oleh Otoritas Jasa Keuangan; dan 5) hasil penilaian ulang materialitas menunjukkan bahwa penyediaan jasa TI tidak berjalan dengan efektif. b. Bank melakukan penilaian atas ketahanan dan keberlangsungan layanan dan data terkait dengan kegiatan yang diserahkan kepada pihak penyedia jasa TI serta pengujian atau simulasi terhadap kelangsungan bisnis Bank dalam hal akan dilakukan penghentian penggunaan pihak penyedia jasa TI. c. Seluruh proses penghentian penggunaan pihak penyedia jasa TI telah didokumentasikan.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
6.	Data	6.a. Tata Kelola Data	6.a.1. Bank memiliki kebijakan mengenai pembagian tugas dan kewenangan pengelolaan data.	a. Pengelolaan data mencakup aktivitas: 1) penyusunan kebijakan dan standar pengelolaan data; 2) pengelolaan kualitas data; dan 3) pelaksanaan kegiatan operasional pengelolaan data. b. Bank memiliki kebijakan mengenai tugas dan tanggung jawab dalam pengelolaan data. c. Bank menetapkan pembagian tugas dan wewenang pengelolaan data sesuai kompleksitas usaha Bank dengan memperhatikan kepemilikan dan kepengurusan data. d. Direksi dan Dewan Komisaris Bank memahami dan secara aktif menerapkan prinsip pemrosesan data dalam rangka pelindungan data di Bank, serta bertanggung jawab atas kepatuhan terhadap prinsip-prinsip tersebut. e. Bank menetapkan kebijakan pengelolaan data secara memadai.
			6.a.2. Bank melakukan pengembangan dan upaya menjaga dan/atau memperbaiki kualitas data.	a. Bank menetapkan standar, persyaratan, dan spesifikasi penerapan kontrol kualitas data. b. Bank melakukan identifikasi permasalahan terkait kualitas data. c. Bank melakukan upaya peningkatan kualitas data yang diidentifikasi. d. Bank melakukan evaluasi tingkat kualitas data.
			6.a.3. Bank memiliki kebijakan dan prosedur pengelolaan data.	a. Bank memiliki kebijakan data yang memuat paling sedikit prinsip dan tujuan Bank dalam pengelolaan data serta aturan dasar yang mengatur pembuatan, akuisisi, keamanan,

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				kualitas, dan penggunaan data dan informasi, termasuk klasifikasi data, serta pemrosesan data nasabah dan calon nasabah. b. Bank menetapkan klasifikasi data berdasarkan kritikalitas dan sensitivitas dari masing-masing jenis data. c. Bank memiliki kebijakan kontrol akses pengelolaan data sesuai klasifikasi data. d. Bank memiliki kebijakan dan strategi pelindungan data sesuai peraturan perundang-undangan mengenai pelindungan data pribadi. e. Bank memiliki kebijakan dan prosedur pemrosesan data yang memuat antara lain: 1) pemrosesan data secara adil dan transparan, seperti data nasabah/calon nasabah diperoleh dengan cara yang sah serta dipergunakan secara sah dan tidak dipergunakan untuk perbuatan melanggar hukum; 2) proses pengumpulan data nasabah/calon nasabah; 3) informasi yang diberikan kepada individu dan pelaksanaan hak individu; 4) langkah teknis pengelolaan keamanan data; 5) prosedur penyelesaian perselisihan dengan nasabah terkait akurasi pencatatan data nasabah; 6) pengelolaan dokumentasi setiap tahap pemrosesan data; 7) pelaporan kebocoran data nasabah; dan 8) analisis dampak pemrosesan data.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			6.a.4. Bank melakukan pengelolaan data secara memadai.	a. Bank memiliki arsitektur data sebagai bagian dari arsitektur TI. b. Bank menerapkan pelindungan data dan informasi, mencakup: 1) penetapan standar pengamanan data sesuai dengan klasifikasi data; dan 2) implementasi kontrol dan prosedur pengamanan data dan informasi. c. Bank mengelola integrasi dan interoperabilitas data. Integrasi data dan interoperabilitas menggambarkan proses terkait pergerakan dan konsolidasi data di dalam dan antara penyimpanan data, aplikasi, dan organisasi. Integrasi merupakan penggabungan data ke dalam bentuk yang konsisten, baik fisik maupun virtual. Interoperabilitas data merupakan kemampuan beberapa sistem untuk berkomunikasi. Penerapan integrasi dan interoperabilitas data memastikan Bank dapat memperoleh data dimanapun, kapanpun, dan dalam bentuk apapun sesuai kebutuhan. d. Bank menerapkan pengelolaan data yang meliputi akuisisi, pembuatan, penyimpanan, pemrosesan, penggunaan, retensi, dan pemusnahan data. e. Bank menerapkan pengelolaan referensi dan manajemen data master. Yang dimaksud pengelolaan referensi dan manajemen data master adalah berbagi data informasi lintas domain bisnis untuk memenuhi tujuan organisasi, mengurangi risiko yang terkait dengan redundansi data, memastikan kualitas

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				data terjaga, dan mengurangi biaya integrasi data. f. Bank mengelola *data warehouse* dan sistem aplikasi *Business Intelligence.* g. Bank melakukan kegiatan perencanaan, implementasi, dan pengendalian untuk memungkinkan akses data kualitas tinggi dan/atau metadata terintegrasi. h. Bank melakukan pengolahan berbagai jenis data untuk memperoleh informasi yang dapat memberikan nilai tambah terutama untuk pengambilan keputusan.
			6.a.5. Bank melakukan pengelolaan pangkalan data secara optimal, baik dari sisi desain dan dukungan penyimpanan data.	a. Bank menerapkan pengelolaan teknologi pangkalan data secara memadai, mencakup: 1) perencanaan mengenai teknologi pangkalan data; 2) pengelolaan teknologi pangkalan data; dan 3) proses evaluasi. b. Bank menerapkan pengelolaan operasional pangkalan data secara memadai, paling sedikit: 1) identifikasi kebutuhan terkait pangkalan data, kebutuhan sistem penyimpanan *file*, kebutuhan penambahan kapasitas penyimpanan, kepatuhan terhadap regulasi, metode dan *tools* yang sesuai untuk akses data; 2) merencanakan kelangsungan usaha (*business continuity*) apabila terjadi bencana yang berdampak pada sistem penyimpanan data. Bank memastikan rencana pemulihan diterapkan pada

