



OTORITAS
JASA
KEUANGAN

CONSULTATIVE PAPER

Prinsip Ketahanan Operasional pada Bank

Departemen Penelitian dan Pengaturan Perbankan
Otoritas Jasa Keuangan

2022

1. Latar Belakang

- 1.1. Sejak krisis keuangan global, telah dilakukan reformasi pengaturan dan pengawasan dalam rangka mendorong stabilitas sistem keuangan, khususnya pengaturan pemodal dan likuiditas. Saat ini, kewajiban pemenuhan rasio pemodal dan likuiditas perbankan mengalami peningkatan dan terbukti telah mampu menjadi bantalan bagi bank untuk menyerap potensi kerugian finansial yang ada, khususnya pada saat pandemi. Namun, dewasa ini, bank semakin terpapar dengan berbagai risiko dan kerentanan operasional sehingga penguatan prudensial dibidang pemodal dan likuiditas saja belum cukup. Masih dibutuhkan standar untuk mengatasi dampak risiko operasional yang dapat menimbulkan kegagalan operasional ataupun disrupsi berskala besar terhadap pasar keuangan.
- 1.2. Dalam beberapa tahun terakhir, bank telah menghadapi tantangan signifikan dari berbagai peristiwa disruptif termasuk kegagalan yang diakibatkan teknologi, wabah pandemi, dan bencana alam. Kemajuan di bidang teknologi telah meningkatkan kemampuan bank untuk mengidentifikasi dan pulih dari berbagai jenis disrupsi tetapi ancaman operasional yang semakin canggih dan pertumbuhan ketergantungan terhadap pihak ketiga terus memaparkan bank terhadap sejumlah risiko operasional. Agar Bank dapat mengatasi berbagai paparan atas risiko operasional tersebut, Bank perlu memperkuat ketahanan operasionalnya.
- 1.3. Ketahanan operasional yang fleksibel dapat meningkatkan kemampuan bank untuk mempersiapkan, menyesuaikan, menghadapi dan pulih dari disrupsi, dan untuk melanjutkan operasional. Melalui ketahanan operasional, bank diwajibkan memiliki kemampuan untuk tetap melangsungkan bisnisnya seiring dengan munculnya gangguan yang tak terduga. Kemampuan tersebut penting dimiliki oleh bank seiring dengan perubahan pasar dan teknologi saat ini, diantaranya semakin tingginya konektivitas bank dengan pihak ketiga, semakin canggihnya serangan pada ketahanan operasional dan potensinya mendisrupsi pasar serta ketergantungan terhadap penyedia tertentu yang berujung pada risiko konsentrasi. Sehubungan dengan hal tersebut, ketahanan operasional perbankan saat ini telah menjadi prioritas baik bagi regulator maupun industri dan posisinya sama penting dengan ketahanan finansial perbankan.
- 1.4. Pandemi Covid-19 menjadi ujian besar bagi ketahanan operasional perbankan Indonesia. Bank harus lebih cekatan dalam menerapkan langkah-langkah kebijakan agar operasional bisnis dapat berjalan dengan lancar di tengah pembatasan sosial yang diterapkan pemerintah, salah satunya dengan menggunakan kanal digital bagi perbankan. Dalam prinsip ketahanan operasional, solusi ini seharusnya berada dalam Rencana Kelanjutan Bisnis atau *business continuity plan* dan manajemen risiko operasional agar bank dapat tetap mempertahankan Layanan Bisnis Kritisnya. Di sisi lain, dalam penggunaan kanal digital, perlu dipastikan agar operasi bisnis masih dapat berjalan dengan lancar, khususnya di tengah semakin cepatnya adopsi teknologi dalam layanan bisnis perbankan, ketergantungan terhadap pihak penyedia jasa tertentu dan kewaspadaan terhadap serangan pada ketahanan operasional yang semakin canggih.
- 1.5. Seiring dengan pentingnya ketahanan operasional bagi perbankan, BCBS (Basel Committee on Banking Supervision) telah mengeluarkan Prinsip Ketahanan Operasional pada maret 2021 yang diharapkan menjadi acuan bagi regulator di berbagai negara untuk meningkatkan ketahanan operasional perbankan.
- 1.6. BCBS mendefinisikan ketahanan operasional sebagai kemampuan bank untuk melangsungkan operasional yang kritis apabila terdapat gangguan. Sebuah perusahaan dianggap memiliki ketahanan operasional apabila tetap dapat mempertahankan

operasionalisasi utamanya serta melindungi konsumen, dan integritas sistem keuangan di tengah disrupsi yang tak terencana. Regulator, pengawas dan industri perbankan perlu bekerja sama dalam memelihara ketahanan operasional perbankan. Regulator menerbitkan sejumlah prinsip dan pengaturan yang menjadi panduan bagi pembentukan ketahanan operasional, industri perbankan melaksanakan panduan dan membentuk ketahanan operasional dengan baik, dan pengawas memastikan industri telah memiliki ketahanan operasional yang mumpuni.

