Yth.

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

di tempat.

RANCANGAN SURAT EDARAN OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA
NOMOR /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 risiko kebocoran data, risiko investasi teknologi yang tidak sesuai dengan strategi bisnis, risiko penyalahgunaan teknologi, risiko serangan siber, risiko alih daya, 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. Adapun salah satu upaya 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, maka diperlukan suatu panduan berupa penilaian tingkat maturitas digital yang dapat digunakan oleh bank dan OJK guna mengukur tingkat keberhasilan dari transformasi digital bank."

2. Tingkat maturitas digital merupakan kondisi yang mencerminkan pemenuhan terhadap seluruh aspek dalam penyelenggaraan teknologi informasi (TI) sesuai dengan Peraturan Otoritas Jasa Keuangan tentang Penyelenggaraan Teknologi Informasi oleh Bank Umum 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. 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 domain sebagai berikut:
      1) tata kelola, yang meliputi sub domain tatanan institusi dan tata kelola TI;
      2) arsitektur, yang meliputi sub domain arsitektur TI Bank;
      3) manajemen risiko, yang meliputi sub domain manajemen risiko TI Bank;
      4) ketahanan dan keamanan siber, sesuai dengan peringkat tingkat risiko terkait keamanan siber dengan mengacu pada ketentuan Otoritas Jasa Keuangan mengenai ketahanan dan keamanan siber bagi bank umum;
      5) teknologi, yang meliputi sub domain adopsi teknologi yang bertanggung jawab dan penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI Bank;
      6) data, yang meliputi sub domain tata kelola data, pelindungan data, dan transfer data;

7) kolaborasi, yang meliputi sub domain kerja sama kemitraan dan penyediaan jasa TI oleh Bank; dan
8) pelindungan konsumen, yang meliputi sub domain pelindungan dan pelayanan konsumen.

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

3. Bank yang tidak menerapkan:
   a. sub domain Kerja Sama Kemitraan dan Penyediaan Jasa TI oleh Bank pada domain Kolaborasi; dan/atau
   b. sub domain Penggunaan Jasa Pihak Ketiga dalam Penyelenggaraan TI Bank (IT Outsourcing) pada domain Teknologi,

tidak perlu memasukkan domain kolaborasi dalam penilaian tingkat maturitas digital Bank.

Contoh: Bank X tidak melakukan kolaborasi dengan mitra terkait penyediaan layanan atau produk kepada nasabah, maka Bank X tidak perlu melakukan penilaian penerapan sub domain kerja sama kemitraan dalam domain kolaborasi.

4. Bank dapat melakukan penilaian tingkat maturitas digital Bank secara mandiri atau menggunakan pihak ketiga. Dalam hal penilaian tingkat maturitas digital dilakukan oleh pihak ketiga, Bank harus:
   a. memastikan pihak ketiga memiliki kompetensi yang memadai sesuai dengan kebutuhan penilaian; dan
   b. tetap bertanggung jawab atas pelaksanaan penilaian tingkat maturitas digital.

   Kompetensi dari pihak ketiga dibuktikan antara lain dengan adanya sertifikasi dan/atau pengakuan dari lembaga yang berwenang di Indonesia atau di luar negeri.
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 wajib menyampaikan laporan hasil penilaian sendiri atas tingkat maturitas digital Bank sebagai bagian dari laporan kondisi terkini penyelenggaraan TI Bank.
2. Hasil penilaian tingkat maturitas digital bank sebagaimana dimaksud pada Romawi II butir 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.
4. Otoritas Jasa Keuangan melakukan penelaahan atas hasil penilaian tingkat maturitas digital Bank sebagaimana dimaksud pada Romawi II butir 2.e. 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 Bank.

IV. PENUTUP

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

Ditetapkan di Jakarta
pada tanggal

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

ttd

DIAN EDIANA RAE

LAMPIRAN I

RANCANGAN SURAT EDARAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR /SEOJK.03/2023

TENTANG

PENILAIAN TINGKAT MATURITAS DIGITAL BANK UMUM

Penilaian Kualitas Kontrol atas Tingkat Maturitas Digital Bank

Matriks Kontrol Penerapan Domain

No	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 teknologi informasi (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, rencana korporasi maupun rencana bisnis bank yang memuat alokasi anggaran untuk pengembangan TI.
			1.a.2. Bank telah mengelola portofolio investasi TI secara memadai.	a. Bank memiliki sumber pendanaan guna melakukan investasi TI, termasuk analisis perhitungan ekspektasi tingkat pengembalian investasi. b. Bank telah melakukan analisis kelayakan rencana investasi yang akan didanai. Melakukan evaluasi rencana investasi mencakup keselarasan dengan strategi bank, keuntungan dan risiko bagi bank, ketersediaan sumber pendanaan dan dampak penambahan investasi

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				terhadap portofolio investasi secara keseluruhan. c. Bank telah menetapkan prioritas alokasi sumber dana pada investasi TI yang bernilai tinggi. b. Bank telah memantau kinerja portofolio investasi seperti tren tingkat pengembalian investasi, deviasi anggaran dan realisasi investasi.
			1.a.3. Bank telah melakukan pengelolaan biaya terkait TI secara efektif.	Bank melakukan pengelolaan biaya secara efektif antara lain: 1) melakukan pemantauan deviasi anggaran, proyeksi biaya, dan realisasi biaya, termasuk analisis biaya dan manfaat; dan 2) melakukan pemantauan penggunaan anggaran sesuai dengan manfaat yang diterima, termasuk jika penyelenggaraan TI disediakan oleh perusahaan penyelenggara 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.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			1.a.5. Bank memiliki struktur organisasi yang mendukung transformasi digital.	Bank memiliki struktur organisasi yang memungkinkan Bank dapat melakukan pekerjaan yang mendukung transformasi digital, antara lain mencakup aspek sebagai berikut: 1) Bank memiliki struktur organisasi yang kolaboratif, sehingga memungkinkan interaksi yang lebih luas antar unit kerja agar proses bisnis Bank berjalan lebih efektif; 2) melaksanakan kewenangan yang terdesentralisasi di unit kerja sehingga pengambilan keputusan dapat dilakukan dengan lebih cepat; 3) pemanfaatan TI untuk menyelesaikan pekerjaan pada setiap proses bisnis Bank; 4) Bank memiliki media komunikasi terpadu untuk memfasilitasi akses pegawai ke sistem informasi bank melalui perangkat seluler pribadi milik pegawai.
			1.a.6. Bank memiliki program pengembangkan budaya digital dan menerapkan budaya digital untuk mendukung transformasi digital.	
			1.a.7. Bank telah melakukan pengembangan talenta digital.	a. Terdapat informasi yang menunjukkan komitmen Dewan Komisaris dan Direksi untuk mengembangkan budaya digital pada

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				laporan tahunan dan rencana bisnis Bank. b. Bank menerapkan program pengembangan budaya digital dengan aspek utama meliputi: 1) inovasi berupa perilaku dan budaya yang mendukung eksplorasi ide baru; 2) pengambilan keputusan berdasarkan data terkini dari berbagai sumber; 3) kolaborasi internal yang meliputi kolaborasi lintas fungsi dan unit kerja untuk mengoptimalkan potensi talenta digital Bank; 4) budaya terbuka melalui kolaborasi dengan pihak eksternal melalui kemitraan; 5) pola pikir mengedepankan aspek digital serta mengutamakan solusi melalui penggunaan teknologi; 6) kemampuan organisasi untuk beradaptasi dengan tuntutan perubahan teknologi; dan 7) berorientasi pada konsumen melalui penggunaan solusi digital untuk memperluas basis konsumen, meningkatkan pengalaman konsumen, dan berkolaborasi dengan konsumen dalam pengembangan dan

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				peningkatan kualitas produk Bank. c. Bank melakukan evaluasi program pengembangan budaya digital.
			1.a.8. Bank memiliki komitmen untuk melakukan edukasi dan sosialisasi terkait literasi digital.	a. Terdapat program untuk meningkatkan edukasi dan literasi digital kepada masyarakat. b. Bank melakukan sosialisasi dan edukasi terkait aspek keamanan dalam bertransaksi secara digital.
		1.b. Tata Kelola TI	1.b.1. Bank memastikan pengaturan dan pengelolaan sistem tata kelola TI telah memadai.	a. Bank mengevaluasi tata kelola TI minimal 1 tahun sekali yang mencakup: 1) menerapkan prinsip-prinsip terkait desain tata kelola TI. 2) menganalisis dan mengidentifikasi faktor lingkungan internal dan eksternal yang dapat mempengaruhi desain tata kelola. 3) menentukan signifikansi penggunaan TI dan fungsinya dalam proses bisnis bank. 4) mematuhi undang-undang, peraturan eksternal, dan kewajiban kontraktual serta memastikan penerapan kepatuhannya dalam tata kelola TI. 5) menentukan implikasi dari lingkungan pengendalian terkait dengan penyelenggaraan TI. 6) menyelaraskan penggunaan dan

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				pemrosesan informasi secara etis serta menganalisis dampaknya terhadap konsumen, maupun pemangku kepentingan sesuai dengan visi, misi, dan tujuan bisnis bank. 7) menentukan pendelegasian wewenang yang sesuai dengan kompleksitas bisnis bank, termasuk penggunaan limit persetujuan dalam pengambilan keputusan terkait penyelenggaraan TI. b. Bank telah menyelaraskan sistem tata kelola sesuai dengan prinsip tata kelola TI yang baik, melalui: 1) penetapan struktur, proses, dan praktik tata kelola TI yang selaras dengan prinsip tata kelola Bank; dan 2) penetapan mekanisme koordinasi dan pelaporan terkait tata kelola TI untuk pengawasan dan pengambilan keputusan. c. Bank telah memantau sistem tata kelola TI minimal 1 (satu) kali dalam setahun. Hal yang perlu diperhatikan Bank dalam memantau sistem tata kelola TI yaitu: 1) frekuensi kaji ulang pihak independen terhadap pelanggaran prinsip tata kelola TI. Yang dimaksud dengan “pihak independen” adalah pihak di luar

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				Bank yang tidak memiliki hubungan keuangan, kepengurusan, kepemilikan saham dan/atau hubungan keluarga dengan Dewan Komisaris, Direksi, Pejabat Eksekutif dan/atau Pemegang Saham Pengendali atau hubungan lain yang dapat mempengaruhi kemampuannya untuk bertindak independen; 2) tingkat kepuasan pemangku kepentingan yang antara lain dapat diukur melalui survei; dan 3) jumlah permasalahan terkait tata kelola TI yang dilaporkan.
			1.b.2. Bank telah mengoptimalkan nilai bisnis dari investasi dalam proses bisnis, layanan dan aset TI.	a. Bank telah menyusun target investasi TI yang selaras dengan aspek berikut: 1) strategi bisnis perusahaan; 2) analisis biaya dan tingkat pengembalian investasi; dan 3) tingkat risiko dan jenis manfaat yang akan diperoleh. b. Bank telah memantau kesesuaian investasi TI dengan keuntungan yang diharapkan. Hal yang perlu diperhatikan Bank yaitu: 1) jumlah peluang pendapatan bisnis baru yang direalisasikan sebagai akibat langsung dari investasi TI;