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				seluruh pangkalan data dan *server* pangkalan data, mencakup skenario yang dapat mengakibatkan hilangnya atau rusaknya data termasuk membuat cadangan pangkalan data dan pengujian pemulihan data secara berkala; dan 3) melakukan pengujian terhadap pangkalan data.
		6.b. Pelindungan Data Pribadi	6.b.1. Bank melakukan pengembangan dan/atau penyelenggaraan TI dengan mempertimbangkan aspek pelindungan data pribadi.	Bank memastikan keamanan data pribadi yang diprosesnya dalam pengembangan dan/atau penyelenggaraan TI, dengan melakukan: a. penyusunan dan penerapan langkah untuk melindungi data pribadi dari gangguan pemrosesan data pribadi yang bertentangan dengan ketentuan peraturan perundang-undangan; dan b. penentuan tingkat keamanan data pribadi dengan memperhatikan sifat dan risiko dari data pribadi yang harus dilindungi dalam pemrosesan data pribadi.
			6.b.2. Proses identifikasi dasar pemrosesan data pribadi nasabah dan/atau calon nasabah dilakukan secara memadai.	Dasar pemrosesan data pribadi meliputi: a. persetujuan dari nasabah dan/atau calon nasabah untuk tujuan tertentu sebagai dasar pemrosesan data pribadi, yang dilakukan sesuai dengan ketentuan peraturan perundang-undangan mengenai pelindungan data pribadi; b. pemenuhan kewajiban perjanjian dalam hal nasabah dan/atau calon nasabah merupakan salah satu pihak atau untuk memenuhi

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				permintaan nasabah dan/atau calon nasabah pada saat akan melakukan perjanjian; c. pemenuhan kewajiban hukum dari pihak yang melakukan pengendalian data pribadi sesuai dengan ketentuan peraturan perundang-undangan; d. pemenuhan pelindungan kepentingan vital nasabah dan/atau calon nasabah; e. pelaksanaan tugas dalam rangka kepentingan umum, pelayanan publik, atau pelaksanaan kewenangan pihak yang melakukan pengendalian data pribadi berdasarkan peraturan perundang-undangan; dan f. pemenuhan kepentingan yang sah lainnya dengan memperhatikan tujuan, kebutuhan, dan keseimbangan kepentingan pihak yang melakukan pengendalian data pribadi dan hak nasabah dan/atau calon nasabah.
			6.b.3. Proses permintaan persetujuan nasabah dalam rangka pemrosesan data pribadi nasabah dan/atau calon nasabah dilakukan secara memadai.	a. Bank memastikan adanya persetujuan nasabah dan/atau calon nasabah sebagai dasar hukum untuk pemrosesan data. b. Permintaan persetujuan Bank tidak berupa persetujuan yang bersifat otomatis tanpa ada instruksi dari nasabah, seperti penggunaan kotak centang (*tick box*) yang telah dicentang sebelumnya atau jenis persetujuan otomatis lainnya. c. Permintaan persetujuan disusun dalam bahasa yang jelas, sederhana dan mudah dimengerti.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				d. Bank menginformasikan kepada nasabah tujuan permintaan data pribadi nasabah oleh Bank. e. Bank memberikan opsi pilihan persetujuan untuk setiap tujuan dan jenis pemrosesan data pribadi yang berbeda. f. Bank memberikan informasi legalitas dari pemrosesan data pribadi nasabah sesuai dengan ketentuan perundang-undangan. g. Bank memberikan informasi hak nasabah untuk menarik persetujuan yang telah diberikan kepada Bank. h. Bank memastikan bahwa nasabah memiliki hak untuk menolak pemberian persetujuan. i. Bank tidak menjadikan pemberian persetujuan atas hal-hal yang tidak terkait langsung dengan nasabah sebagai prasyarat pemberian layanan Bank. j. Bank melakukan penghapusan data setelah masa retensi data pribadi (hanya untuk kepentingan *maintenance*/audit/rekam jejak) berakhir sesuai dengan peraturan perundang-undangan mengenai pelindungan data pribadi.
			6.b.4. Proses rekam dan pengelolaan persetujuan nasabah dalam rangka pemrosesan data pribadi dilakukan secara memadai.	a. Bank memelihara catatan mengenai kapan dan bagaimana persetujuan nasabah dan/atau calon nasabah diperoleh. b. Bank menyimpan catatan persis sesuai dengan yang disampaikan nasabah dan/atau calon nasabah saat pemberian persetujuan. c. Bank meninjau persetujuan secara berkala melalui pemeriksaan khusus atau sistem

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				pencatatan secara periodik untuk memastikan bahwa hubungan, pemrosesan, dan tujuannya tidak berubah. d. Bank memiliki proses untuk memperbarui persetujuan pada selang waktu yang sesuai dengan kebutuhan Bank untuk memastikan konsistensi antara persetujuan nasabah, pengumpulan, pemrosesan, dan tujuan pemrosesan. e. Bank memberikan kemudahan untuk nasabah dan/atau calon nasabah untuk menarik persetujuan kapanpun dan mempublikasikan cara melakukannya serta bertindak atas penarikan persetujuan sesegera mungkin.
			6.b.5. Kerja sama antara Bank dan pihak ketiga untuk aktivitas pemrosesan data pribadi didukung oleh perjanjian kerja sama yang memadai.	a. Perjanjian kerja sama Bank dengan pihak ketiga paling sedikit memuat: 1) ruang lingkup dan durasi pemrosesan; 2) sifat dan tujuan pemrosesan; 3) jenis data pribadi dan kategori data nasabah; dan 4) kewajiban dan hak pengendali data. b. Cakupan perjanjian kerja sama Bank dengan pihak ketiga selaku pemroses data pribadi: 1) pemroses hanya boleh bertindak berdasarkan instruksi tertulis dari Bank, kecuali diharuskan oleh hukum untuk bertindak tanpa instruksi tersebut; 2) pemroses memastikan bahwa orang yang memproses data pribadi tunduk pada kewajiban kerahasiaan;