- 1.7. Sehubungan dengan semakin berkembangnya layanan perbankan, penggunaan teknologi, dan kegagalan operasional karena manusia dan proses serta dampak pandemi yang menimbulkan cara kerja baru secara virtual sehingga mempengaruhi pengelolaan operasional kritikal perbankan, dibutuhkan suatu pedoman (*guidance*) baru yang dapat mendukung ketahanan operasional perbankan. Untuk itu, *Consultative Paper* ini berisikan prinsip-prinsip ketahanan operasional yang perlu diadopsi perbankan Indonesia dengan didasarkan pada perkembangan prinsip ketahanan operasional di BCBS dan beberapa negara.

2. Tujuan, Ruang Lingkup dan Batas Waktu Tanggapan

- 2.1. Implementasi prinsip ketahanan operasional diharapkan dapat mewujudkan bank yang:
 - a. mampu menanggapi disrupsi dengan cepat dan efektif sehingga dapat mengurangi dampak negatif yang muncul dari disrupsi tersebut,
 - b. menjaga kualitas pelayanan jika terdapat disrupsi,
 - c. memiliki disrupsi operasional yang lebih sedikit.
- 2.2. Prinsip ketahanan operasional diharapkan dapat diimplementasikan bagi seluruh bank umum konvensional dan bank umum syariah (Bank). Sehubungan dengan hal tersebut, kami mengeluarkan *Consultative Paper* ini yang berisikan prinsip-prinsip ketahanan operasional perbankan untuk mendapat masukan dari seluruh pemangku kepentingan.
- 2.3. Kami meminta tanggapan atas *Consultative Paper* bagi prinsip ketahanan operasional dapat disampaikan kepada Departemen Penelitian dan Pengaturan Perbankan paling lambat 30 November 2022.

3. Definisi

Ketahanan Operasional

- 3.1. Ketahanan operasional didefinisikan sebagai kemampuan Bank untuk tetap menjalankan Layanan Bisnis Kritikal meskipun terjadi disrupsi yang dapat mengganggu keberlangsungan Layanan Bisnis Kritikal tersebut. Ketahanan operasional memungkinkan bank untuk mengidentifikasi disrupsi sehingga bank dapat beradaptasi, menanggapi, pulih dan belajar dari disrupsi operasional. Bank diharapkan dapat mengatasi berbagai jenis disrupsi baik skala kecil hingga skala besar dengan memperhatikan karakteristik dan kompleksitas bank serta tingkat risiko yang akan diambil (*risk appetite*) dan Toleransi atas disrupsi yang terjadi.
- 3.2. Toleransi atas disrupsi yang terjadi didefinisikan sebagai batas dampak yang muncul atas suatu disrupsi yang terjadi yang dapat ditanggung oleh bank guna mempertahankan operasionalisasi Layanan Bisnis Kritikal.¹

¹ Toleransi atas disrupsi harus ditetapkan dengan ukuran yang jelas, umumnya menggunakan patokan waktu. Metrik lain pun dapat ditambahkan selama relevan seperti volume atau nilai transaksi. Toleransi atas disrupsi harus mempertimbangkan kapabilitas operasional bank dan berbagai scenario terburuk yang dapat mempengaruhi Layanan Bisnis Kritikal. Penetapan Toleransi atas disrupsi memungkinkan bank untuk mengukur dan memantau ketahanan operasional. Agar ketahanan operasional tetap terjaga, Layanan Bisnis Kritikal harus selalu berada di bawah Batasan Toleransi Dampak.