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				2) tujuan strategis perusahaan yang dicapai sebagai hasil dari inisiatif TI; dan 3) tingkat kepuasan pemangku kepentingan terhadap inisiatif TI.
			1.b.3. Bank telah memastikan risiko terkait penggunaan TI telah diidentifikasi dan dikelola secara memadai.	a. Bank telah mengidentifikasi dan mengevaluasi risiko penggunaan TI saat ini dan pada masa depan. Bank telah memastikan bahwa risiko penggunaan TI tidak melebihi toleransi risiko Bank. b. Bank telah menerapkan praktik manajemen risiko terhadap penggunaan TI, yaitu: 1) Bank memiliki strategi pengelolaan risiko TI yang telah terintegrasi dalam praktik manajemen risiko bank secara keseluruhan; dan 2) Bank telah memiliki mekanisme atau proses untuk identifikasi risiko, memonitor risiko, mitigasi terhadap risiko, dan pelaporan risiko.
			1.b.4. Bank telah memastikan sumber daya terkait TI (manusia, proses, dan teknologi) tersedia untuk mendukung Bank secara efektif dan dengan biaya optimal.	a. Bank telah mengevaluasi kebutuhan sumber daya terkait TI minimal 1 tahun sekali saat ini dan masa depan yang mencakup kebutuhan pendanaan, manusia, pilihan atau strategi pemenuhan kebutuhan, dan

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				pengembangan kapabilitas yang diperlukan. b. Bank telah memonitor pengelolaan sumber daya telah dijalankan secara optimal. Hal yang perlu diperhatikan Bank yaitu: 1) Bank memiliki mekanisme atau proses untuk identifikasi permasalahan, respon atau mitigasi terhadap permasalahan dan pelaporan permasalahan; 2) tingkat umpan balik pemangku kepentingan tentang pengoptimalan sumber daya; 3) jumlah manfaat (misalnya, penghematan biaya) yang dicapai melalui optimalisasi pemanfaatan sumber daya; 4) jumlah target kinerja pengelolaan sumber daya yang direalisasikan; dan 5) jumlah proyek dan program dengan status berisiko sedang atau tinggi karena masalah pengelolaan sumber daya.
			1.b.5. Bank telah mengidentifikasi seluruh pemangku kepentingan dan melibatkan mereka dalam sistem tata kelola TI.	a. Bank melakukan evaluasi pemangku kepentingan yang terlibat dalam sistem tata kelola TI dan kebutuhan komunikasi dan pelaporan kepada pemangku kepentingan (termasuk kepada regulator).

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				b. Bank memastikan keterlibatan pemangku kepentingan dan efektifitas komunikasi dengan pemangku kepentingan. Hal yang perlu diperhatikan Bank dalam memastikan keterlibatan pemangku kepentingan yaitu: 1) tingkat keterlibatan pemangku kepentingan dengan TI Bank; 2) 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 telah 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 5) standar maupun regulasi terkait.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				b. Bank mengkomunikasikan tujuan dan arah penggunaan TI ke seluruh perusahaan. Hal yang perlu diperhatikan Bank yaitu memastikan informasi yang dikomunikasikan mencakup misi, tujuan layanan, dan pengendalian internal. c. Bank telah menetapkan struktur organisasi sesuai dengan desain sistem manajemen (contoh: komite). d. Bank telah menetapkan peran dan tanggung jawab untuk pengelolaan TI Bank termasuk tingkat otoritas, tanggung jawab, dan akuntabilitas. e. Bank telah mengoptimalkan penempatan fungsi TI dalam struktur organisasi. Penempatan fungsi TI (terpusat, terdesentralisasi, atau kombinasi) dalam organisasi mencerminkan kepentingan strategis dan ketergantungan operasional TI dalam Bank, model operasi Bank dan pilihan pengisian sumber daya pada fungsi TI. f. Bank telah menentukan kepemilikan informasi (data) dan sistem informasi. g. Bank telah menentukan target keterampilan dan kompetensi yang diperlukan untuk mencapai tujuan manajemen yang relevan.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				h. Bank telah menetapkan dan mengkomunikasikan kebijakan dan prosedur kontrol TI pada setidaknya area utama seperti kualitas, keamanan, privasi, kontrol internal, penggunaan aset TI, etika, dan hak kekayaan intelektual. i. Bank telah menetapkan dan mengimplementasikan infrastruktur, layanan, dan aplikasi untuk mendukung tata kelola dan sistem manajemen.
			1.b.7. Bank memastikan bahwa setiap inisiatif digitisasi atau transformasi digital telah sesuai dengan arah dan strategi Bank ke depan sebagaimana yang dimuat dalam rencana strategis TI (RSTI) 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 operasi saat ini, dan target tingkat digitalisasi. b. Bank menilai kemampuan, kinerja, dan tingkat 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.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				d. Bank melakukan analisis kesenjangan antara lingkungan TI saat ini dan target ke depan, yang dapat dituangkan pada RBBR tahunan yang dikomunikasikan kepada pengawas terlebih dahulu. e. Bank menetapkan rencana strategis dan peta jalan transformasi yang akan dilakukan. Rencana tersebut tercantum pada rencana strategis TI (RSTI). f. Bank mengkomunikasikan strategi dan arah pengembangan TI kepada seluruh pengampu kepentingan dan pengguna akhir terkait.
			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. (Peran dan tanggung jawab hubungan telah ditentukan dan ditetapkan, komunikasi difasilitasi). c. Bank telah melakukan komunikasi melalui sistem internal yang transparan dengan semua pemangku kepentingan yang relevan dan mengkordinasikan *delivery* dan solusi layanan TI yang diberikan kepada unit bisnis.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				d. Bank secara berkesinambungan memperbaiki dan mengembangkan layanan TI yang diperlukan oleh organisasi agar tetap relevan dengan perkembangan dinamika 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 I&T apa pun; dan 2) jumlah layanan usang yang telah teridentifikasi. 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:

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				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 pernurunan kinerja layanan TI. Hal yang perlu diperhatikan dalam memantau tingkat layanan TI yaitu: 1) tingkat keparahan pelanggaran layanan; 2) persentase nasabah yang puas terhadap layanan; dan 3) persentase target layanan terpenuhi.
			1.b.10. Bank telah menerapkan praktek 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 telah mengetahui kebutuhan pemangku kepentingan dan memastikan kebutuhan tersebut telah terintegrasi pada praktek manajemen kualitas. c. Bank telah mengelola standar, praktik, dan prosedur kualitas serta integrasikan manajemen kualitas ke dalam semua proses.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				d. Bank telah melakukan pemantauan, pengendalian, dan evaluasi terhadap kualitas proses dan layanan secara berkesinambungan sesuai standar manejemen 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 telah menetapkan dan mengelola rencana penanganan risiko keamanan informasi dan data pribadi. c. Bank telah memantau dan meninjau sistem manajemen keamanan informasi minimal 1 tahun sekali yang paling sedikit: 3) frekuensi tinjauan keamanan terjadwal; 4) jumlah temuan dalam tinjauan keamanan yang dijadwalkan secara teratur; 5) tingkat kepuasan pemangku kepentingan dengan rencana keamanan; dan 6) jumlah insiden terkait keamanan yang disebabkan oleh kegagalan

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				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 manajement tools*. b. Bank mengelola seluruh program dari portofolio investasi terkait TI sesuai dengan strategi perusahaan secara terkoordinasi. c. Bank melakukan identifikasi solusi dan analisis persyaratan sebelum akuisisi atau pengembangan untuk memastikan bahwa solusi tersebut selaras dengan sasaran strategis perusahaan yang mencakup proses bisnis, aplikasi, informasi/data, infrastruktur, dan layanan. d. Bank telah merancang solusi TI, proses bisnis, dan alur kerja sesuai dengan persyaratan perusahaandan 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

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				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 telah 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 telah mengelola perubahan terkait TI (perubahan standar dan pemeliharaan yang berkaitan dengan proses bisnis, aplikasi, dan infrastruktur) yang mencakup evaluasi dampak 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

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				awal, dan tinjauan pasca-implementasi. i. Bank menjaga ketersediaan pengetahuan dan informasi manajemen yang relevan, terkini, tervalidasi, dan andal untuk mendukung semua aktivitas proses dan untuk 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 telah 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 telah 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 fasilitas terkait seperti peralatan daya dan komunikasi.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				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 dan 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 SLA yang disepakati; dan 3) persentase masalah yang diidentifikasi dengan tepat, termasuk klasifikasi, kategorisasi, dan prioritas.
			1.b.14. Bank menetapkan rencana pemeliharaan untuk memungkinkan bisnis dan organisasi TI merespon insiden dan beradaptasi dengan cepat terhadap gangguan.	a. Bank telah 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

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				waktu terhadap fungsi bisnis 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 perusahaan sesuai tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai kebijakan keamanan, melakukan penerapan dan pemeliharaan peran keamanan informasi dan hak akses, serta melakukan pemantauan keamanan terhadap informasi perusahaan.	a. Bank telah mengelola keamanan pada level sistem aplikasi. b. Bank telah mengelola keamanan jaringan dan konektivitas. c. Bank telah mengelola keamanan *endpoint,* seperti pada laptop, desktop, server, perangkat jaringan atau perangkat aplikasi. d. Bank telah mengelola identitas pengguna dan *logical access*. e. Bank telah mengelola *physical access* ke aset TI.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				f. Bank telah mengelola *output devices* seperti *printer* dan *security tokens*. g. Bank telah mengelola kerentanan dan memantau infrastruktur untuk kejadian terkait keamanan.
			1.b.16. Aktivitas pemantauan kinerja layanan TI telah memadai.	a. Bank telah melakukan evaluasi kesesuaian TI dengan target kinerja yang disepakati minimal 1 (satu) kali dalam setahun. b. Bank telah memiliki mekanisme untuk melakukan evaluasi atas kecukupan kontrol internal. c. Bank telah mengevaluasi bahwa proses bisnis yang didukung TI patuh terhadap persyaratan perjanjian dan ketentuan peraturan perundang-undangan d. Bank telah melakukan pemeriksaan independen oleh audit internal Bank 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. *Senior Management* (Direksi, Komite Pengarah TI) terlibat secara aktif dalam penyusunan arsitektur TI.	*Senior Management* Bank terlibat secara aktif dalam proses penyusunan arsitektur TI sesuai kewenangannya. Keterlibatan