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				3) pemroses mengambil tindakan yang tepat untuk memastikan keamanan pemrosesan. 4) pemroses dapat menggunakan subpemroses dengan persetujuan dari Bank berdasarkan perjanjian tertulis; 5) pemroses membantu Bank dalam menyediakan akses data pribadi dan mengizinkan nasabah menggunakan haknya; 6) pemroses membantu Bank dalam memenuhi kewajiban terkait keamanan pemrosesan, pemberitahuan pelanggaran data pribadi, dan penilaian dampak pelindungan data pribadi; 7) pemroses menghapus atau mengembalikan semua data pribadi ke Bank seperti yang sesuai perjanjian kerja sama; 8) pemroses tunduk pada audit dan inspeksi, memberikan seluruh informasi yang diperlukan Bank untuk memastikan bahwa pemroses dan Bank memenuhi peraturan mengenai pelindungan data pribadi, dan segera memberi tahu Bank jika diminta untuk melakukan sesuatu yang melanggar peraturan mengenai pelindungan data pribadi; dan 9) tidak terdapat klausul dalam perjanjian kerja sama yang menyatakan bahwa pemroses bebas dari tanggung jawab dan kewajiban langsungnya sendiri.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			6.b.6. Proses identifikasi, dokumentasi, dan evaluasi tujuan proses pengumpulan dan pemrosesan data pribadi dilakukan secara memadai.	a. Bank melakukan identifikasi tujuan pemrosesan data pribadi. b. Bank mendokumentasikan tujuan dari pemrosesan data pribadi. c. Bank mencantumkan tujuan dari pemrosesan data pribadi dalam informasi kepada nasabah/calon nasabah. d. Dalam hal Bank akan menggunakan data pribadi nasabah untuk tujuan lain, Bank melakukan identifikasi apakah pemrosesan data pribadi selaras dengan tujuan awal atau telah mendapat persetujuan dari nasabah untuk tujuan lain. e. Bank memiliki prosedur untuk memastikan data pribadi yang dibutuhkan sesuai dengan tujuan.
			6.b.7. Bank melakukan pemrosesan data pribadi secara akurat, lengkap, dan dapat dipertanggungjawabkan.	a. Bank memiliki prosedur untuk memastikan akurasi data pribadi yang dikumpulkan dan Bank merekam sumber perolehan data pribadi yang dimiliki. b. Bank memiliki prosedur terkait proses perubahan data pribadi. c. Bank memiliki data jejak audit (*audit trail*) untuk mengetahui kapan perubahan data pribadi dilakukan. d. Bank memberikan hak kepada nasabah untuk melengkapi, memperbarui, memperbaiki, dan/atau menghapus data pribadi milik nasabah.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			6.b.8. Prosedur penanganan permintaan nasabah untuk pengkinian, perbaikan, penghapusan, atau pemusnahan data pribadi nasabah dilakukan secara memadai.	a. Bank memiliki kebijakan mengenai pengkinian, perbaikan, penghapusan, dan pemusnahan data pribadi nasabah. b. Bank memiliki kebijakan atau prosedur penolakan atas permintaan perubahan data pribadi nasabah sesuai peraturan perundang-undangan. c. Bank memiliki prosedur untuk menginformasikan kepada nasabah dalam hal Bank melakukan pengkinian, perbaikan, penghapusan, dan pemusnahan data pribadi nasabah.
			6.b.9. Proses retensi data pribadi dilakukan secara memadai.	a. Bank mengklasifikasikan data pribadi nasabah sesuai dengan pengelolaan dan peruntukannya. b. Bank memiliki dasar pertimbangan penetapan jangka waktu retensi data pribadi nasabah. c. Bank memiliki kebijakan periode retensi data pribadi. d. Bank memiliki prosedur untuk mereviu informasi secara berkala dan menghapus data pribadi yang tidak lagi dibutuhkan. e. Bank memiliki prosedur untuk menghapus data pribadi nasabah sesuai permintaan nasabah. f. Bank mengidentifikasi kebutuhan data pribadi yang disimpan untuk riset dan statistik.
			6.b.10. Proses pengamanan data pribadi dilakukan secara memadai.	a. Bank memiliki kebijakan keamanan data pribadi dan informasi. b. Bank melakukan peninjauan secara berkala atas penerapan kebijakan keamanan data pribadi dan informasi.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				c. Bank menerapkan keamanan data pribadi dan informasi sesuai dengan kerangka atau standar tertentu. d. Bank melakukan enkripsi dan/atau pseudonimisasi atas data pribadi nasabah sesuai kebutuhan. e. Bank melakukan pengujian sistem pengamanan data pribadi secara berkala untuk mengukur dan memastikan efektivitas keamanan data pribadi.
			6.b.11. Proses penilaian dampak atas penerapan pelindungan data pribadi dilakukan secara memadai.	a. Bank melakukan identifikasi kriteria data pribadi yang berisiko tinggi sesuai dengan kriteria yang diatur dalam peraturan perundang-undangan mengenai pelindungan data pribadi. b. Bank melakukan penilaian dampak pelindungan data pribadi nasabah dalam hal pemrosesan data pribadi memiliki potensi risiko tinggi terhadap nasabah.
			6.b.12. Proses dokumentasi aktivitas pemrosesan data pribadi dilakukan secara memadai.	a. Bank mendokumentasikan aktivitas pemrosesan data pribadi oleh Bank. b. Bank mendokumentasikan informasi yang diperlukan untuk pemberitahuan privasi, catatan persetujuan, perjanjian kerja sama antara Bank dan pihak ketiga, lokasi data pribadi, laporan penilaian dampak atas penerapan pelindungan data, dan catatan pelanggaran data pribadi. c. Bank mendokumentasikan kegiatan pemrosesan data pribadi oleh Bank dalam bentuk elektronik sehingga Bank dapat

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				menambah, menghapus, dan mengubah informasi dengan mudah.
			6.b.13. Prosedur pemberian informasi pemrosesan data kepada nasabah yang memadai.	a. Bank memberikan informasi kepada nasabah antara lain mengenai kejelasan identitas, dasar kepentingan hukum, tujuan permintaan, dan penggunaan data pribadi nasabah. b. Bank memberikan informasi tersebut secara ringkas, transparan, mudah diakses, serta menggunakan bahasa sederhana dan jelas dalam bentuk yang sesuai dengan struktur dan/atau format yang lazim digunakan atau dapat dibaca oleh sistem elektronik.
			6.b.14. Prosedur pemberian akses data pribadi dan informasi kepada nasabah yang memadai.	a. Bank memiliki kebijakan mengenai permintaan akses data pribadi yang dikelola oleh Bank. b. Bank memilliki mekanisme untuk melakukan verifikasi hak akses terhadap data pribadi. c. Bank memahami kondisi yang memungkinkan Bank untuk menolak permintaan akses data pribadi dan informasi sesuai peraturan perundang-undangan.
			6.b.15. Proses penanganan permintaan nasabah untuk pembatasan pemrosesan data pribadi milik nasabah dilakukan secara memadai.	a. Bank memiliki kebijakan penanganan permintaan nasabah untuk pembatasan pemrosesan data pribadi. b. Bank memiliki kebijakan terkait batas waktu untuk menanggapi permintaan pembatasan pemrosesan data pribadi sesuai dengan peraturan perundang-undangan. c. Bank telah memiliki prosedur untuk membatasi pemrosesan data pribadi di sistem Bank dan memiliki prosedur untuk menginformasikan

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				kepada pihak ketiga selaku penerima data pribadi terkait pembatasan pemrosesan data pribadi milik nasabah.
			6.b.16. Proses penanganan permintaan nasabah untuk mentransfer data pribadi milik nasabah ke pihak ketiga dilakukan secara memadai.	a. Bank memiliki kebijakan penanganan permintaan nasabah untuk mentransfer data pribadi milik nasabah kepada pihak ketiga. b. Bank memiliki proses untuk penanganan permintaan nasabah untuk mentransfer data pribadi milik nasabah kepada pihak ketiga dengan menggunakan metode yang aman untuk mengirimkan data pribadi. c. Bank memiliki kebijakan atau prosedur penolakan atas permintaan nasabah untuk mentransfer data pribadi milik nasabah ke pihak ketiga.
			6.b.17. Proses penanganan penolakan nasabah atas pemrosesan data pribadi dilakukan secara memadai.	a. Bank memiliki kebijakan atau prosedur bagi nasabah untuk mengajukan keberatan atas pemrosesan data pribadi secara otomatis. b. Bank memiliki kebijakan untuk menolak keberatan nasabah disertai dengan informasi dan alasan penolakan. c. Bank menginformasikan mengenai hak nasabah dan/atau calon nasabah untuk menolak pemrosesan data pribadi dalam pemberitahuan privasi Bank dan media lainnya. d. Bank memiliki prosedur untuk menghapus atau menghentikan pemrosesan data pribadi.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
		6.c. Transfer Data	6.c.1. Bank memiliki kebijakan, prosedur, dan standar mengenai pengendalian pertukaran atau transfer data dan infomasi yang memadai.	Bank memastikan bahwa kebijakan, prosedur, dan standar pertukaran atau transfer data dan informasi mencakup paling sedikit: a. jenis data nasabah untuk pertukaran atau transfer data dan informasi; b. persetujuan nasabah untuk pertukaran atau transfer data dan informasi; c. mekanisme permintaan informasi oleh pihak ekstern dan pemberian informasi kepada pihak ekstern; d. mekanisme transfer data di internal Bank kepada pihak selain pemilik data; e. media yang diperkenankan untuk dipergunakan dalam pertukaran data dan informasi; f. pengamanan jaringan komunikasi dan transmisi data dan informasi termasuk penggunaan enkripsi; g. hak nasabah dalam transaksi yang melibatkan pertukaran atau transfer data dan informasi; dan h. pembagian tanggung jawab pihak yang terlibat dalam pertukaran atau transfer data atas risiko kebocoran data nasabah.
			6.c.2. Bank memiliki perjanjian kerja sama dengan pihak ketiga dalam rangka pertukaran atau transfer data.	Perjanjian pertukaran atau transfer data paling sedikit memuat aspek: a. pihak pengendali data pada setiap tahap pertukaran atau transfer data; b. tujuan pertukaran atau transfer data yang meliputi:

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				1) tujuan khusus dan alasan dibutuhkannya pertukaran atau transfer data; dan 2) keuntungan yang diperoleh dari pertukaran atau transfer data, tidak digunakan untuk peruntukan selain yang tercantum dalam perjanjian; c. pihak ketiga lain yang mungkin terlibat dalam pertukaran atau transfer data; d. data yang akan dipertukarkan; e. prosedur pemenuhan hak subjek data seperti akses subjek data terhadap data yang dilakukan proses pertukaran atau transfer data; f. pengaturan teknis pertukaran atau transfer data (contoh: standar data, standar keamanan informasi, prosedur permintaan akses data, penghentian pertukaran data, SLA pengiriman data, dan penanganan masalah kegagalan perpindahan data); dan g. pengaturan perjanjian kerahasiaan (*nondisclosure agreement*) bahwa data yang disampaikan kepada pihak ketiga tidak akan diteruskan kepada pihak lain dan tidak digunakan untuk peruntukan lain selain yang tercantum dalam perjanjian tanpa persetujuan Bank.
			6.c.3. Bank menerapkan pengamanan atas data nasabah yang dipertukarkan sesuai dengan klasifikasi data.	a. Bank menerapkan serangkaian langkah teknis untuk memastikan keamanan jaringan komunikasi yang dipergunakan. b. Bank melakukan enkripsi atas data yang dipertukarkan.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				c. Bank menerapkan standar integritas data. d. Bank menerapkan metode autentikasi. e. Bank menerapkan standar otorisasi.
			6.c.4. Bank menerapkan pelindungan data pribadi nasabah dalam pertukaran data pribadi nasabah.	a. Bank memperoleh persetujuan nasabah untuk dapat mentransfer data pribadinya. b. Bank pelaksana transfer data pribadi nasabah dan Bank penerima transfer data pribadi nasabah mematuhi peraturan perundang-undangan mengenai pelindungan data pribadi. c. Bank hanya dapat melakukan transfer data pribadi nasabah kepada pihak lain dalam wilayah hukum Negara Republik Indonesia. d. Bank dapat melakukan transfer data pribadi nasabah kepada pihak lain di luar wilayah negara Republik Indonesia apabila negara penerima transfer data pribadi memiliki tingkat pelindungan data pribadi yang setara atau lebih tinggi dari yang diatur dalam ketentuan peraturan perundang-undangan mengenai pelindungan data pribadi. e. Dalam hal poin d tidak terpenuhi, Bank memastikan terdapat kebijakan pelindungan data pribadi yang memadai dan bersifat mengikat. f. Dalam hal huruf d dan huruf e tidak terpenuhi, Bank wajib mendapatkan persetujuan nasabah.
7.	Kolaborasi	7.a. Kerja Sama Kemitraan	7.a.1. Direksi dan Dewan Komisaris menetapkan strategi dan kebijakan terkait kemitraan.	a. Penerapan strategi terkait kemitraan telah dimuat dalam RSTI dan/atau rencana bisnis Bank. b. Penerapan strategi dan kebijakan terkait kemitraan telah sesuai dengan visi, misi,

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				strategi bisnis, dan *risk appetite* Bank, serta kecukupan permodalan Bank. c. Penerapan strategi dan kebijakan terkait kemitraan telah mempertimbangkan faktor analisis biaya dan manfaat. d. Penerapan strategi dan kebijakan kemitraan telah memperhatikan kecukupan dan kesiapan SDM Bank yang dapat dibuktikan dengan telah memiliki tugas dan tanggung jawab atas unit atau satuan kerja yang terlibat dalam proses kerja sama kemitraan.
			7.a.2. Perjanjian kemitraan oleh Bank memiliki standar baku perjanjian kerja sama kemitraan.	Standar baku perjanjian kerja sama kemitraan oleh Bank paling sedikit: a. memenuhi prinsip kehati-hatian; b. memperhatikan analisis biaya dan manfaat; c. memenuhi prinsip hubungan kerja sama secara wajar; d. memenuhi ketentuan peraturan perundang-undangan; e. terdapat klausul bahwa masing-masing pihak akan bertanggung jawab atas keamanan sistemnya sendiri; f. terdapat klausul bahwa mitra akan menyampaikan informasi kepada Bank sesegera mungkin setelah mengetahui setiap pelanggaran keamanan di sistem mitra yang berpotensi berdampak terhadap layanan Bank; g. dalam hal mitra memberikan layanan berupa penerusan instruksi nasabah, mitra hanya berkomunikasi dengan Bank berdasarkan

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				instruksi nasabah yang telah disetujui nasabah; h. mitra, termasuk pihak ketiga dari mitra, bertanggung jawab untuk menerapkan proses pencegahan penipuan atau penyimpangan (*fraud*); i. Bank dan/atau mitra bertanggung jawab atas kekurangan pelayanan dalam pelaksanaan transaksi karena kesalahan atau kelalaiannya; j. mitra bertanggung jawab atas segala penyalahgunaan merek Bank dan untuk setiap aktivitas yang menyebabkan kerusakan reputasi Bank, termasuk namun tidak terbatas pada penipuan, penyalahgunaan API, kesalahan penyajian produk dan layanan Bank, keamanan, atau layanan yang kurang memuaskan terus-menerus kepada konsumen; k. mitra telah memiliki asuransi yang memadai untuk menutupi seluruh kewajibannya selama jangka waktu perjanjian kerja sama; l. Bank dapat melakukan pemeriksaan/ audit/investigasi ketika terdapat indikasi pelanggaran; m. Bank tidak dibebankan tanggung jawab dan/atau tidak dianggap melanggar perjanjian kemitraan: 1) atas pelanggaran perjanjian kemitraan atau kegagalan Bank untuk menyediakan akses, jika hal tersebut disebabkan oleh kegagalan mitra dalam memenuhi kewajibannya berdasarkan perjanjian kemitraan; dan