Layanan Bisnis Kritisal

- 3.3. Layanan bisnis adalah suatu kegiatan operasional perbankan yang disediakan untuk melayani nasabah ataupun calon nasabah. Dalam menentukan layanan bisnis yang dikategorikan kritisal, bank dapat mempertimbangkan dampak layanan bisnis tersebut terhadap: (a) Stabilitas keuangan, (b) Keberlangsungan bisnis bank, (c) Keberlangsungan pemangku kepentingan bank (termasuk konsumen).
- 3.4. Disrupsi terhadap Layanan Bisnis Kritisal berpotensi mempengaruhi stabilitas keuangan, khususnya layanan yang disediakan bank dan terkait dengan fungsi ekonomi tertentu seperti penghimpunan dana, penyaluran dana, investasi dan *treasury, wholesale funding market* dan pembayaran, kliring, penitipan dan *settlement*. Apabila tidak segera diperbaiki, dapat berdampak bagi pihak lawan yang menyediakan infrastruktur pasar keuangan dan infrastruktur nasional yang kritisal. Untuk itu, bank perlu mengidentifikasi beberapa kriteria untuk memastikan kritisalitas layanan bisnis, antara lain: potensi menghambat fungsi sistem keuangan Indonesia, potensi untuk mempengaruhi Tingkat Kesehatan Bank, stabilitas dan ketahanan sistem keuangan, kepentingan layanan tersebut terhadap sistem keuangan yang dapat dilihat melalui pangsa pasar, persentase klien yang dilayani dan klien sensitif seperti pemerintahan atau dana pensiun.
- 3.5. Disrupsi pada Layanan Bisnis Kritisal dapat mempengaruhi keberlangsungan bisnis bank yang ditandai dengan penurunan rentabilitas bank, pemburukan risiko reputasi, risiko hukum dan kepatuhan. Kritisalitas layanan bisnis dari sisi keberlangsungan usaha dapat dilihat apabila gangguan atas layanan bisnis: (a) berpotensi mempengaruhi posisi keuangan bank dan mengancam keberlangsungan bank, (b) berpotensi menyebabkan kerusakan reputasi, (c) berpotensi menyebabkan pelanggaran hukum atau kepatuhan terhadap pengaturan.
- 3.6. Layanan Bisnis Kritisal yang terganggu akan mempengaruhi keberlangsungan pemangku kepentingan yang bergantung pada operasionalisasi layanan tersebut. Kritisalitas layanan bisnis dari sisi keberlangsungan pemangku kepentingan bank (termasuk konsumen) dapat dilihat: (a) karakteristik dasar dari nasabah dan pihak ketiga, termasuk kerentanan yang dapat membuat klien tersebut lebih rentan terhadap bahaya akibat disrupsi, (b) kemampuan klien untuk memperoleh layanan dari penyedia jasa lain (ketergantian, ketersediaan dan aksesibilitas), (c) kritisalitas waktu bagi klien untuk menerima jasa tersebut, (d) jumlah klien yang dilayani, (e) potensi menyebabkan efek lanjutan bagi peserta pasar lain, khususnya jika bank menyediakan jasa yang bersifat sebagai infrastruktur pasar.
- 3.7. Suatu layanan bisnis dapat tersusun dari sejumlah rangkaian kegiatan operasional bank. Untuk itu, setiap rangkaian kegiatan operasional yang berkaitan dengan Layanan Bisnis Kritisal harus dipastikan tahan terhadap disrupsi. Layanan Bisnis Kritisal setiap bank berbeda-beda bergantung pada kriteria di atas. Jumlah Layanan Bisnis Kritisal akan bervariasi tetapi harus proporsional dengan ukuran dan kompleksitas bank. Hasil identifikasi terhadap Layanan Bisnis Kritisal harus ditinjau ulang minimal satu tahun sekali atau pada saat terjadi perubahan signifikan pada kegiatan operasional bank.

Fungsi Terkait

- 3.8. Istilah fungsi terkait yang digunakan di dokumen secara eksplisit mengacu pada fungsi yang sesuai pada tiga lini pertahanan bank, yang meliputi (i) manajemen unit bisnis; (ii) fungsi manajemen risiko operasional; dan (iii) pengendalian internal.

4. Prinsip Ketahanan Operasional

- 4.1. Ketahanan operasional yang efektif diperlukan untuk mempertahankan operasional, menanggapi dan memulihkan bank dari disrupsi terutama pada Layanan Bisnis Kritis.
- 4.2. Agar bank dapat memelihara keberlangsungan Layanan Bisnis Kritis, bank harus menerapkan prinsip-prinsip ketahanan operasional yang terdiri dari (a) Tata Kelola, (b) Manajemen Risiko Operasional, (c) Rencana dan Pengujian Kelanjutan Bisnis (*Business Continuity Planning and Testing*), (d) Pemetaan keterkaitan (*interconnections*) dan ketergantungan (*interdependencies*), (e) Manajemen Ketergantungan Pihak Ketiga, (f) Manajemen Insiden, (g) Analisis dan Pengujian Skenario, (h) Penilaian mandiri, Pengawasan dan Pelaporan