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				senior management dilihat dari adanya rapat rutin sesuai kebutuhan Bank (minimum 1 tahun sekali) untuk pembahasan terkait penyusunan arsitektur TI termasuk perubahannya apabila ada.
			2.a.3. Pengelolaan arsitektur TI secara 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; dan 4) tata kelola TI Bank. 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 terkait.	
			2.a.5. Bank memiliki mekanisme permintaan dan pemberian informasi terkait arsitektur TI ke pihak berwenang.	Bank memiliki media komunikasi yang dapat diakses oleh pihak yang berkepentingan.
			2.a.6. Pelaksanaan strategi investasi TI, akuisisi TI, dan pengambilan	a. Investasi TI dan akusisi TI Bank selaras dengan arsitektur TI Bank.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			keputusan bisnis TI selaras dengan arsitektur TI Bank.	b. Arsitektur TI Bank telah menjadi salah satu referensi pengambil 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 memastikan adanya *risk awareness* di seluruh lini bisnis Bank, yang mencakup terdapatnya: 1) *risk awareness* dari Direksi dan pejabat eksekutif; 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. d. Risiko untuk aspek penyelenggaraan TI pada risiko operasional harus dikaji ulang bersamaan dengan risiko lain

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				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 mencakup 4 (empat) langkah penting berikut: 1) melakukan pengumpulan data atau dokumen atas aktivitas terkait TI yang berpotensi menimbulkan atau meningkatkan risiko, baik dari kegiatan yang sedang maupun yang akan berjalan termasuk namun tidak terbatas pada: a) hasil kaji ulang rencana strategis bisnis, khususnya kaji ulang terhadap penilaian risiko potensial; b) hasil uji tuntas (*due dilligence*) 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

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				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 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

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				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 mencakup: 1) penetapan aset, proses, produk, atau kejadian yang mengandung risiko; 2) pengukuran atau pemeringkatan kemungkinan kejadian dan dampak (*inherent risk assessment*); 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

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				keuangan Bank. Dokumentasi 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 (*feedback*) 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.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				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; 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;

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				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) menerapan kebijakan, standar, dan prosedur, serta struktur organisasi termasuk alur kerjanya; 2) menerapkan pengendalian intern yang efektif yang dapat memitigasi risiko dalam proses TI; 3) menerapkan identifikasi persyaratan spesifik pengendalian intern yang diperlukan dalam setiap kebijakan dan prosedur yang diterapkan; 4) penetapan 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 rencana pemulihan bencana (*disaster recovery plan*/DRP) untuk setiap bagian operasional yang kritis;

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				6) penetapan 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) pemakaian 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 (SIM) yang memadai dan cakupan SIM risiko operasional telah memadai dan disampaikan secara rutin kepada Direksi.	a. Direksi memberikan arahan staretegis atas ketersediaan SIM yang dapat menghasilkan informasi yang diperlukan dalam rangka mendukung peran dan fungsi manajemen secara efektif. b. Bank telah memastikan SIM telah dapat: 1) memfasilitasi pengelolaan operasional bisnis Bank termasuk pelayanan kepada nasabah;

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				2) melakukan pencatatan dan mengumpulkan informasi secara obyektif; 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 risiko terkait keamanan siber		
5	Teknologi	5.a. Adopsi teknologi yang	5.a.1. Bank memiliki kebijakan terkait proses adopsi teknologi yang	Kebijakan terkait proses adopsi teknologi Bank mencakup:

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
		bertanggung jawab	memberi manfaat bagi Bank dan nasabah.	a. kajian/*feasibility study,* strategi, dan metode implementasi teknologi; b. rencana untuk mengadopsi teknologi tertuang pada rencana strategis teknologi informasi; c. penciptaan lingkungan yang kondusif untuk inovasi seperti antara lain program bagi pegawai, nasabah, dan mitra bisnis untuk menyampaikan ide inovasi bagi Bank; d. Proses analisis kondisi internal Bank untuk memahami strategi perusahaan, lingkungan bisnis, dan tantangan yang dihadapi Bank untuk mengidentifikasi kebutuhan adopsi teknologi informasi; e. Proses pemantauan dan pemindaian lingkungan eksternal Bank untuk mengidentifikasi teknologi baru yang memiliki potensi untuk menciptakan manfaat bagi bank dan nasabah; Proses konsultasi kepada pihak ketiga (*third-party experts*) untuk mendukung kajian atau memberikan informasi terkait potensi adopsi teknologi.
			5.a.2. Bank melakukan *feasibility study* untuk adopsi teknologi.	*Feasibility study* yang dilakukan Bank mencakup hal berikut: a. potensi bisnis dari ide inovasi yang dihasilkan dari penggunaan teknologi bagi Bank dan nasabah;

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				b. analisis berbagai aspek terkait implementasi teknologi antara lain risiko inheren teknologi, kesesuaian dengan arsitektur TI Bank, keselarasan dengan strategi bisnis Bank, dampak hukum yang ditimbulkan dari pemanfaatan teknologi, regulasi terkait pemanfaatan teknologi baru, keselarasan dengan strategi TI Bank, serta mitigasi atas risiko yang ditimbulkan; c. metode pengukuran dan pemantauan risiko yang muncul atas adopsi teknologi; perencanaan implementasi adopsi teknologi atau ide inovasi yang mencakup target output, kebutuhan anggaran dan analisis *return on investment*, jangka waktu pengembangan, akuntabilitas dari adopsi teknologi.
			5.a.3. Bank memiliki strategi implementasi TI.	Strategi implementasi TI Bank mencakup: a. keterlibatan satuan kerja terkait; b. kesesuaian adopsi sistem teknologi; c. metode implementasi antara lain *big bang, piloting* atau *paralel;* dan penggunaan sistem pendukung atau utama.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			5.a.4. Bank melakukan evaluasi atas adopsi teknologi.	Evaluasi atas adopsi teknologi mencakup: a. Bank memantau penerapan dan penggunaan teknologi untuk memastikan bahwa manfaat yang diharapkan dari penggunaan teknologi terealisasi; b. Bank menjalankan validasi terhadap teknologi/TI yang digunakan. Kegiatan validasi termasuk pada frekuensi pengembangan (misalnya tahunan atau dua tahunan) atau cakupan (yaitu antara lain tinjauan dokumentasi, data perkembangan, pengujian kinerja, backtesting, benchmarking, pengujian sensitivitas, pengujian stabilitas); Bank mengidentifikasi pelajaran terpetik dari adopsi teknologi dan merekomendasikan tindak lanjut atas hasil evaluasi.
			5.a.5. Bank menerapkan transparansi dan pengungkapan yang bertanggung jawab atas teknologi informasi yang digunakan oleh Bank untuk memastikan bahwa nasabah memahami *output* yang dihasilkan oleh sistem.	Penerapan transparansi dan pengungkapan yang bertanggung jawab mencakup: a. Bank memberikan penjelasan kepada nasabah mengenai pemahaman umum tentang sistem berbasis teknologi informasi yang digunakan oleh Bank dalam memberikan layanan kepada nasabah; dan

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				Bank telah memberikan penjelasan kepada nasabah mengenai sarana dan prosedur bagi nasabah untuk melakukan klarifikasi atas hasil sistem berbasis teknologi informasi.
		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 Republik Indonesia.	Pengelolaan pihak penyedia jasa TI dalam penyelenggaraan TI Bank secara memadai mencakup: a. Bank memahami strategi dan kebijakan terkait penggunaan pihak penyedia jasa TI dalam Penyelenggaraan TI Bank; b. Bank memahami risiko yang timbul dari penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI Bank, memastikan bahwa potensi risiko atas kegiatan penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI Bank telah diidentifikasi melalui penilaian risiko secara komprehensif, serta secara aktif memantau/mengevaluasi risiko penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI Bank secara periodik; c. 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;

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				d. Bank melakukan penilaian dan pengelolaan risiko yang spesifik terkait penempatan sistem elektronik di luar wilayah Indonesia; e. Bank menetapkan kebijakan dan prosedur yang memadai dan komprehensif terkait penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI di Bank; f. 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; Bank melakukan monitoring, pengawasan, dan evaluasi atas strategi dan kebijakan penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI Bank secara periodik paling sedikit 1 (satu) kali dalam setahun.
			5.b.2. Bank melakukan identifikasi dan pengukuran risiko atas penggunaan pihak penyedia jasa TI secara memadai.	a. Bank melakukan identifikasi dan pengukuran risiko atas penggunaan pihak penyedia jasa TI secara memadai yang mencakup: 1) melakukan identifikasi fungsi kritikal dan penting;

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				2) melakukan analisis manfaat dan biaya; dan 3) melakukan identifikasi potensi risiko dari penggunaan pihak penyedia jasa TI antara lain terkait teknologi komunikasi (*communication technology*), keamanan informasi, kelangsungan bisnis, aspek hukum dan kepatuhan, risiko reputasi, risiko operasional, risiko konsentrasi, dan dampak terhadap profil risiko Bank. b. Pengukuran risiko terkait penggunaan pihak penyedia jasa TI terintegrasi dengan pengukuran risiko terkait TI lainnya dengan menggunakan pendekatan pengukuran risiko yang sama. Hasil pengukuran risiko terkait penggunaan pihak penyedia jasa TI menghasilkan suatu tingkat risiko yang selanjutnya menjadi salah satu parameter untuk penilaian risiko TI Bank secara keseluruhan.
			5.b.3. Satuan Kerja TI/terkait melakukan uji kelayakan (*due diligence*) dan memiliki standar/prosedur yang sesuai dan memadai dalam menentukan perusahaan penyedia jasa TI.	a. Terdapat dokumen tertulis yang memuat standar dan prosedur uji kelayakan (*due diligence*) penggunaan jasa TI dengan cakupan aspek yang dinilai antara lain:

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				1) eksistensi dan sejarah perusahaan penyedia jasa TI; 2) kualifikasi, latar belakang, dan reputasi pemilik perusahaan penyedia jasa TI; 3) perusahaan lain yang menggunakan jasa yang sama dari penyedia jasa TI sebagai referensi; 4) kemampuan teknis dan efektivitas pemberian jasa, termasuk dukungan purna jual; 5) teknologi dan arsitektur sistem; 6) lingkungan pengendalian intern, sejarah pengamanan, dan cakupan audit; 7) kepatuhan terhadap hukum dan ketentuan peraturan perundang-undangan; 8) kepercayaan dan keberhasilan dalam berhubungan dengan sub kontraktor; 9) jaminan pemeliharaan; 10) kemampuan untuk menyediakan pemulihan bencana dan keberlanjutan bisnis; 11) penerapan manajemen risiko; 12) laporan hasil pemeriksaan pihak independen; 13) kondisi keuangan termasuk kaji ulang atas laporan keuangan yang telah diaudit;