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				2) atas kehilangan dan/atau kerusakan yang disebabkan secara langsung atau tidak langsung oleh tindakan atau kelalaian pihak ketiga yang bekerja sama dengan mitra; dan n. Bank dan mitra memiliki narahubung yang bertugas sebagai kontak utama untuk segala hal yang berkaitan dengan perjanjian kerja sama.
			7.a.3. Bank memiliki kebijakan terkait pengujian kelayakan mitra.	Kebijakan antara lain memuat pelaksanaan kemitraan terkait: a. kondisi keuangan mitra (termasuk kemampuan mitra untuk memenuhi kewajiban yang mungkin timbul dari penyediaan layanan oleh mitra); b. mitra memiliki semua izin yang diperlukan untuk kegiatan yang ingin dilakukan; c. tindakan dan kontrol keamanan mitra, termasuk kebijakan keamanan siber dan pemantauannya; d. mitra memiliki BCP dan DRP; e. operasi dan kontrol manajemen risiko keamanan yang dimiliki mitra, khususnya terkait dengan pelindungan data pribadi (misalnya, pelatihan pegawai dalam undang-undang dan praktik kerahasiaan data, praktik penyimpanan dan penghancuran data, langkah untuk menghindari pengumpulan data pribadi yang berlebihan); dan

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				f. tidak memiliki reputasi buruk dan tidak melakukan kegiatan yang melanggar hukum atau ketentuan.
			7.a.4. Bank melakukan pemantauan dan evaluasi hubungan kerja sama dengan mitra.	Bank melakukan pemantauan dan evaluasi hubungan kerja sama dengan mitra untuk menentukan tindakan tertentu dalam hal: a. mitra tidak lagi memenuhi kriteria kelayakan; b. mitra telah melanggar salah satu ketentuan yang tercantum pada bagian "autentikasi dan persetujuan nasabah"; c. mitra menggunakan API untuk tujuan yang tidak diungkapkan kepada Bank; d. mitra menyatakan atau mengakui kepailitannya atau tidak mampu membayar utang pada saat jatuh tempo atau pada saat diajukannya proses kepailitan; e. mitra memasukkan *malware* yang dapat mengganggu sistem Bank; f. mitra melakukan penawaran layanan dengan cara yang dapat merusak reputasi Bank; g. mitra menggunakan data nasabah selain untuk tujuan yang diizinkan/diperjanjikan; h. terdapat dugaan pelanggaran keamanan oleh mitra; dan/atau i. terdapat dugaan pelanggaran perjanjian kerja sama oleh mitra.
			7.a.5. Bank memastikan penerapan metode autentikasi secara aman bagi nasabah yang mengakses layanan Bank melalui mitra.	Dalam rangka melakukan autentikasi terhadap nasabah yang mengakses layanan Bank melalui mitra, Bank paling sedikit: a. menerapkan faktor autentikasi multifaktor;

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				b. memiliki kendali atas proses autentikasi; c. memastikan mitra tidak menyimpan data kredensial konsumen (menggunakan *interface* mitra); d. bersama dengan mitra memastikan keamanan proses autentikasi melalui penggunaan perangkat atau saluran terpisah dari perangkat atau saluran milik mitra untuk menyelesaikan autentikasi nasabah; e. memproses permintaan data nasabah yang diminta oleh mitra setelah Bank melakukan autentikasi nasabah dan mitra; dan f. memberikan data yang diperlukan kepada mitra untuk layanan yang diakses oleh nasabah setelah Bank meyakini bahwa proses autentikasi telah berjalan sesuai prosedur yang telah disepakati.
			7.a.6. Bank menentukan dan mendokumentasikan standar teknis interkoneksi antara mitra dan Bank.	a. Bank menerapkan dan mendokumentasikan standar teknis interkoneksi yang mencakup protokol komunikasi, struktur dan format data, metode autentikasi, metode otorisasi, metode enkripsi, dan persyaratan pengelolaan akses, termasuk manajemen pengelolaan kunci (*key management*). b. Bank memberitahukan mitra apabila terjadi perubahan di standar teknis interkoneksi.
		7.b. Penyediaan Jasa TI oleh Bank	7.b.1. Penyediaan jasa TI oleh Bank sesuai ketentuan peraturan perundang-undangan dan menerapkan aspek kehati-hatian.	a. Bank hanya dapat menyediakan jasa TI kepada lembaga jasa keuangan lain yang diawasi oleh Otoritas Jasa Keuangan dan/atau di luar wilayah Indonesia yang diawasi otoritas

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				pengawas dan pengatur lembaga jasa keuangan setempat. b. Bank memenuhi persyaratan penyediaan jasa TI tidak menjadi salah satu kegiatan pokok Bank. c. Bank memenuhi prinsip kehati-hatian. d. Bank memperhatikan analisis biaya dan manfaat. e. Bank memenuhi prinsip hubungan kerja sama secara wajar. f. Bank memenuhi ketentuan peraturan perundang-undangan. g. Bank memperoleh izin Otoritas Jasa Keuangan untuk setiap rencana penyediaan jasa TI. h. Penyediaan jasa TI berupa aplikasi kepada lembaga jasa keuangan selain bank dapat dilakukan sepanjang lembaga jasa keuangan pengguna jasa TI berada dalam satu grup atau kelompok dengan Bank dan penggunaan aplikasi ditujukan untuk mendukung kegiatan operasional yang umum.
			7.b.2. Satuan kerja terkait melakukan identifikasi, pengukuran, pemantauan, dan pengendalian risiko atas penyediaan jasa TI oleh Bank.	Satuan kerja terkait mempertimbangkan beberapa hal dalam melakukan identifikasi, pengukuran, pemantauan, dan pengendalian risiko atas penyediaan jasa TI oleh Bank secara memadai yang mencakup: a. aktivitas dan fungsi penyediaan jasa TI meliputi sensitivitas data yang diakses, dilindungi, atau dikendalikan oleh Bank; b. teknologi yang digunakan meliputi keandalan (*reliability*), keamanan (*security*), ketersediaan