(a) Tata Kelola

- 4.3. Bank wajib memiliki struktur tata kelola untuk menyusun, mengawasi dan mengimplementasikan pendekatan ketahanan operasional yang efektif sehingga Bank mampu menanggapi dan beradaptasi dan juga pulih dari kejadian disruptif untuk memperkecil pengaruhnya dalam menjalankan operasi kritis selama disrupsi.
- 4.4. Tata kelola yang efektif perlu melibatkan berbagai pihak dari dewan komisaris, direksi, pejabat eksekutif dan pelaksana teknis. bertanggung jawab atas keberlangsungan strategi ketahanan operasional dalam bank. Dewan komisaris berfungsi untuk melakukan evaluasi secara berkala terhadap pelaksanaan strategi ketahanan operasional. Direksi berfungsi untuk menetapkan, memantau dan memastikan prinsip-prinsip ketahanan operasional telah diterapkan secara efektif. Direksi bertanggung jawab atas keberlangsungan strategi ketahanan operasional. Pejabat eksekutif dan pelaksana teknis berfungsi sebagai pelaksana implementasi strategi ketahanan operasional. Penerapan ketahanan operasional dapat memanfaatkan beberapa satuan kerja eksisting yang memiliki fungsi serupa, antara lain: fungsi kaji ulang dapat dilakukan oleh Satuan Kerja Audit Internal.
- 4.5. Direksi menyetujui, memantau dan meninjau ulang secara periodik penerapan prinsip ketahanan operasional dengan mempertimbangkan *risk appetite* dan Toleransi atas disrupsi dari Layanan Bisnis Kritis. Direksi harus memastikan bahwa bank memiliki kebijakan yang mengatasi kondisi pada saat kapabilitas operasional bank tidak mampu mempertahankan Toleransi atas disrupsi.²
- 4.6. Dalam menerapkan prinsip ketahanan operasional Direksi harus memastikan kecukupan sumber daya yang dimiliki antara lain: sumber daya manusia, keuangan, teknologi informasi pendukung, dan memastikan implementasi budaya ketahanan operasional yang efektif.
- 4.7. Direksi memberikan laporan secara tepat waktu mengenai ketahanan operasional setiap bisnis unit untuk mendukung pengawasan Dewan Komisaris, khususnya apabila ada kejadian defisiensi yang dapat mempengaruhi keberlangsungan Layanan Bisnis Kritis.
- 4.8. Direksi secara aktif mengkomunikasikan kebijakan terkait dengan ketahanan operasional kepada seluruh pihak seperti karyawan, pihak ketiga dan entitas dalam grup .

(b) Manajemen Risiko Operasional

- 4.9. Bank memanfaatkan Satuan Kerja Manajemen Risiko untuk:
 - (i) mengidentifikasi Layanan Bisnis Kritis yang dimiliki oleh Bank, kaji ulang atas hasil identifikasi perlu dilaksanakan secara berkala minimal tiga tahun sekali.,

² Penerapan prinsip ketahanan operasional termasuk identifikasi Layanan Bisnis Kritis dan penetapan Toleransi atas disrupsi.

- (ii) mengidentifikasi secara berkelanjutan ancaman internal, eksternal dan potensi kegagalan terhadap orang, proses dan sistem yang berperan dalam keberlangsungan Layanan Bisnis Kritisal.
 - (iii) menilai dengan segera kerentanan dari Layanan Bisnis Kritisal sesuai dengan hasil identifikasi ancaman dan risiko yang telah dilaksanakan dengan memperhitungkan Toleransi atas disrupsi dan
 - (iv) mengelola risiko agar sesuai dengan prinsip ketahanan operasional, yaitu dengan memitigasi paparan risiko operasional sesuai dengan Toleransi atas disrupsi.
- 4.10. Fungsi manajemen risiko operasional bekerja sama dengan fungsi lain yang relevan untuk mengelola dan mengatasi risiko yang mengancam keberlangsungan Layanan Bisnis Kritisal. Bank harus mengkoordinasikan Rencana Kelanjutan Bisnis, Manajemen Pihak Ketiga, Rencana Resolusi dan Pemulihan dan kerangka manajemen risiko lainnya untuk memperkuat ketahanan operasional bank.
- 4.11. Bank harus memiliki prosedur dan pengendalian yang cukup untuk mengidentifikasi dan menilai ancaman dan kerentanan secara tepat waktu dan sebisa mungkin mencegah ancaman dan kerentanan tersebut mempengaruhi keberlangsungan Layanan Bisnis Kritisal. Fungsi Terkait harus menilai dan menguji efektivitas dari implementasi prosedur dan pengendalian tersebut secara reguler, terutama apabila ada perubahan pada komponennya dan setelah mengalami ancaman/insiden untuk memasukkan pembelajaran atas insiden tersebut.
- 4.12. Bank harus meningkatkan kapabilitas manajemen perubahan yang sejalan dengan proses manajemen perubahan di bawah manajemen risiko operasional secara keseluruhan sebagai cara untuk dapat menilai efek potensial perubahan pada keberlangsungan Layanan Bisnis Kritisal dan pada keterkaitan dan ketergantungan.