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				14) rencana pengembangan; 15) kemampuan mengikuti inovasi TI; dan 16) pengamanan sistem TI. b. Satuan kerja yang bertanggung jawab telah mengimplementasikan prosedur uji kelayakan secara memadai, antara lain: 1) penggunaan jasa TI telah melalui studi kelayakan proyek pengadaan; 2) mendapatkan persetujuan manajemen; 3) terdapat pendefinisian kebutuhan pengguna; 4) memiliki pengendalian dan pengamanan sistem yang memadai; dan 5) terdapat pengujian dan implementasi produk. c. Satuan kerja TI/terkait menerapkan prosedur uji kelayakan atas penggunaan jasa TI serta dievaluasi dan dikinikan secara berkala sesuai dengan rencana strategis TI Bank. Bank menerapkan standar dan prosedur uji kelayakan atas penggunaan jasa TI serta dilakukan diaudit secara berkala oleh satuan kerja audit internal.
			5.b.4. Satuan kerja yang menjalankan fungsi TI memiliki standar isi	Satuan kerja yang menjalankan fungsi TI memiliki standar isi perjanjian kerja sama

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			perjanjian kerja sama dengan penyedia jasa TI.	dengan penyedia jasa TI yang paling sedikit memuat aspek: a. cakupan pekerjaan atau jasa; b. biaya dan jangka waktu perjanjian kerja sama; c. hak dan kewajiban Bank maupun pihak penyedia jasa TI; d. jaminan pengamanan dan kerahasiaan data, terutama data nasabah; e. jaminan tingkat pelayanan (SLA); f. SLA tetap berlaku apabila terjadi perubahan kepemilikan baik pada Bank maupun penyedia jasa TI; g. laporan hasil pemantauan kinerja penyedia jasa TI yang terkait dengan SLA; h. batasan risiko yang ditanggung oleh Bank dan penyedia jasa TI; i. persetujuan Bank secara tertulis dalam hal pihak penyedia jasa TI melakukan pengalihan sebagian kegiatan (subkontrak) kepada subkontraktor; j. tersedianya sarana komunikasi yang terkoneksi dengan jaringan internet serta pengamanan terhadap akses dan transmisi data dari dan ke Pusat Data dan/atau Pusat Pemulihan Bencana;

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				k. pengaturan yang jelas mengenai rekam cadang (*back-up*) data, kebijakan saat keadaan yang mengancam kelangsungan operasional Bank (*contingency*), perlindungan terhadap data Bank (*record protection*) termasuk perangkat keras, perangkat lunak, dan perlengkapan (*equipment*), untuk menjamin kelangsungan penyelenggaraan TI; l. pengaturan mengenai pengamanan dalam pengiriman dokumen sumber (*source document*) yang diperlukan dari dan ke Pusat Data dan/atau Pusat Pemulihan Bencana; m. kesediaan pihak penyedia jasa TI untuk diaudit baik oleh intern Bank, Otoritas Jasa Keuangan, dan/atau pihak ekstern yang ditunjuk oleh Bank maupun oleh Otoritas Jasa Keuangan dan tersedianya informasi untuk keperluan pemeriksaan, termasuk hak akses, baik secara *logic* maupun fisik terhadap data yang dikelola oleh penyedia jasa TI; n. kewajiban pihak penyedia jasa TI untuk memberikan dokumen teknis kepada Bank terkait jasa yang dikerjakan oleh penyedia jasa TI

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				antara lain alur proses TI dan struktur pangkalan data (*database*); o. kewajiban pihak penyedia jasa TI melaporkan setiap kejadian penting (*critical*) yang dapat mengakibatkan kerugian keuangan dan/atau mengganggu kelancaran operasional Bank; p. kewajiban pihak penyedia jasa TI menyampaikan hasil audit TI yang dilakukan auditor independen secara berkala terhadap penyelenggaraan Pusat Data, Pusat Pemulihan Bencana, dan/atau Pemrosesan Transaksi Berbasis Teknologi Informasi, kepada Otoritas Jasa Keuangan melalui Bank yang bersangkutan; q. tanggung jawab penyedia jasa TI dalam menyediakan sumber daya manusia (SDM) yang memiliki kualifikasi dan kompetensi sesuai jasa yang disediakan agar operasional Bank tetap terjamin; r. kewajiban pihak penyedia jasa TI untuk melakukan transfer ilmu kepada personel Bank terutama mengenai alur proses TI dan struktur pangkalan data dari sistem yang disediakan oleh pihak penyedia jasa TI;

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				s. kepemilikan dan lisensi; t. jaminan dari penyedia jasa TI bahwa penyediaan jasa masih akan diberikan kepada Bank selama periode tertentu setelah implementasi; u. perubahan, pengakhiran, atau pemutusan perjanjian termasuk dalam hal Otoritas Jasa Keuangan memerintahkan Bank menghentikan penyediaan jasa TI sebelum berakhirnya jangka waktu perjanjian; v. sanksi dan penalti terhadap alasan yang tidak jelas terhadap pembatalan perjanjian dan pelanggaran isi perjanjian; w. kewajiban kepatuhan pada hukum dan ketentuan peraturan perundang-undangan di Indonesia; x. kewajiban pemenuhan standar pengamanan sistem oleh penyedia jasa TI. y. kewajiban pemenuhan standar tingkat pelayanan oleh penyedia jasa TI. z. laporan pemantauan kinerja penyedia jasa TI. aa. perjanjian penyimpanan dokumen (*escrow agreement*). bb. kesepakatan atas review klausul perjanjian secara berkala.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			5.b.5. Satuan kerja hukum atau penasehat hukum telah meninjau ulang kontrak perjanjanjian antara Bank dan pihak penyedia jasa TI sebelum ditandatangani kedua belah pihak.	Bank memiliki pegawai yang berkompetensi untuk melakukan evaluasi atas kontrak yang terkait dengan penyediaan jasa TI.
			5.b.6. Bank melakukan koordinasi dan komunikasi yang efektif dengan pihak penyedia jasa TI mengenai aspek-aspek yang telah disepakati dalam kontrak/perjanjian kerja sama untuk memastikan kedua belah pihak memiliki pemahaman yang sama dan pihak penyedia jasa memahami dan mematuhi hal-hal yang diperjanjikan.	a. Satuan Kerja TIatau satuan kerja terkait telah melakukan koordinasi dan komunikasi yang efektif dengan pihak penyedia jasa TI mengenai aspek yang telah disepakati dalam kontrak/perjanjian 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 sudah 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 secara berkala untuk mengidentifikasi klausul yang perlu dinegosiasikan dan diperbaharui kembali, disesuaikan	a. Terdapat dokumen tertulis atau laporan mengenai peninjauan klausul perjanjian dengan penyedia jasa TI secara berkala kepada Direksi.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			dengan perubahan strategi bisnis Bank.	b. Bank melakukan koordinasi dan komunikasi yang efektif dengan pihak penyedia jasa TI mengenai penyesuaian perjanjian kerjasama 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 antara lain mencakup: a. keamanan informasi organisasi; b. pengelolaan akses; c. manajemen enkripsi dan sandi d. keamanan jaringan dan operasi e. aplikasi pemrograman antarmuka *(application programming interfaces*/API); f. lokasi data; dan kerahasiaan data pribadi konsumen.
			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.	a. Bank melakukan pemantauan dan kontrol paling sedikit dengan cakupan: 1) kinerja pihak penyedia jasa TI sesuai SLA yang disepakati dalam perjanjian; 2) masalah yang bersifat material yang dialami oleh pihak penyedia jasa TI; dan

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				3) kondisi keuangan dan hasil audit independen dari pihak penyedia jasa TI. b. Bank memiliki dokumentasi dan prosedur pelaporan secara berkala atas hasil pemantauan dan evaluasi keandalan pihak penyedia jasa TI secara berkala terkait kinerja, reputasi pihak penyedia jasa TI, dan kelangsungan penyediaan layanan.
			5.b.10. Rencana kelangsungan bisnis (*business continuity plan*/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 ketiga. b. Bank dapat 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 oleh auditor intern Bank dan audit ekstern untuk menilai pelaksanaan proses dan standar perjanjian kerja sama antara Bank dan pihak penyedia jasa TI serta	a. Rencana kerja tahunan audit intern mencakup pemeriksaan berkala terhadap proses dan standar perjanjian kerjasama dengan pihak penyedia jasa TI. b. Terdapat prosedur audit terhadap pihak penyedia jasa TI, baik dilakukan

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			dilakukan tindak lanjut atas temuan pemeriksaan.	oleh audit intern Bank maupun pihak audit ekstern yang ditunjuk oleh Bank. c. Terdapat laporan hasil audit intern dan ekstern terhadap proses dan standar perjanjian kerjasama dengan pihak penyedia jasa TI dan pelaksanaan audit intern tersebut telah berjalan dengan efektif dengan memperhatikan faktor sebagai berikut: 1) cakupan dan kedalaman audit telah meliputi seluruh proses dan standar perjanjian kerjasama 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 cakupan, prosedur, temuan audit, dan tanggapan manajemen atas 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

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				pemeriksaan tidak ditindaklanjuti oleh manajemen.
			5.b.12. Bank memiliki *exit plan* apabila terjadi gangguan pada jasa TI yang digunakan dan melakukan penilaian atas ketahanan layanan dan data yang dialihdayakan serta pengujian/simulasi terhadap kelangsungan bisnis Bank.	a. Terdapat kebijakan dan prosedur internal mengenai rencana penghentian penggunaan pihak penyedia jasa TI 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 data pribadi nasabah; 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

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				jasa TI tidak berjalan dengan efektif. b. Bank melakukan penilaian atas ketahanan 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.
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) pembangunan dan pengelolaan metadata; 2) penyusunan kebijakan dan standar penglolaan data; 3) pengelolaan kualitas data; dan/atau 4) 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, mencakup antara lain:

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				1) manajemen senior yang memimpin tata kelola data bank (*Chief Data Steward*); 2) pengawas domain data di seluruh fungsi bisnis (*Enterprise Data Steward*); 3) pemilik data yang bertanggung jawab atas klasifikasi, perlindungan, penggunaan, dan kualitas satu set data atau lebih dalam suatu organisasi (*Data Owner*); dan/atau 4) penanggung jawab atas penerapan dan pemeliharaan kontrol keamanan data tertentu untuk memenuhi persyaratan yang ditentukan oleh pemilik data (*Data Custodian*).
			6.a.2. Bank telah melakukan pengembangan dan upaya menjaga/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. Bank memastikan tingkat kepuasan pemangku kepentingan atas kualitas data.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			6.a.3. Bank memiliki kebijakan dan prosedur pengelolaan data.	a. Bank memiliki kebijakan data, mencakup paling sedikit prinsip dan tujuan bank dalam pengelolaan data dan aturan dasar yang mengatur pembuatan, akuisisi, keamanan, kualitas, dan penggunaan data dan informasi, termasuk klasifikasi data, serta pengumpulan dan pemrosesan data nasabah/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 perlindungan data sesuai peraturan perundang-undangan mengenai pelindungan data pribadi. e. Bank memiliki kebijakan dan prosedur pengumpulan dan pemrosesan data yang mencakup: 1) pemrosesan data secara adil dan transparan (data tidak diperoleh dengan cara menipu dan menjebak nasabah serta data nasabah/calon nasabah dipergunakan secara sah dan tidak dipergunakan untuk perbuatan melanggar hukum)