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				(*availability*), dan ketepatan waktu (*timeliness*); dan c. Identifikasi risiko meliputi: 1) risiko operasional; 2) risiko hukum; 3) risiko reputasi; 4) risiko kepatuhan; dan 5) risiko stratejik.
8.	Pelindungan Konsumen	8.a. Pemenuhan Aspek Pelayanan Konsumen	8.a.1. Bank memperhatikan aspek keterlibatan nasabah (*customer engagement*) dan memiliki strategi untuk mempertahankan nasabah dalam menilai keberhasilan produk dan layanan Bank.	a. Bank memiliki mekanisme untuk mengukur keterlibatan nasabah dalam rangka melakukan penyesuaian dan perbaikan terhadap produk dan layanan kepada nasabah. b. Bank memiliki strategi untuk mempertahankan nasabah melalui pengembangan produk dan peningkatan layanan Bank.
			8.a.2. Bank menyediakan layanan dan/atau produk yang ramah bagi penyandang disabilitas dan memiliki standar minimal pelayanan keuangan kepada nasabah dan/atau calon nasabah dengan disabilitas.	a. Bank memiliki dokumen standar pelayanan keuangan kepada penyandang disabilitas. b. Bank mengadopsi prinsip pelayanan keuangan yang bersifat desain universal. 1) Prinsip desain universal untuk pelayanan fisik yaitu dapat digunakan oleh semua orang, fleksibel dalam penggunaannya, menggunakan tenaga fisik yang minimal, serta ruang dan ukuran yang memadai. 2) Prinsip desain universal untuk pelayanan nonfisik maupun pelayanan dokumen yaitu dapat digunakan oleh semua orang, sederhana, fleksibel dalam penggunaannya, komunikasi yang efektif, dan mentoleransi kesalahan.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				c. Teknologi yang dapat digunakan Bank antara lain: 1) kompatibel dengan *voice over*, *talk back*, atau *screen reader*; 2) menggunakan desain dan bahasa yang sederhana untuk menghindari kebingungan; 3) akses *login* ke dalam layanan *internet banking* yang dapat diakses tanpa menggunakan *mouse* dan dapat dibaca dengan menggunakan alat pembaca layar; 4) alternatif kode *Completely Automatic Public Turing Test to Tell Computers and Human Apart* (CAPTCHA), tersedia dalam kode audio atau pertanyaan matematika sederhana; 5) menyediakan waktu yang cukup untuk memasukkan kata sandi yang diterima melalui pesan singkat atau surat elektronik; dan 6) pesan kekeliruan (*error*) tersedia dalam bentuk teks dan audio, namun tidak spesifik menginformasikan jenis kesalahan (*username* atau *password* atau *pin* dan lainnya).
			8.a.3. Bank memanfaatkan data nasabah dalam mengembangkan produk dan layanan.	a. Bank memanfaatkan data nasabah antara lain aspek demografi, perilaku, preferensi dan kebutuhan nasabah, dalam mengembangkan produk dan layanan. b. Bank melakukan kolaborasi dengan nasabah dalam menciptakan produk Bank dengan

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				melibatkan ide ataupun peran serta nasabah dalam proses penyusunan produk dan layanan Bank. Kolaborasi yang dimaksud harus jelas mengenai tanggung jawab dan kewenangan serta hak dan kewajiban yang didokumentasikan dalam dokumen tertulis.
			8.a.4. Bank mengevaluasi produk dan layanan berdasarkan persepsi dan tingkat kepercayaan nasabah.	a. Bank memiliki mekanisme untuk perolehan persepsi nasabah dan tata cara analisis data tersebut yang paling sedikit terkait dengan: 1) *product quality* yaitu persepsi nasabah terhadap kualitas produk dan layanan Bank; 2) *customer support quality* yaitu persepsi nasabah terhadap kualitas *customer support* Bank; 3) *positioning* yaitu persepsi nasabah terhadap produk dan layanan Bank dibandingkan dengan produk dan layanan kompetitor; 4) *price* yaitu persepsi nasabah terhadap biaya, contoh suku bunga simpanan dan kredit yang ditawarkan oleh Bank; dan 5) *reputation* yaitu persepsi nasabah terhadap citra produk dan layanan Bank, yang diperoleh melalui antara lain media sosial, atau reviu aplikasi Bank pada *platform* distribusi. b. Bank telah memiliki saluran umpan balik untuk mendapatkan masukan dari nasabah.
			8.a.5. Bank mengevaluasi produk dan layanan berdasarkan pengalaman nasabah.	a. Bank menganalisis pengalaman nasabah dalam menggunakan produk dan/atau layanan yang diberikan oleh Bank, antara lain:

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				1) desain produk, dapat berupa tampilan *mobile apps* Bank, kenyamanan interaksi user dengan *mobile apps*, serta alur proses (*flow*) menu aplikasi; 2) *range of products*, yaitu jenis produk yang ditawarkan dalam aplikasi Bank; dan/atau 3) *speed of delivery*, yaitu kecepatan akses aplikasi Bank. b. Bank melakukan perbaikan serta peningkatan kualitas atas produk dan layanan dengan mengacu antara lain pada sistematika *Define, Measure, Analyze, Improve, dan Control* (DMAIC).
		8.b. Pemenuhan Aspek Pelindungan Konsumen	8.b.1. Bank memastikan aspek pelindungan data nasabah dalam perjanjian kerja sama kemitraan.	a. Bank dan mitra hanya dapat memproses data nasabah sesuai dengan ketentuan perundang-undangan mengenai pelindungan data pribadi. b. Mitra menggunakan dan mengamankan semua data yang disediakan oleh Bank dan/atau nasabah sesuai dengan persyaratan keamanan yang disepakati oleh Bank dan mitra, termasuk dari ancaman serangan siber. c. Permintaan data kepada nasabah Bank, sebatas keperluan pemberian layanan Bank kepada nasabah. d. Bank mengecek persetujuan konsumen dari mitra meliputi: 1) prosedur untuk memberikan persetujuan dan bagaimana persetujuan harus ditarik (*withdrawn*);

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				2) tidak terdapat batasan atau larangan dimana konsumen tidak dapat lagi menarik persetujuan; 3) konsumen diinformasikan dan memiliki hak untuk menyetujui atau menolak tentang data yang dapat diakses oleh mitra pada saat konsumen menandatangani kontrak dengan mitra; dan 4) mitra hanya dapat mengakses data konsumen terbatas dengan jangka waktu tertentu (syarat waktu dapat ditentukan lebih lanjut antar Bank dan mitra). e. Mitra menggunakan alat pendeteksi untuk memindai *malware*. f. Mitra melakukan analisis risiko secara teratur dan mengambil langkah untuk memperbarui tindakan pengamanan yang diperlukan untuk memperbaiki insiden keamanan atau kerentanan yang teridentifikasi. g. Bank dan mitra melakukan pertemuan secara berkala untuk membahas setiap pengaduan konsumen atau nasabah yang diterima oleh mitra. Bank berhak untuk meminta informasi lebih lanjut tentang pengaduan konsumen atau nasabah serta penanganannya kepada mitra. h. Bank dan mitra membahas perselisihan dalam jangka waktu tertentu yang telah ditentukan. i. Bank menetapkan strategi kelangsungan bisnis dalam hal layanan mitra tidak dapat diakses oleh Bank atau mengalami permasalahan, untuk memastikan bahwa layanan kepada konsumen tetap berjalan.