(c) Rencana dan Pengujian Kelanjutan Bisnis (*Business Continuity Planning and Testing*)

- 4.13. Bank harus memiliki Rencana Kelanjutan Bisnis dan menyelenggarakan Latihan Kelanjutan Bisnis (*business continuity exercises*) di bawah skenario terburuk yang mungkin terjadi untuk menguji kemampuan penyelenggaraan Layanan Bisnis Kritisal selama disrupsi terjadi.
- 4.14. Suatu Rencana Kelanjutan Bisnis yang efektif harus:
- *Forward-looking* dalam menilai dampak dari disrupsi potensial
 - mengidentifikasi Layanan Bisnis Kritisal dan ketergantungan utama terhadap faktor internal dan eksternal untuk menilai risiko dan dampak potensial dari berbagai skenario disrupsi atas Layanan Bisnis Kritisal. Kaji ulang atas hasil identifikasi perlu dilaksanakan secara berkala minimal tiga tahun sekali.
 - terdiri dari (a) *Business Impact Analysis* (BIA), (b) strategi pemulihan, (c) program pengujian, (d) program pelatihan dan kesadaran (e) program komunikasi dan manajemen krisis.
 - mengembangkan, mengimplementasikan dan memelihara Latihan Kelanjutan Bisnis reguler yang memuat Layanan Bisnis Kritisal dan ketergantungan serta keterkaitannya, termasuk hubungannya dengan, tapi tak terbatas pada pihak ketiga dan entitas intragrup. Di antara tujuan dari kelanjutan bisnis, Latihan kelanjutan Bisnis harus mendukung kesadaran ketahanan operasional staf termasuk pelatihannya sehingga staf dapat dengan efektif beradaptasi dan menanggapi insiden.
 - memuat panduan rinci untuk mengimplementasi kerangka kerja pemulihan bencana yang berisi peran dan tanggung jawab pengelolaan disrupsi dan panduan delegasi wewenang ketika disrupsi mempengaruhi personil.

- secara jelas memuat proses pengambilan keputusan internal
 - mendefinisikan pemicu yang dapat menjadi tanda dijalankannya *Business Continuity Plan* (BCP) operasional
- 4.15. Pengujian Rencana Kelanjutan Bisnis diselenggarakan melalui Latihan Kelanjutan Bisnis. Latihan Kelanjutan Bisnis diselenggarakan dan divalidasi untuk serangkaian skenario terburuk yang mungkin dapat terjadi yang menggabungkan peristiwa dan insiden disruptif.
 - 4.16. Bank menguji Rencana Kelanjutan Bisnis, meninjau ulang pelaksanaan pengujian, dan mengembangkan rencana dengan menambahkan pembelajaran dari peristiwa yang telah terjadi. Pengujian dan pelaksanaan kelanjutan bisnis melibatkan pihak ketiga yang terasosiasi dengan Layanan Bisnis Kritis.
 - 4.17. Rencana Kelanjutan Bisnis untuk keberlangsungan Layanan Bisnis Kritis, termasuk yang menggunakan atau melibatkan pihak ketiga, yang terdapat dalam Rencana Resolusi dan Pemulihan harus konsisten dengan pendekatan ketahanan operasional.
 - 4.18. Bank secara berkala meninjau ulang Rencana Kelanjutan Bisnis untuk memastikan strategi kontinjensi tetap konsisten dengan operasional saat ini, risiko dan ancaman, toleransi disrupsi dan prioritas pemulihan. Latihan Kelanjutan Bisnis dilaksanakan oleh bank secara berkala, minimal setahun sekali.
 - 4.19. Bank mengidentifikasi dan mengelola ketersediaan personel yang esensial terhadap eksekusi operasional kritis dan lini bisnis inti. Bank memiliki lokasi alternatif yang memiliki sumber daya yang cukup (termasuk personil), kapabilitas teknologi, dan fungsionalitas untuk mengeksekusi operasional kritis dan lini bisnis inti pada saat disrupsi. Lokasi alternatif harus terletak pada jarak geografis yang memadai dari lokasi utama dan memiliki profil risiko yang berbeda.
 - 4.20. Bank mencantumkan Rencana dan Pengujian Kelanjutan Bisnis ke dalam Rencana Bisnis Bank. Rencana dan Pengujian Kelanjutan Bisnis akan menjadi informasi tambahan yang berkaitan dengan aktivitas bisnis bank dan dapat memberikan gambaran atas kualitas penerapan manajemen risiko bank dalam menjalankan bisnisnya.