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				2) proses pengumpulan data nasabah/calon nasabah; 3) informasi yang diberikan kepada individu dan pelaksanaan hak individu; 4) langkah-langkah teknis dan pengelolaan keamanan data; 5) prosedur penyelesaian perselisihan dengan nasabah terkait akurasi pencatatan data nasabah; 6) pengelolaan dokumentasi setiap tahap proses pengumpulan dan pemrosesan data; 7) pelaporan kebocoran data nasabah; dan 8) analisis dampak pemrosesan data.
			6.a.4. Proses pengelolaan data sudah dilakukan secara memadai	a. Bank memiliki arsitektur data sebagai bagian dari arsitektur TI (Data Architecture dan Data Modeling & Design). b. Bank menerapkan pelindungan data dan informasi. (*Data and Information Security*). Pelindungan data dan informasi mencakup: 1) Penetapan standar pengamanan data sesuai dengan klasifikasi data; dan

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				2) Implementasi kontrol dan prosedur pengamanan data dan informasi. c. Bank mengelola integrasi dan interoperabilitas data (*Data Integration and Interoperability*). Yang dimaksud Integrasi dan Interoperabilitas data yaitu proses yang terkait dengan pergerakan dan konsolidasi data di dalam dan di antara penyimpanan data, aplikasi, dan organisasi. Integrasi dan Interoperabilitas data melibatkan mendapatkan data di tempat yang dibutuhkan, saat dibutuhkan, dan dalam bentuk yang dibutuhkan. d. Bank menerapkan pengelolaan dokumen dan konten secara memadai dalam rangka penyimpanan dan log audit (*Document and Content Management*). Yang dimaksud document and content management adalah kegiatan perencanaan, pelaksanaan, dan pengendalian untuk mengelola siklus hidup data dan informasi yang ditemukan di berbagai media yang tidak terstruktur, terutama dokumen yang diperlukan untuk pemenuhan persyaratan kepatuhan hukum dan peraturan.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				e. Bank menerapkan pengelolaan referensi dan manajemen data master (Reference and Master Data Management). 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 data terjaga dan mengurangi biaya integrasi data. f. Bank mengelola data *warehouse* dan portofolio inteligensi bisnis (*Data Warehousing and Business Intelligence*-DWBI). Yang dimaksud Portofolio *Business Intelligence* yaitu identifikasi tools yang tepat bagi komunitas dan pengguna data yang tepat. g. Bank melakukan kegiatan perencanaan, implementasi, dan pengendalian untuk memungkinkan akses data kualitas tinggi dan/atau metadata terintegrasi (*Metadata Management*). h. Bank mengelola *big data* dan *data science* dari berbagai jenis data untuk memperoleh informasi yang dapat memberikan nilai tambah (*Big Data and Data Science).*

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			6.a.5. Bank sudah melakukan pengelolaan teknologi dan operasional database secara maksimal, baik dari sisi desain dan dukungan penyimpanan data (*Data Storage and Operations*).	a. Bank menerapkan pengelolaan teknologi pangkalan data (*database*) secara memadai, mencakup: 1) pemahaman mengenai teknologi pangkalan data 2) proses evaluasi; dan 3) pengelolaan teknologi pangkalan data b. Bank menerapkan pengelolaan operasional pangkalan data secara memadai, mencakup: 1) memahami kebutuhan terkait pangkalan data, mencakup kebutuhan sistem penyimpanan *file*; kebutuhan penambahan ruang tambahan, kepatuhan terhadap regulasi, prediksi pasang surut pola penggunaan data, metode dan *tools* yang sesuai untuk akses data. 2) merencanakan kelangsungan usaha (*business continuity*) ~~j~~apabila terjadi bencana yang berdampak pada sistem penyimpanan data. Bank memastikan rencana pemulihan diterapkan pada seluruh pangkalan data dan server pangkalan data, mencakup skenario yang dapat mengakibatkan hilangnya atau

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				rusaknya data termasuk membuat cadatangan basis data dan pengujian pemulihan data secara berkala. 3) mengembangkan *database instances* yang mencakup pengelolaan terhadap lingkungan penyimpanan fisik, kontrol akses data. 4) mengelola kinerja dari pangkalan data termasuk memastikan ketersediaan ruang, optimalisasi kueri, dan faktor lain yang memungkinkan pangkalan data menarik data dalam cara yang efisien. 5) melakukan pengujian terhadap pangkalan data. 6) melakukan pengujian mencakup verifikasi bahwa serangkaian input yang diberikan menghasilkan output yang diharapkan atau pengujian atas kemampuan pemrograman untuk merespons input yang tidak biasa, ekstrem, luar biasa, atau tidak terduga.
			6.a.6. Bank telah melakukan pengelolaan data secara memadai.	Bank melakukan pengelolaan data secara memadai, meliputi: a. Komisaris dan Direksi Bank memahami prinsip–prinsip

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				pengumpulan dan pemrosesan data dalam rangka pelindungan data, secara aktif menerapkan prinsip-prinsip tersebut dalam proses pengumpulan dan pemroses data di Bank, serta bertanggung jawab atas kepatuhan terhadap prinsip-prinsip tersebut; b. Bank menetapkan kebijakan pelindungan data; c. Bank menunjuk pejabat yang bertanggung jawab terhadap pelindungan data (*data protection officer*) atau membentuk fungsi atau unit yang bertanggung jawab atas kepatuhan terhadap prinsip pemrosesan dan pengumpulan data; dan d. Bank telah menetapkan kebijakan pengelolaan data secara memadai.
		6.b. Pelindungan Data	6.b.1. Kebijakan dan strategi perlindungan data telah disusun dengan pendekatan "*data protection by design*"	Definisi data *protection by design* adalah : a. Pelindungan data menjadi aspek penting dalam mengembangkan sistem, produk, layanan dan proses bisnis. b. Pelindungan data menjadi komponen penting dalam proses layanan dan sistem.
			6.b.2. Proses identifikasi dasar hukum untuk pengumpulan dan pemrosesan	a. Bank telah meninjau tujuan dari aktivitas pemrosesan data nasabah

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			data nasabah/calon nasabah telah memadai.	dan memiliki dasar hukum yang sesuai untuk masing-masing aktivitas. b. Bank telah mengidentifikasi bahwa pemrosesan data yang diperlukan Bank digunakan untuk tujuan tertentu dan tidak terdapat metode lain untuk mencapai tujuan tertentu selain menggunakan data yang diminta. c. Bank memiliki dasar hukum yang sah dalam melakukan pemrosesan data, antara lain: 1) diwajibkan Perundangan (l*egal obligation*) dalam rangka pengumpulan dan pemrosesan. Dasar hukum ini berlaku bagi Bank jika Bank diharuskan melakukan pemrosesan data agar patuh terhadap Undang-Undang 2) pemenuhan *public task* dalam rangka pengumpulan dan pemrosesan data. Dasar hukum ini berlaku bagi Bank jika Bank melaksanakan tugas tertentu untuk kepentingan umum yang ditetapkan dengan undang-undang; atau menjalankan wewenang resmi (misalnya tugas, fungsi, tugas, atau wewenang badan publik)

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				yang ditetapkan dalam peraturan perundang-undangan yang berlaku. 3) *Legitimate interest* dalam rangka pemrosesan data Dasar hukum ini hanya dapat dipergunakan oleh Bank yang memenuhi kriteria *Legitimate Interest Assesment* (LIA). LIA terdiri dari: a) *Purpose test* yaitu apakah bank memiliki kepentingan yang sah. b) *Necessity test* yaitu apakah pengolahan data dibutuhkan untuk mencapai tujuan atau kepentingan yang sah. c) *Balancing test* yaitu apakah kepentingan individu mengesampingkan kepentingan bank yang sah. Bank menyeimbangkan kepentingan Bank dan kepentingan nasabah. Dalam hal nasabah tidak memberikan persetujuan kepada Bank untuk menggunakan data nasabah atau dalam hal pemrosessan data dinilai nasabah dapat merugikan nasabah maka kepentingan nasabah dapat

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				mengesampingkan kepentingan Bank. Dalam hal terdapat konflik kepentingan, kepentingan Bank dapat didahulukan sepanjang terdapat alasan yang jelas akan dampaknya terhadap nasabah. Proses pemenuhan *legitimate interest* memadai mencakup : a) Bank telah memeriksa bahwa kepentingan yang sah adalah dasar yang paling tepat. b) Bank telah memahami tanggung jawab untuk melindungi kepentingan individu. c) Bank telah melakukan *Legitimate Interest Assesment* (LIA) dan mencatatnya, untuk memastikan bahwa bank dapat membenarkan keputusannya. d) Bank telah mengidentifikasi kepentingan yang sah yang relevan. e) Bank telah memeriksa bahwa pemrosesan diperlukan dan tidak ada cara lain yang tidak terlalu mengganggu untuk mencapai hasil yang sama. f) Bank telah melakukan *balancing test*, dan yakin

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				bahwa kepentingan nasabah tidak mengesampingkan kepentingan Bank yang sah. g) Bank hanya menggunakan data nasabah dengan cara yang wajar. h) Bank telah mempertimbangkan terkait perlindungan data. i) Jika hasil LIA mengidentifikasi dampak privasi yang signifikan, Bank telah mempertimbangkan apakah bank juga perlu melakukan *Data Protection Impact Assesment*. j) Bank terus meninjau LIA, dan mengulanginya jika keadaan berubah. k) Bank menyertakan informasi tentang kepentingan sah dalam informasi *privacy note* d. Bank telah melakukan identifikasi terhadap kondisi untuk melakukan melakukan proses data. e. Bank telah memasukan informasi tujuan pemrosesan data dan dasar hukum untuk memproses data dalam *privacy notice*.
			6.b.3. Proses permintaan consent nasabah dalam rangka proses	a. Bank memastikan persetujuan nasabah/calon nasabah dapat