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				j. Bank menetapkan alternatif layanan dengan keamanan yang memadai.
			8.b.2. Bank memiliki kebijakan dan mekanisme penyelesaian pengaduan nasabah layanan digital.	a. Bank memiliki saluran untuk menerima pengaduan nasabah yang dapat diakses nasabah setiap saat secara daring. b. Bank memiliki fungsi/unit kerja yang berwenang dalam penyelesaian pengaduan nasabah. c. Bank memiliki kebijakan penyelesaian pengaduan nasabah sesuai dengan peraturan perundang-undangan. d. Bank melakukan monitoring proses penyelesaian pengaduan nasabah dan memiliki SLA yang jelas untuk setiap jenis pengaduan. e. Bank melakukan evaluasi secara periodik atas kinerja penyelesaian pengaduan nasabah. f. Bank memiliki mekanisme pengaduan kembali bagi nasabah yang tidak setuju dengan keputusan penyelesaian pengaduan oleh Bank.
			8.b.3. Bank memiliki komitmen untuk melakukan sosialisasi terkait literasi keuangan di era digital.	a. Bank memiliki dan menjalankan program untuk meningkatkan literasi keuangan di era digital kepada nasabah dan/atau masyarakat. b. Bank melakukan sosialisasi terkait aspek keamanan dalam bertransaksi secara digital.
			8.b.4. Bank menerapkan transparansi dan pengungkapan yang bertanggung jawab atas TI yang digunakan dalam hal adopsi TI berdampak langsung terhadap nasabah untuk memastikan bahwa nasabah memahami *output*	Penerapan transparansi dan pengungkapan yang bertanggung jawab mencakup: a. Bank memberikan penjelasan kepada nasabah mengenai pemahaman umum tentang sistem berbasis TI yang digunakan oleh Bank dalam memberikan layanan kepada nasabah; dan

No	Aspek/ Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			yang dihasilkan oleh sistem berbasis TI.	b. Bank telah memberikan penjelasan kepada nasabah mengenai sarana dan prosedur bagi nasabah untuk melakukan klarifikasi atas hasil sistem berbasis TI.

Ditetapkan di Jakarta
pada tanggal 14 Desember 2023

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Mufli Asmawidjaja

LAMPIRAN II
SURAT EDARAN OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 24/SEOJK.03/2023
TENTANG
PENILAIAN TINGKAT MATURITAS DIGITAL BANK UMUM

Kertas Kerja Penilaian Kualitas Penerapan Aspek Maturitas Digital Bank

No.	Aspek/ Domain[1)]	Subdomain[1)]	Kontrol[1)]	Penerapan Kontrol[2)]	Penjelasan[3)]	Referensi Dokumen[4)]	Departemen/Unit/Jabatan yang Bertanggung Jawab
1.	Tata Kelola	1.a. Tatanan Institusi	1.a.1. Bank memiliki permodalan yang memadai untuk mendukung rencana pengembangan TI.				
			1.a.2.				
2.	Arsitektur	2.a. Arsitektur TI	2.a.1. Direksi memastikan arsitektur TI disusun selaras dengan strategi bisnis dan sesuai dengan kebutuhan bisnis Bank.				
			2.a.2. ...				
3.	Manajemen Risiko	3.a. Manajemen Risiko TI	3.a.1. Bank melakukan identifikasi risiko terkait penyelenggaraan TI secara memadai.				
			3.a.2. ...				

5.	Teknologi	5.a. Adopsi TI secara bertanggung jawab	5.a.1. Bank memiliki kebijakan terkait adopsi TI.				
			5.a.2. ...				
...	...	...	...				

Keterangan:

1) Diisi dengan aspek/domain, subdomain, dan kontrol sebagaimana tercantum dalam Lampiran I Matriks Kontrol atas Aspek Maturitas Digital Bank, kecuali untuk aspek/domain ketahanan dan keamanan siber.
2) Diisi dengan penilaian atas kondisi penerapan kontrol pada Bank, yaitu: **"Tidak Memadai/Belum Diterapkan", "Kurang/Belum Memadai", "Cukup Memadai", "Memadai",** atau **"Sangat Memadai"**. Penilaian mempertimbangkan penjelasan/kriteria pemenuhan kontrol sebagaimana tercantum dalam Lampiran I Matriks Kontrol atas Aspek Maturitas Digital Bank.
3) Diisi dengan penjelasan atas kondisi penerapan kontrol (jika ada).
4) Diisi dengan dokumen yang dapat dijadikan acuan dalam menilai penerapan kontrol.

Ditetapkan di Jakarta
pada tanggal 14 Desember 2023

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Mufli Asmawidjaja

LAMPIRAN III
SURAT EDARAN OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 24/SEOJK.03/2023
TENTANG
PENILAIAN TINGKAT MATURITAS DIGITAL BANK UMUM

A. Matriks Penetapan Kualitas Penerapan Aspek Maturitas Digital Bank

Peringkat	Definisi Peringkat
1 (*Strong*)	Kualitas penerapan aspek/domain sangat memadai. Meskipun terdapat kelemahan minor tetapi kelemahan tersebut tidak signifikan sehingga dapat diabaikan. Contoh karakteristik Bank yang termasuk dalam peringkat 1 (*Strong*): a. penerapan tatanan institusi dan tata kelola TI secara keseluruhan sangat memadai; b. penyusunan dan pengelolaan arsitektur TI sangat memadai, termasuk keselarasan arsitektur TI dengan visi, misi, dan rencana korporasi Bank; c. manajemen risiko TI sangat memadai yang tercermin dari proses identifikasi, pengukuran, pemantauan dan pengendalian risiko terkait penyelenggaraan TI; d. penerapan adopsi TI yang bertanggung jawab sangat memadai dan penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI sangat andal dan teruji; e. tata kelola data, pelindungan data pribadi, dan transfer data secara keseluruhan sangat memadai; f. kerja sama kemitraan dan penyediaan jasa TI oleh Bank dilaksanakan secara sangat memadai; dan/atau g. pemenuhan aspek pelindungan dan pelayanan konsumen sangat memadai yang meliputi *customer engagements, customer experience, customer insight, customer trust and perception,* dan *customer with disability*.
2 (*Satisfactory*)	Kualitas penerapan aspek/domain memadai. Meskipun terdapat kelemahan minor, kelemahan tersebut dapat diselesaikan pada aktivitas bisnis normal. Contoh karakteristik Bank yang termasuk dalam peringkat 2 (*Satisfactory*): a. penerapan tatanan institusi dan tata kelola TI secara keseluruhan memadai; b. penyusunan dan pengelolaan arsitektur TI memadai, termasuk keselarasan arsitektur TI dengan visi, misi, dan rencana korporasi Bank; c. manajemen risiko TI memadai yang tercermin dari proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko terkait penyelenggaraan TI; d. penerapan adopsi TI yang bertanggung jawab memadai dan penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI andal dan teruji; e. tata kelola data, pelindungan data pribadi, dan transfer data secara keseluruhan memadai; f. kerja sama kemitraan dan penyediaan jasa TI oleh Bank dilaksanakan secara memadai; dan/atau g. pemenuhan aspek pelindungan dan pelayanan konsumen memadai yang meliputi *customer engagements, customer experience, customer insight, customer trust and perception,* dan *customer with disability*.
3 (*Fair*)	Kualitas penerapan aspek/domain cukup memadai. Meskipun persyaratan minimum terpenuhi, terdapat beberapa kelemahan yang membutuhkan perhatian manajemen.