(d) Pemetaan Keterkaitan dan Ketergantungan

- 4.21. Setelah Bank mendefinisikan Layanan Bisnis Kritis, Bank harus memetakan interkoneksi dan interdependensi internal dan eksternal yang dibutuhkan untuk menjalankan Layanan Bisnis Kritis konsisten dengan kebijakan ketahanan operasionalnya. Pemetaan atas sumber daya dibutuhkan agar Bank mampu mengidentifikasi kerapuhan pada Layanan Bisnis Kritis sehingga Bank dapat melaksanakan tindakan tertentu sesuai dengan kebijakan dan strategi ketahanan operasional.
- 4.22. Fungsi terkait wajib memetakan (dengan mengidentifikasi dan mendokumentasikan) sumber daya manusia, teknologi, proses, informasi, fasilitas, dan interkoneksi dan interdependensi dari hal tersebut yang dibutuhkan untuk menjalankan Layanan Bisnis Kritis, termasuk yang bergantung pada, tapi tidak terbatas pada, pihak ketiga atau perjanjian antargrup. Kaji ulang atas hasil identifikasi perlu dilaksanakan secara berkala minimal tiga tahun sekali.
- 4.23. Sumber Daya Manusia (SDM) yang dimaksud adalah SDM yang mendukung penyediaan Layanan Bisnis Kritis. Bank perlu memahami SDM yang bertanggungjawab atas proses, teknologi dan mengimplementasikan serta memantau pengendalian. Juga pemahaman menyeluruh atas akuntabilitas pejabat eksekutif. Hal ini termasuk individu yang bertanggungjawab untuk kapabilitas tertentu, ukuran dan kekuatan tim, Latihan/pembelajaran dan tantangan organisasi seperti pengendalian SDM, pengurangan karyawan, praktik perekrutan dan perencanaan suksesi personil.

- 4.24. Teknologi adalah sistem dan arsitektur yang mendasari untuk mendukung penyediaan layanan bisnis.
- 4.25. Proses adalah sebuah kumpulan aktivitas terstruktur yang dirancang untuk menghasilkan keluaran tertentu. Kemampuan untuk mendefinisikan proses apa yang bertanggungjawab untuk mengeluarkan hasil tertentu dalam organisasi adalah elemen kunci dari pendekatan organisasi pada teknologi.
- 4.26. Informasi adalah data atau material apapun yang dibutuhkan oleh bank untuk melaksanakan jasanya yang mendukung keberlangsungan Layanan Bisnis Kritisal.
- 4.27. Fasilitas adalah alat dan infrastruktur yang digunakan untuk mendukung layanan bisnis kritisal, antara lain: lokasi kantor, fasilitas pencetakan, persuratan, produksi kartu kredit, pernyataan dan komunikasi dengan klien.
- 4.28. Bank harus mempertimbangkan apakah kebijakan ketahanan operasional-nya secara memadai terharmonisasi dengan pemetaan organisasi dari Layanan Bisnis Kritisal dan jasa pihak ketiga kritisal dalam Rencana Resolusi dan Pemulihannya.
- 4.29. Pendekatan dan granularitas pemetaan harus cukup bagi bank untuk mengidentifikasi kerentanan dan mendukung pengujian terhadap kemampuan bank untuk melangsungkan Layanan Bisnis Kritisal, dengan mempertimbangkan *risk appetite* (RA) dan Toleransi atas disrupsi.