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			pengumpulan dan pemrosesan data nasabah telah memadai.	digunakan merupakan dasar hukum yang tepat untuk pengumpulan dan pemrosesan data. b. Bank telah membuat permintaan consent dan permintaan tersebut terpisah dari syarat dan ketentuan pemrosesan data. c. Permintaan persetujuan bank tidak berupa penggunaan kotak (*tick box*) yang telah dicentang sebelumnya atau jenis persetujuan *default* lainnya. d. Permintaan persetujuan disusun dalam bahasa yang jelas dan sederhana yang mudah dimengerti. e. Bank telah menjelaskan kepada nasabah mengapa bank menginginkan data dan apa yang akan dilakukan terhadap data nasabah. f. Bank telah memberikan opsi pilihan persetujuan persetujuan untuk setiap tujuan dan jenis pemrosesan data yang berbeda. g. Bank telah memberikan informasi semua institusi yang terlibat dalam pemrosesan data sebagai akibat persetujuan nasabah/calon nasabah. h. Bank telah memberikan informasi hak nasabah untuk menarik persetujuan yang telah diberikan kepada bank.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				i. Bank memastikan bahwa nasabah memiliki hak untuk menolak pemberian persetujuan j. Bank tidak menjadikan pemberian consent atas hal-hal yang tidak terkait langsung dengan nasabah sebagai prasyarat pemberian layanan Bank. k. Bank melakukan penghapusan data setelah masa retensi data (hanya untuk kepentingan maintenance/audit/rekam jejak) berakhir sesuai dengan peraturan perundang-undangan mengenai pelindugan data pribadi.
			6.b.4. Proses rekam dan pengelolaan consent nasabah dalam rangka proses pengumpulan dan pemrosesan data telah memadai.	a. Bank memelihara catatan mengenai kapan dan bagaimana consent persetujuan nasabah/calon nasabah diperoleh. b. Bank menyimpan catatan tepat sesuai dengan apa yang disampaikan nasabah/calon nasabah saat pemberian persetujuan. c. Bank meninjau consent berkala melalui pemeriksaan khusus atau sistem pencatatan secara periodik untuk memastikan bahwa hubungan, pemrosesan, dan tujuannya tidak berubah. d. Bank memiliki proses untuk (memastikan konsistensi antara persetujuan nasabah, pengumpulan

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				pemrosesan dan tujuan) memperbarui consent pada interval (ketika ada permintaan perubahan persetujuan) yang sesuai. e. Bank memberikan kemudahan untuk nasabah/calon nasabah untuk menarik persetujuan kapan saja, dan mempublikasikan cara melakukannya serta bertindak atas penarikan persetujuan sesegera mungkin.
			6.b.5. Kerjasama antara bank dengan pihak ketiga untuk aktivitas pemrosesan data didukung oleh kontrak kerjasama yang memadai	a. Kontrak mencakup elemen: 1) ruang lingkup dan durasi pemrosesan; 2) sifat dan tujuan pemrosesan; 3) jenis data pribadi dan kategori data nasabah: kategori nasabah, data pribadi; dan 4) kewajiban dan hak pengendali data. b. Kontrak mencakup persyaratan: 1) pemroses hanya boleh bertindak berdasarkan instruksi tertulis dari bank (kecuali diharuskan oleh hukum untuk bertindak tanpa instruksi tersebut); 2) pemroses wajib memastikan bahwa orang yang memproses data tunduk pada kewajiban kerahasiaan;

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				3) pemroses wajib mengambil tindakan yang tepat untuk memastikan keamanan pemrosesan. Pemroses dapat menggunakan sub-pemroses dengan persetujuan dari bank berdasarkan kontrak tertulis; 4) pemroses wajib membantu bank dalam menyediakan akses data dan mengizinkan nasabah menggunakan haknya; 5) pemroses wajib membantu bank dalam memenuhi kewajiban terkait keamanan pemrosesan, pemberitahuan pelanggaran data pribadi, dan penilaian dampak perlindungan data; 6) pemroses wajib menghapus atau mengembalikan semua data pribadi ke Bank seperti yang sesuai kontrak; 7) pemroses wajib tunduk pada audit dan inspeksi, memberikan informasi apa pun yang diperlukan bank untuk memastikan bahwa pemroses dan bank memenuhi aturan perlindungan data, dan segera memberi tahu bank jika diminta untuk melakukan sesuatu yang melanggar aturan atau perlindungan data;

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				8) tidak tertuang di dalam kontrak yang membebaskan pemroses dari tanggung jawab dan kewajiban langsungnya sendiri dan mencerminkan ganti rugi yang telah disepakati.
			6.b.6. Proses pengumpulan data nasabah/calon nasabah dilakukan memenuhi prinsip adil.	a. Data tidak diperoleh dengan cara menipu dan menjebak nasabah. b. Data nasabah/calon nasabah dipergunakan secara sah dan tidak dipergunakan untuk perbuatan melanggar hukum.
			6.b.7. Proses identifikasi, dokumentasi dan evaluasi tujuan proses pengumpulan dan pemrosesan data telah memadai (*purpose limitation*).	a. Bank melakukan identifikasi tujuan pemrosesan data. b. Bank mendokumentasikan tujuan dari pemrosesan data. c. Bank mencantumkan tujuan dari pemrosesan data dalam informasi kepada nasabah/calon nasabah. d. Dalam hal bank akan mengunakan data nasabah untuk tujuan lain, bank melakukan identifikasi apakah proses data selaras dengan tujuan awal atau telah mendapat persetujuan dari nasabah untuk tujuan lain.
			6.b.8. Proses pengumpulan data nasabah/calon nasabah telah memenuhi prinsip *data minimization*	Bank memiliki prosedur untuk memastikan data yang dibutuhkan sesuai dengan tujuan.
			6.b.9. Proses pemeriksaan keakuratan data nasabah/calon nasabah telah	a. Bank memiliki prosedur untuk memastikan akurasi data yang

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			dilakukan secara memadai (Prinsip akurat).	dikumpulkan dan bank merekam sumber perolehan data yang dimiliki. b. Bank memiliki prosedur terkait proses perubahan data. c. Bank memiliki data audit trail untuk mengetahui kapan perubahan data. d. Bank memberikan hak kepada nasabah untuk memperbaiki data.
			6.b.10. Proses pengelolaan waktu penyimpanan data telah dilakukan secara memadai (Prinsip *storage limitation/*batasan pengelolaan penyimpanan)	a. Bank mengklasifikasikan data nasabah sesuai dengan pengelolaan dan peruntukannya. b. Bank memiliki dasar pertimbangan penetapan jangka waktu penyimpanan data nasabah. c. Bank memiliki kebijakan periode retensi data. d. Bank secara berkala memiliki prosedur untuk mereviu informasi dan menghapus data yang tidak lagi dibutuhkan. e. Bank memiliki prosedur untuk menghapus data nasabah sesuai permintaan nasabah. f. Bank mengidentifikasi kebutuhan data yang disimpan untuk riset dan statistik.
			6.b.11. Proses pengamanan data telah dilakukan secara memadai (Prinsip *integrity* dan *confidentiality*).	a. Bank memiliki kebijakan keamanan informasi dan melakukan manajemen risiko yang memadai analisis risiko. b. Bank memiliki kebijakan keamanan informasi yang ditinjau secara berkala

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				dan mengambil tindakan untuk memastikan kebijakan diterapkan. c. Dalam menentukan tindakan pengamanan data, Bank mempertimbangkan aspek teknis dan aspek biaya dan Bank menerapkan teknis keamanan informasi sesuai dengan kerangka atau standar tertentu. d. Bank melakukan pengujian bahwa kebijakan keamanan informasi ditinjau secara berkala dan disesuaikan jika diperlukan. e. Bank melakukan enkripsi dan/atau pseudonimisasi jika diperlukan. f. Bank melakukan pengujian sistem pengamanan data secara berkala untuk mengukur dan memastikan efektifitas keamanan data.
			6.b.12. Proses penilaian dampak pelindungan data (*data protection impact assessment*/DPIA) yang dilakukan oleh Bank memadai.	a. Bank melakukan identifikasi kriteria data yang berisiko tinggi sesuai dengan kriteria yang diatur dalam peraturan perundang-undangan mengenai pelindungan data pribadi. b. Bank menetapkan kriteria proyek berisiko tinggi yang harus menggunakan DPIA dan kriteria potensi risiko tinggi dengan mengacu pada peraturan perundang-undangan mengenai pelindungan data pribadi.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			6.b.13. Proses dokumentasi aktivitas pemrosesan data telah memadai.	a. Bank mendokumentasikan aktivitas pemrosesan data pribadi oleh Bank. b. Bank telah melakukan audit informasi untuk mengetahui data pribadi apa yang dimiliki oleh Bank dan meninjau kebijakan, prosedur, kontrak, dan perjanjian Bank untuk menangani bidang seperti penyimpanan, keamanan, dan berbagi data. c. Sebagai bagian dari catatan aktivitas pemrosesan Bank, Bank mendokumentasikan, atau menautkan ke dokumentasi, tentang informasi yang diperlukan untuk pemberitahuan privasi, catatan persetujuan, kontrak pengontrol-prosesor, lokasi data pribadi, laporan penilaian dampak perlindungan data, dan catatan pelanggaran data pribadi. d. Bank mendokumentasikan kegiatan pemrosesan Bank dalam bentuk elektronik sehingga Bank dapat menambah, menghapus, dan mengubah informasi dengan mudah.
			6.b.14. Prosedur pemberian informasi pengumpulan dan pemrosesan data kepada nasabah telah memadai *(right to be informed*).	a. Bank memberikan informasi kepada nasabah dalam *privacy note* informasi sebagai berikut: 1) nama dan detil kontak Bank; 2) nama dan detik kontak representative bank (jika relevan);

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				3) nama dan detil kontak *data protection officer* (jika relevan); 4) tujuan pemrosesan data; 5) dasar hukum pemrosesan data; 6) kepentingan sah untuk pemrosesan data (jika relevan); 7) kategori data individu yang diperoleh; 8) penerima atau kategori penerima data; 9) detil transfer data kepada pihak ketiga (jika relevan); 10) periode retensi data; 11) hak nasabah terkait pemrosesan data; 12) hak nasabah untuk menarik kembali persetujuan/*consent*; 13) hak untuk mengajukan keluhan kepada regulator; 14) sumber data nasabah (jika diperoleh tidak langsung dari nasabah); dan 15) detil dari proses *automated decision making* termasuk *profiling* (jika relevan). b. Bank memberikan informasi tersebut secara ringkas, transparan, mudah diakses dan menggunakan bahasa sederhana dan jelas.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			6.b.15. Prosedur pemberian akses data dan informasi kepada nasabah telah memadai (*right of access*).	a. Bank memiliki kebijakan permintaan akses data pribadi yang dikelola oleh bank apabila diminta oleh nasabah. b. Bank memilliki mekanisme untuk melakukan verifikasi hak akses. c. Bank telah memiliki rincian data ketika dimintakan akses data nasabah sesuai ketentuan yang berlaku. d. Bank memahami kondisi yang memungkinkan bank untuk menolak permintaan akses data dan informasi.
			6.b.16. Prosedur penangan permintaan nasabah untuk pengkinian/memperbaiki/menghapus data nasabah telah memadai (*right to rectification and right to erasure*).	a. Bank memiliki kebijakan mengenai pengkinian dan penghapusan data. b. Bank memahami kondisi yang memungkinkan Bank untuk menolak permintaan pengkinian data nasabah. c. Bank memiliki proses untuk memastikan bahwa bank menanggapi permintaan untuk perbaikan/penghapusan tanpa penundaan yang tidak semestinya. d. Bank memiliki prosedur untuk memberi tahu pemilik data (nasabah) dalam hal Bank melakukan perubahan atau penghapusan data yang telah Bank bagikan kepada pemilik data. e. Bank memiliki prosedur untuk menginformasikan penerima data dalam hal Bank melakukan