Peringkat	Definisi Peringkat
	Contoh karakteristik Bank yang termasuk dalam peringkat 3 (*Fair*): a. penerapan tatanan institusi dan tata kelola TI secara keseluruhan cukup memadai; b. penyusunan dan pengelolaan arsitektur TI cukup memadai, termasuk keselarasan arsitektur TI dengan visi, misi, dan rencana korporasi Bank; c. manajemen risiko TI cukup memadai yang tercermin dari proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko terkait penyelenggaraan TI; d. penerapan adopsi TI yang bertanggung jawab cukup memadai dan penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI cukup andal dan teruji; e. tata kelola data, pelindungan data pribadi, dan transfer data secara keseluruhan cukup memadai; f. kerja sama kemitraan dan penyediaan jasa TI oleh Bank dilaksanakan secara cukup memadai; dan/atau g. pemenuhan aspek pelindungan dan pelayanan konsumen cukup memadai yang meliputi *customer engagements, customer experience, customer insight, customer trust and perception,* dan *customer with disability*.
4 (*Marginal*)	Kualitas penerapan aspek/domain kurang memadai. Terdapat kelemahan signifikan pada berbagai kontrol yang memerlukan tindakan korektif segera. Contoh karakteristik Bank yang termasuk dalam peringkat 4 (*Marginal*): a. penerapan tatanan institusi dan tata kelola TI secara keseluruhan kurang memadai; b. penyusunan dan pengelolaan arsitektur TI kurang memadai, termasuk keselarasan arsitektur TI dengan visi, misi, dan rencana korporasi Bank; c. manajemen risiko TI kurang memadai yang tercermin dari proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko terkait penyelenggaraan TI; d. penerapan adopsi TI yang bertanggung jawab kurang memadai dan penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI kurang andal dan teruji; e. tata kelola data, pelindungan data pribadi, dan transfer data secara keseluruhan kurang memadai; f. kerja sama kemitraan dan penyediaan jasa TI oleh Bank dilaksanakan secara kurang memadai; dan/atau g. pemenuhan aspek pelindungan dan pelayanan konsumen kurang memadai yang meliputi *customer engagements, customer experience, customer insight, customer trust and perception,* dan *customer with disability*.
5 (*Unsatisfactory*)	Kualitas penerapan aspek/domain tidak memadai. Terdapat kelemahan signifikan pada berbagai kontrol yang tindakan penyelesaiannya di luar kemampuan manajemen. Contoh karakteristik Bank yang termasuk dalam peringkat 5 (*Unsatisfactory*): a. penerapan tatanan institusi dan tata kelola TI secara keseluruhan tidak memadai; b. penyusunan dan pengelolaan arsitektur TI tidak memadai;

Peringkat	Definisi Peringkat
	c. manajemen risiko TI tidak memadai yang tercermin dari proses identifikasi, pengukuran, pemantauan, dan pengendalian risiko terkait penyelenggaraan TI yang tidak memadai; d. penerapan adopsi TI yang bertanggung jawab tidak memadai dan penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI tidak andal dan teruji; e. tata kelola data, pelindungan data pribadi, dan transfer data secara keseluruhan tidak memadai; f. kerja sama kemitraan dan penyediaan jasa TI oleh Bank dilaksanakan secara tidak memadai; dan/atau g. pemenuhan aspek pelindungan dan pelayanan konsumen tidak memadai yang meliputi *customer engagements, customer experience, customer insight, customer trust and perception,* dan *customer with disability*.

B. Matriks Penetapan Tingkat Maturitas Digital Bank

Peringkat	Definisi Peringkat
Tingkat 1	Mencerminkan kondisi tingkat maturitas digital Bank yang secara umum sangat tinggi, tercermin dari seluruh aktivitas telah berjalan dengan sangat baik dan Bank telah menjalankan mekanisme *continuous improvement*. Dalam hal terdapat kelemahan maka secara umum kelemahan tersebut tidak signifikan.
Tingkat 2	Mencerminkan kondisi tingkat maturitas digital Bank yang secara umum tinggi, tercermin dari seluruh aktivitas yang dibutuhkan telah dilaksanakan secara konsisten. Dalam hal terdapat kelemahan maka secara umum kelemahan tersebut kurang signifikan.
Tingkat 3	Mencerminkan kondisi tingkat maturitas digital Bank secara umum cukup, tercermin dari sebagian besar aktivitas yang dibutuhkan telah dilaksanakan secara konsisten. Dalam hal terdapat kelemahan maka secara umum kelemahan tersebut cukup signifikan dan apabila tidak berhasil diatasi dengan baik oleh manajemen dapat mengganggu kelangsungan usaha Bank.
Tingkat 4	Mencerminkan kondisi tingkat maturitas digital Bank yang secara umum rendah, tercermin dari beberapa aktivitas atau proses yang dibutuhkan telah diidentifikasi, namun belum seluruhnya dilaksanakan secara konsisten. Terdapat kelemahan yang secara umum signifikan dan tidak dapat diatasi dengan baik oleh manajemen serta mengganggu kelangsungan usaha Bank.
Tingkat 5	Mencerminkan kondisi tingkat maturitas digital Bank yang secara umum sangat rendah, tercermin dari aktivitas atau proses yang dibutuhkan belum diidentifikasi dan belum dilaksanakan. Terdapat kelemahan yang secara umum sangat signifikan sehingga untuk mengatasinya diperlukan dukungan dana dari pemegang saham atau sumber dana dari pihak lain untuk memperkuat tingkat maturitas digital pada Bank.

Ditetapkan di Jakarta
pada tanggal 14 Desember 2023

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Mufli Asmawidjaja

LAMPIRAN IV
SURAT EDARAN OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR 24/SEOJK.03/2023
TENTANG
PENILAIAN TINGKAT MATURITAS DIGITAL BANK UMUM

Hasil Penilaian Tingkat Maturitas Digital Bank

Nama Bank :
Tahun :

Penilaian Penerapan Aspek Maturitas Digital Bank

No.	Aspek Penilaian	Peringkat
1	Tata Kelola	
2	Arsitektur	
3	Manajemen Risiko	
4	Ketahanan dan Keamanan Siber[1)]	
5	Teknologi	
6	Data	
7	Kolaborasi	
8	Pelindungan Konsumen	
Analisis		
Penjelasan lebih lanjut mengenai penilaian kualitas penerapan aspek maturitas digital Bank, termasuk pertimbangan Bank untuk setiap aspek/domain sehingga memperoleh peringkat kualitas penerapan pada tiap aspek/domain.		

Tingkat Maturitas Digital Bank	
Analisis	
Penjelasan lebih lanjut mengenai penetapan tingkat maturitas digital pada Bank, termasuk pertimbangan Bank atas peringkat kualitas penerapan aspek terkait sehingga memperoleh tingkat maturitas digital Bank.	

Lampiran
1. Kertas kerja penilaian maturitas digital Bank.

Keterangan:
1) Peringkat diisi sesuai dengan peringkat tingkat maturitas keamanan siber dengan mengacu pada ketentuan Otoritas Jasa Keuangan mengenai ketahanan dan keamanan siber bagi bank umum.

Ditetapkan di Jakarta
pada tanggal 14 Desember 2023

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

DIAN EDIANA RAE

Salinan ini sesuai dengan aslinya
Direktur Hukum 1
Departemen Hukum

ttd

Mufli Asmawidjaja