(e) Manajemen Ketergantungan Pihak Ketiga

- 4.30. Bank harus mengelola ketergantungan hubungannya terhadap pihak ketiga atau entitas lain dalam satu kelompok usaha untuk keberlangsungan Layanan Bisnis Kritisal. Pengelolaan dilakukan dengan Identifikasi, analisis dan penetapan prioritas pihak ketiga yang terkait dengan Layanan Bisnis Kritisal sesuai dengan signifikansinya.
- 4.31. Bank harus melaksanakan penilaian risiko dan uji kelayakan sebelum bekerja sama dengan pihak ketiga sesuai dengan (i) Kebijakan manajemen risiko operasional; (ii) Kebijakan manajemen alih daya, (iii) Kebijakan terkait Teknologi Informasi (MRTI dan PTI) dan (iv) Kebijakan Ketahanan operasional. Bank harus memiliki perjanjian hubungan kerja sama dengan pihak ketiga yang mencantumkan kewajiban dan hak kedua pihak yang sesuai dengan prinsip ketahanan operasional. Sebelum bekerja sama, bank harus memastikan pihak ketiga memiliki kondisi ketahanan operasional yang setara untuk menjaga Layanan Bisnis Kritisal baik pada kondisi normal maupun kondisi disrupsi. Bank harus meminta pihak ketiga yang mempengaruhi penyediaan Layanan Bisnis Kritisal untuk menyusun dan memiliki perencanaan kontinjensi untuk memelihara ketahanan operasional. Bank harus memastikan bahwa pihak ketiga memiliki rencana kontinjensi terkait operasional bisnis sebelum sepakat untuk kerjasama dengan pihak yang bersangkutan. Selama kerja sama Bank wajib memantau dan meninjau praktik ketahanan operasional pihak ketiga.
- 4.32. Bank harus mengembangkan prosedur perencanaan Kontinjensi dan Kelanjutan Bisnis yang memadai, serta strategi keluar (*exit strategy*) untuk memelihara ketahanan operasional pada saat terjadi kegagalan atau disrupsi pada pihak ketiga yang mempengaruhi penyediaan Layanan Bisnis Kritisal. Skenario di bawah Rencana Kelanjutan Bisnis harus menilai ketergantungan dari pihak ketiga yang menyediakan jasa terhadap Layanan Bisnis Kritisal, dan alternatif yang layak yang dapat memfasilitasi ketahanan operasional disaat pihak ketiga tidak dapat beroperasi, seperti melaksanakan sendiri layanan tersebut.
- 4.33. Bank mengidentifikasi risiko dari konsentrasi layanan bisnis yang melibatkan pihak ketiga atau vendor dan menghubungkan data yang sifatnya rahasia dalam rangka memitigasi risiko kegagalan/gangguan yang terkait dengan jaringan maupun ketersediaan layanan pihak ketiga.

- 4.34. Bank mengidentifikasi risiko dari pihak ketiga yang menyediakan infrastruktur publik dan kritikal seperti energi dan telekomunikasi. Bank memiliki proses untuk mengelola disrupsi dari layanan dimaksud dan memperbaiki proses tersebut selayak mungkin untuk tetap berada pada toleransi disrupsi.

(f) Manajemen Insiden

- 4.35. Untuk menanggapi disrupsi/insiden yang dapat mengganggu kelangsungan Layanan Bisnis Kritikal Bank, Bank wajib memiliki Manajemen Insiden.
- 4.36. Manajemen insiden adalah proses identifikasi, analisis, perbaikan dan belajar dari insiden, dan mencegah kejadian berulang atau memitigasi tingkat keparahan insiden. Tujuan dari manajemen insiden adalah untuk membatasi disrupsi dan mengembalikan Layanan Bisnis Kritikal, sejalan dengan Toleransi atas disrupsi.
- 4.37. Manajemen insiden wajib mencakup beberapa hal di bawah ini untuk menggambarkan siklus hidup dari insiden, antara lain:
- a. Klasifikasi dari dampak insiden berdasarkan kriteria yang telah ditetapkan sebelumnya (contoh: ekspektasi waktu untuk kembali kepada *business-as-usual*), sehingga Bank mampu menetapkan skala prioritas dan alokasi sumber daya yang memadai untuk menanggapi sebuah insiden.
 - b. Prosedur penanggulangan dan pemulihan insiden termasuk hubungannya dengan kelanjutan bisnis bank, pemulihan bencana dan prosedur dan rencana manajemen terasosiasi lainnya, dan
 - c. Implementasi dari rencana komunikasi untuk melaporkan insiden kepada pihak internal dan eksternal termasuk ukuran kinerja selama insiden dan analisis dari hasil pembelajaran setelah accident
- 4.38. Bank mengembangkan rencana penanggulangan dan pemulihan (*response* dan *recovery plan*) untuk mengelola insiden yang bisa mengganggu kelangsungan Layanan Bisnis Kritikal sejalan dengan *risk appetite* dan Toleransi atas disrupsi. Bank harus terus mengembangkan *response* dan *recovery plan* dengan menambahkan setiap pelajaran dari insiden sebelumnya.
- 4.39. Bank harus memiliki inventaris atas *incident response and recovery* (penanggulangan dan pemulihan insiden), sumber daya internal dan pihak ketiga untuk mendukung kapabilitas tanggapan dan pemulihan bank. Inventaris atas *incident response and recovery* dilakukan dengan menyiapkan pangkalan data atas insiden sebagai salah satu bagian dari proses belajar dari insiden.
- 4.40. Prosedur penanggulangan dan pemulihan insiden harus dikaji ulang, diuji, dan diperbarui. Bank harus mengidentifikasi dan menyampaikan akar penyebab dari insiden untuk mencegah atau meminimalisir terulangnya kejadian.
- 4.41. Program manajemen insiden perlu dikinikan dan mencerminkan pembelajaran dari insiden sebelumnya atau insiden bank lain. Program manajemen insiden juga perlu mengelola seluruh insiden yang mempengaruhi bank termasuk yang berkaitan dengan pihak ketiga dan entitas intragrup.