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				penghapusan datayang telah Bank bagikan kepada penerima data.
			6.b.17. Proses penanganan permintaan nasabah untuk pembatasan pemrosesan data telah memadai (*right to restrict processing*).	a. Bank memiliki kebijakan penanganan permintaan nasabah untuk pembatasan pemrosesan data dan Bank memahami kapan hak dapat diberlakukan. b. Bank memiliki proses untuk memastikan bahwa Bank menanggapi permintaan pembatasan pemrosesan data. c. Bank telah menyadari keadaan ketika bank dapat memperpanjang batas waktu untuk menanggapi permintaan. d. Bank telah memiliki prosedur untuk membatasi pemrosesan data pribadi di sistem Bank dan memiliki prosedur untuk memberi tahu penerima mana pun jika Bank membatasi data apa pun yang telah bank bagikan dengan mereka.
			6.b.18. Proses permintaan nasabah untuk sharing/transfer datanya ke pihak lain memadai (*Right to data portability*).	a. Bank memiliki kebijakan penanganan permintaan nasabah untuk sharing/transfer datanya ke pihak lain. b. Bank memiliki kebijakan tentang cara mencatat permintaan yang bank terima secara lisan. c. Bank memiliki proses untuk penanganan permintaan nasabah

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				untuk sharing/transfer data ke pihak lain dan menggunakan metode yang aman untuk mengirimkan data pribadi. d. Bank memahami kondisi yang memungkinkan bank untuk menolak permintaan nasabah untuk sharing/transfer datanya ke pihak lain.
			6.b.19. Proses penanganan penolakan nasabah atas pemrosessan data pribadi telah memadai (*right to object*).	a. Bank memiliki kebijakan atau prosedur bagi nasabah untuk mengajukan keberatan atas pemrosesan data pribadi secara otomatis. b. Bank memiliki proses untuk menolak keberatan dan mengetahui informasi yang perlu bank berikan kepada nasabah/calon nasabah ketika bank melakukan penolakan keberatan c. Bank memahami prosedur menginformasikan nasabah/calon nasabah mengenai hak nasabah/calon nasabah untuk menolak selain memasukkannya ke dalam pemberitahuan privasi Bank. d. Bank memiliki prosedur untuk menghapus atau menghentikan pemrosesan data pribadi.
		6.c. Transfer Data	6.c.1. Bank telah memiliki kebijakan, prosedur dan standar mengenai	Bank memastikan bahwa kebijakan tersebut mencakup paling sedikit:

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			pengendalian pertukaran data dan infomasi yang memadai.	a. jenis data nasabah untuk pertukaran data dan informasi; b. kebutuhan konsensus nasabah untuk pertukaran data dan informasi; c. mekanisme permintaan dan pemberian informasi oleh pihak ekstern; d. kepemilikan kebijakan dan operasional data transfer di internal Bank kepada pihak di luar 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 data dan informasi; h. alokasi tanggung jawab pihak yang terlibat dalam pertukaran data atas risiko kebocoran data nasabah
			6.c.2. Kerjasama dengan pihak ketiga yang menyebabkan terjadinya pertukaran data telah dipayungi oleh perjanjian pertukaran data.	Perjanjian mencakup aspek pertukaran data paling sedikit memuat: a. pihak pengendali data pada setiap tahap pertukaran data; b. tujuan pertukaran data yang meliputi: 1) tujuan khusus mengapa pertukaran data dibutuhkan; dan

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				2) keuntungan yang diperoleh dari pertukaran data, tidak digunakan untuk peruntukan lain selain yang tercantum dalam perjanjian; c. pihak ketiga lain yang mungkin terlibat dalam pertukaran data; d. data yang akan dipertukarkan; e. prosedur pemenuhan hak subjek data seperti: akses subjek data terhadap data yang dilakukan proses pertukaran data; f. pengaturan teknis pertukaran data (contoh: standar data, standar keamanan informasi, prosedur permintaan akses data, penghentian pertukaran data; *Service Level Agreement* pengiriman data dan penanganan masalah kegagalan perpindahan data); dan g. Pengaturan Perjanjian Kerahasiaan (*Non-Disclosure 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 telah menerapkan pengamanan untuk melindungi data	a. Bank menerapkan serangkaian langkah teknis untuk memastikan

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			nasabah yang dipertukarkan sesuai dengan klasifikasi data.	keamanan jaringan komunikasi yang dipergunakan. b. Bank melakukan enkripsi atas data yang dipertukarkan. c. Bank menerapkan standar integritas data. d. Bank menerapkan metode otentifikasi. e. Bank menerapkan standar otorisasi.
			6.c.4. Bank telah menerapkan pelindungan data nasabah ketika mempertukarkan data nasabah.	a. Bank memperoleh consent nasabah untuk dapat mentransfer data pribadinya. b. Bank pelaksana transfer Data nasabah dan Bank penerima transfer Data nasabah mematuhi peraturan perundang-udangan mengenai pelindungan data pribadi. c. ank hanya dapat melakukan transfer Data nasabah kepada pihak lain dalam wilayah hukum Negara Republik Indonesia. d. Bank dapat melakukan transfer data 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-iudangan mengenai pelindungan data pribadi.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				e. Dalam hal poin d tidak terpenuhi, Bank memastikan terdapat kebijakan pelindungan data pribadi yang memadai dan bersifat mengikat.
7	Kolaborasi	7.a. Kerja Sama Kemitraan	7.a.1. Komisaris dan Direksi menetapkan strategi dan kebijakan terkait kemitraan.	a. Penerapan strategi terkait kemitraan telah dimuat dalam rencana kerja strategis TI. b. Penerapan strategi dan kebijakan terkait kemitraan telah sesuai dengan visi, misi, 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 dengan telah memiliki tugas dan tanggung jawab unitsatuan kerja yang terlibat dalam proses penyediaan jasa TI.
			7.a.2. Perjanjian kemitraan oleh Bank sudah memiliki standar baku perjanjian kemitraan.	Standar baku perjanjian kerja sama kemitraan oleh Bank meliputi: a. memenuhi persyaratan penyediaan jasa TI tidak menjadi salah satu kegiatan pokok Bank; b. memenuhi prinsip kehati-hatian;

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				c. memperhatikan analisis biaya dan manfaat; d. memenuhi prinsip hubungan kerja sama secara wajar; e. memenuhi ketentuan peraturan perundang-undangan; f. terdapat klausul bahwa masing-masing pihak akan bertanggung jawab atas keamanan sistemnya sendiri; g. 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; h. mitra bertanggung jawab untuk setelah memperoleh persetujuan konsumen dan dalam parameter kewenangannya; i. mitra termasuk pihak ketiga lain mitra bertanggung jawab untuk menerapkan proses pencegahan penipuan atau penyimpangan (*fraud*); j. Bank dan/atau mitra bertanggung jawab atas kekurangan pelayanan dalam pelaksanaan transaksi karena kesalahan atau kelalaiannya; k. mitra bertanggung jawab atas segala penyalahgunaan merek Bank dan untuk setiap aktivitas yang menyebabkan kerusakan reputasi

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				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; l. mitra telah memiliki asuransi yang memadai untuk menutupi seluruh kewajibannya berdasarkan Kontrak API setiap saat selama jangka waktu kontrak; dan m. Bank tidak akan bertanggung jawab atau melanggar kontrak kemitraan: 1) untuk setiap pelanggaran oleh Bank atas kontrak kemitraan atau kegagalan Bank untuk menyediakan akses, sejauh kegagalan tersebut disebabkan oleh kegagalan mitra untuk memenuhi kewajiban mitra berdasarkan kontrak kemitraan; dan 2) kehilangan atau kerusakan apapun yang disebabkan secara langsung atau tidak langsung oleh tindakan atau kelalaian pihak ketiga yang bekerja sama dengan mitra untuk menerima layanan berdasarkan kontrak kemitraan. n. Bank dan mitra memiliki *service managers* yang bertugas sebagai

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				kontak utama untuk segala hal yang berkaitan dengan Kontrak.
			7.a.3. Bank memastikan aspek pelindungan data konsumen di dalam kontrak kemitraan.	a. Bank dan mitra hanya dapat memproses data konsumen sesuai dengan ketentuan perundang-undangan mengenai pelindungan data pribadi yang berlaku. b. Mitra menggunakan dan mengamankan semua data yang disediakan oleh Bank dan/atau konsumen sesuai dengan persyaratan keamanan yang disepakati oleh Bank dan mitra. c. Permintaan data kepada konsumen, sebatas keperluan pemberian layanan Bank kepada konsumen. d. Bank mengecek persetujuan konsumen dari mitra meliputi: 1) prosedur untuk memberikan persetujuan dan bagaimana persetujuan harus ditarik (*withdrawn*); 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

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				4) mitra hanya dapat mengakses data konsumen terbatas dengan jangka waktu tertentu (syarat waktu dapat ditentukan lebih lanjut antar Bank dan mitra). 5. Mitra menggunakan alat pendeteksi untuk memindai *malware*. 6. Mitra melakukan analisis risiko secara teratur dan mengambil langkah untuk memperbarui tindakan pengamanan yang diperlukan untuk memperbaiki insiden keamanan atau kerentanan yang teridentifikasi. 7. *Service manager* melakukan pertemuan secara berkala untuk membahas setiap pengaduan konsumen yang diterima oleh mitra. *Service manager* Bank berhak untuk meminta informasi lebih lanjut tentang pengaduan konsumen atau penanganannya kepada mitra. 8. *Service manager* membahas perselisihan dalam jangka waktu tertentu yang telah ditentukan. 9. Bank menetapkan strategi kelangsungan bisnis apabila layanan mitra tidak dapat diakses oleh Bank atau mengalami permasalahan, untuk memastikan bahwa layanan kepada konsumen tetap berjalan.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				10. Bank menetapkan proses alternatif memiliki keamanan yang memadai.
			7.a.4. Satuan kerja terkait melakukan identifikasi, pengukuran, pemantauan, dan pengendalian risiko atas kemitraan.	Satuan Kerja terkait mempertimbangkan beberapa hal dalam melakukan identifikasi, pengukuran, pemantauan, dan pengendalian risiko risiko atas penyediaan jasa TI 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 (*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.
			7.a.5. Bank memiliki kebijakan terkait pengujian kelayakan mitra.	Kebijakan antara lain memuat pelaksanaan kemitraan terkait: d. kesehatan keuangan mitra (termasuk kemampuan mitra untuk memenuhi kewajiban yang mungkin timbul dari penyediaan layanan mereka dan perlindungan asuransi dimiliki oleh mitra);

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				e. mitra memiliki semua izin atau otorisasi yang diperlukan (misalnya, peraturan) untuk kegiatan yang ingin dilakukan (jika ada f. tindakan dan kontrol keamanan mitra, termasuk kebijakan keamanan siber dan pemantauannya; g. Bank memiliki BCP dan DRP; h. operasi dan kontrol manajemen risiko keamanan yang dimiliki mitra, khususnya terkait dengan perlindungan 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; i. tidak memiliki reputasi buruk dan tidak melakukan kegiatan yang melanggar hukum atau ketentuan; dan j. pemantauan terhadap kinerja dan reputasi mitra.
			7.a.6 Bank melakukan pemantuan terhadap kinerja dan reputasi mitra.	Pemantauan terhadap kinerja dan reputasi mitra sebagai berikut: k. mitra tidak lagi memenuhi kriteria kelayakan (*eligibility criteria*); l. mitra telah melanggar salah satu ketentuan yang tercantum pada

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				bagian "*customer authentication and consent*"; m. mitra menggunakan API untuk tujuan yang tidak diungkapkan kepada Bank selama proses orientasi; n. mitra menyatakan atau mengakui bahwa kepailitannya atau tidak mampu membayar utangnya pada saat jatuh tempo atau pada saat diajukannya proses kepailitan o. mitra memasukkan *malware* yang dapat mengganggu sistem Bank; p. mitra menawarkan layanannya atau melakukan sendiri dengan cara yang dapat merusak reputasi Bank, baik dengan konsumen maupun dengan pasar secara lebih luas, termasuk namun tidak terbatas pada regulator; q. mitra telah menggunakan data konsumen selain yang diizinkan; r. terdapat dugaan pelanggaran keamanan oleh mitra; s. terdapat dugaan pelanggaran kontrak terkait kemitraan oleh mitra.
			7.a.7 Bank memastikan penerapan metode otentikasi yang aman bagi nasabah yang mengakses layanan Bank melalui mitra.	Dalam rangka melakukan autentikasi terhadap nasabah yang mengakses layanan Bank melalui mitra: t. Bank memiliki kendali atas proses otentikasi dan data tidak disimpan oleh mitra sebelum ada persetujuan konsumen;

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				u. mitra tidak menyimpan data kredensial konsumen; v. penggunaan perangkat atau saluran terpisah untuk menyelesaikan otentikasi konsumen memiliki tingkat keamanan tinggi; w. Bank memproses permintaan data konsumen yang diminta oleh mitra setelah Bank melakukan otentikasi konsumen dan mitra; dan x. Bank memberikan data yang diperlukan kepada mitra untuk layanan yang diakses oleh konsumen setelah Bank meyakini bahwa proses otentikasi telah berjalan sesuai prosedur yang telah disepakati.
			7.a.8. Bank menentukan dan mendokumentasikan standar teknis interkoneksi antara mitra dan Bank.	a. Bank telah mendokumentasikan standar teknis dan keamanan dan standar data yang mencakup protokol komunikasi, struktur dan format data, metode otentikasi, metode otorisasi, metode enkripsi, dan persyaratan pengelolaan akses. b. Bank memberitahukan mitra apabila terjadi perubahan di standar teknis interkoneksi. c. Bank memiliki manajemen pengelolaan kunci (*key management*). d. Bank menetapkan kualitas data yang diberikan kepada mitra.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				e. Bank telah memenuhi kualitas data yang diminta dan diberikan kepada mitra. f. Mitra pernah melakukan aduan karena data yang diberikan kepada Bank tidak sesuai dengan perjanjian.
		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 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

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				TI berada dalam satu grup atau kelompok dengan Bank dan penggunaan aplikasi ditujukan untuk mendukung kegiatan operasional yang umum.
8	Pelindungan Konsumen	8.a. Pemenuhan Aspek Pelindungan dan Pelayanan Konsumen	8.a.1. Bank memperhatikan aspek *customer engagement* dan memiliki strategi untuk *retain customer* dalam menilai keberhasilan produk dan layanan Bank	a. Bank memiliki mekanisme untuk mengukur *customer engagement* dalam rangka melakukan *improvement*. b. Bank memiliki stratregi untuk mempertahankan konsumen.
			8.a.2. Bank menyediakan layanan dan/atau produk yang ramah bagi penyandang disabilitas dan memiliki standar minimal pelayanan keuangan kepada konsumen/calon konsumen 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 non fisik yaitu dapat digunakan oleh semua orang, sederhana, fleksibel dalam penggunaannya, komunikasi yang efektif, dan mentoleransi kesalahan.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				3) Prinsip desain universal untuk pelayanan dokumen yaitu dapat digunakan oleh semua orang, sederhana, fleksibel dalam penggunaannya, komunikasi yang efektif, dan mentoleransi kesalahan. 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 CAPTCHA, tersedia dalam kode audio atau pertanyaan matematika sederhana; 5) menyediakan waktu yang cukup untuk memasukkan kata sandi yang diterima melalui SMS atau surat elektronik; dan 6) pesan kekeliruan (*error*) tersedia dalam bentuk teks dan audio.
			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,

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
				dalam mengembangkan produk dan layanan. b. Bank melakukan kolaborasi dengan nasabah dalam menciptakan produk Bank dengan melibatkan baik ide ataupun peran serta nasabah dalam proses penyusunan produk dan layanan Bank.
			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 mencakup: 1) *Product Quality* - persepsi nasabah terhadap kualitas produk dan layanan digital Bank. 2) *Customer support quality* - persepsi nasabah terhadap kualitas *customer support* Bank. 3) *Positioning* - persepsi nasabah terhadap produk Bank. 4) *Price* - persepsi nasabah terhadap suku bunga simpanan dan kredit yang ditawarkan oleh Bank 5) *Reputation* - persepsi nasabah terhadap *review mobile banking app*. b. Bank telah memiliki saluran umpan balik untuk mendapatkan masukan dari nasabah.

No	Domain	Subdomain	Kontrol	Penjelasan/Kriteria Pemenuhan Kontrol
			8.a.5. Bank mengevaluasi produk dan layanan berdasarkan pengalaman nasabah.	a. Bank menganalisis pengalaman nasabah dalam menggunakan produk dan/atau layanan digital yang diberikan oleh Bank, antara lain: 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; 3) *speed of delivery,* yaitu kecepatan akses aplikasi Bank. b. Bank melakukan perbaikan atas produk dan layanan digital.

Ditetapkan di Jakarta

pada tanggal

KEPALA EKSEKUTIF PENGAWAS PERBANKAN

OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA,

DIAN EDIANA RAE

LAMPIRAN II

RANCANGAN SURAT EDARAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR /SEOJK.03/2023

TENTANG

PENILAIAN TINGKAT MATURITAS DIGITAL BANK UMUM

Kertas Kerja Penilaian Kualitas Penerapan Kontrol atas Tingkat Maturitas Digital Bank

No.	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 teknologi informasi (TI)				
…	…	…	…				
…	…	…	…				

Keterangan:

1) Diisi dengan domain, subdomain, dan kontrol sebagaimana tercantum dalam Lampiran I Matriks Kontrol Penerapan Domain Penilaian Tingkat Maturitas Digital Bank.
2) Diisi dengan penilaian atas kondisi penerapan kontrol pada Bank, yaitu: **"Belum Diterapkan", "Belum Memadai", "Cukup Memadai", "Memadai",** atau **"Sangat Memadai"**. Penilaian mempertimbangkan penjelasan/kriteria pemenuhan kontrol sebagaimana tercantum dalam Lampiran I Matriks Kontrol Penerapan Domain Penilaian Tingkat 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

KEPALA EKSEKUTIF PENGAWAS PERBANKAN

OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA,

DIAN EDIANA RAE

LAMPIRAN III

RANCANGAN SURAT EDARAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR /SEOJK.03/2023

TENTANG

PENILAIAN TINGKAT MATURITAS DIGITAL BANK UMUM

B. Matriks Penetapan Kualitas Penerapan Domain

Peringkat	Definisi Peringkat
1 (*Strong*)	Kualitas penerapan 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 teknologi yang bertanggung jawab sangat memadai dan penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI sangat andal dan teruji; e. tata kelola data, pelindungan data, dan transfer data secara keseluruhan sangat memadai sesuai ketentuan perundangan-undangan yang berlaku; f. kerja sama kemitraan dan penyediaan jasa TI oleh Bank dilaksanakan secara sangat memadai; 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 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 teknologi yang bertanggung jawab memadai dan penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI andal dan teruji; e. tata kelola data, pelindungan data, dan transfer data secara keseluruhan memadai sesuai ketentuan perundangan-undangan yang berlaku;

Peringkat	Definisi Peringkat
	f. kerjasama kemitraan dan penyediaan jasa TI oleh Bank dilaksanakan secara memadai; 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 domain cukup memadai. Meskipun persyaratan minimum terpenuhi, terdapat beberapa kelemahan yang membutuhkan perhatian manajemen. 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 teknologi yang bertanggung jawab cukup memadai dan penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI cukup andal dan teruji; e. tata kelola data, pelindungan data, dan transfer data secara keseluruhan cukup memadai sesuai ketentuan perundangan-undangan yang berlaku; f. kerjasama kemitraan dan penyediaan jasa TI oleh Bank dilaksanakan secara cukup memadai; 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 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;

Peringkat	Definisi Peringkat
	d. penerapan adopsi teknologi yang bertanggung jawab kurang memadai dan penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI kurang andal dan teruji; e. tata kelola data, pelindungan data, dan transfer data secara keseluruhan kurang memadai; f. kerjasama kemitraan dan penyediaan jasa TI oleh Bank dilaksanakan secara kurang memadai; g. pemenuhan aspek pelindungan dan pelayanan konsumen yang meliputi *customer engagements, customer experience, customer insight, customer trust and perception* dan *customer with disability* kurang memadai.
5 (*Unsatisfactory*)	Kualitas penerapan 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; 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 teknologi yang bertanggungjawab tidak memadai dan penggunaan pihak penyedia jasa TI dalam penyelenggaraan TI tidak andal dan teruji; e. tata kelola data, pelindungan data, dan transfer data secara keseluruhan tidak memadai dan tidak sesuai ketentuan perundangan-undangan yang berlaku. f. Kerja sama kemitraan dan penyediaan jasa TI oleh Bank dilaksanakan secara tidak memadai; g. pemenuhan aspek pelindungan dan pelayanan konsumen yang meliputi *customer engagements, customer experience, customer insight, customer trust and perception,* dan *customer with disability* tidak memadai.

C. 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/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/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

KEPALA EKSEKUTIF PENGAWAS PERBANKAN

OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA,

DIAN EDIANA RAE

LAMPIRAN IV

RANCANGAN SURAT EDARAN OTORITAS JASA KEUANGAN

REPUBLIK INDONESIA

NOMOR /SEOJK.03/2023

TENTANG

PENILAIAN TINGKAT MATURITAS DIGITAL BANK UMUM

Hasil Penilaian Tingkat Maturitas Digital Bank

Nama Bank :
Tahun :

Penilaian Penerapan Domain

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

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

Lampiran
1. Kertas kerja penilaian maturitas digital Bank.

Ditetapkan di Jakarta
pada tanggal

KEPALA EKSEKUTIF PENGAWAS PERBANKAN
OTORITAS JASA KEUANGAN
REPUBLIK INDONESIA,

DIAN EDIANA RAE