(g) Analisis dan Pengujian Skenario

- 4.42. Analisis dan Pengujian Skenario dalam ketahanan operasional digunakan untuk membantu institusi mengembangkan, memvalidasi dan mengalibrasi Toleransi atas disrupsi dari suatu Institusi.
- 4.43. Kerentanan ketahanan operasional yang teridentifikasi melalui Manajemen Risiko Operasional, Manajemen Kelanjutan Bisnis, Pemetaan dan Interkoneksi, Manajemen Pihak

Ketiga dan Manajemen Insiden digabungkan dalam membentuk suatu skenario *severe but plausible* yang mempengaruhi Layanan Bisnis Kritis. Bank merancang skenario sehingga dapat digunakan untuk menguji Toleransi atas disrupsi dari bank.

- 4.44. Bank mempertahankan kerangka tata kelola yang kokoh dan fungsi peninjauan ulang yang independen untuk mengawasi integritas dan konsistensi dari proses pengembangan skenario.
- 4.45. Bank menggunakan analisis skenario untuk pengujian balik (*back-testing*) atas disrupsi parah yang muncul di masa lalu dan untuk pengujian atas potensi disrupsi lain yang dapat ditemui di masa depan. Hasil dari pengujian balik digunakan untuk memurnikan skenario dan meningkatkan efektivitas skenario kedepannya. Skenario digunakan juga untuk memperbaiki berbagai upaya ketahanan operasional yang telah disusun untuk mengantisipasi disrupsi.
- 4.46. Analisis dan Pengujian Skenario harus dilakukan untuk seluruh Layanan Bisnis Kritis dan seluruh kemungkinan disrupsi yang fatal tetapi masuk akal sehingga dapat membahayakan keberlangsungan Layanan Bisnis Kritis. Analisis dan Pengujian Skenario juga harus dilakukan proporsional dengan ukuran, skala dan kompleksitas dari aktivitas bank.
- 4.47. Apabila setelah melakukan uji skenario, Bank menemukan kondisi dimana Bank tidak bisa mempertahankan Layanan Bisnis Kritis, Bank wajib melaporkan kondisi tersebut kepada OJK paling lambat tujuh hari kerja. Apabila ditemukan suatu kelemahan terhadap ketahanan operasional Bank setelah dilakukan Analisis dan Pengujian Skenario, Bank wajib menyusun rencana aksi dan melakukan tindakan yang diperlukan untuk memperbaiki kerapuhan tersebut serta melaporkan ke OJK paling lambat tujuh hari kerja.

(h) Penilaian mandiri, Pengawasan dan Pelaporan

- 4.48. Untuk memastikan bank telah melaksanakan seluruh kewajiban dalam prinsip ketahanan operasional, bank wajib melakukan penilaian mandiri, pengawasan dan pelaporan atas strategi ketahanan operasional yang telah diimplementasi.
- 4.49. Bank melakukan penilaian sejauh mana Bank telah mengatasi hambatan terhadap kelangsungan Layanan Bisnis Kritis dan mengidentifikasi analisis *gap* yang ada dengan mengacu antara lain: gap antara hasil pemetaan Layanan kritis dengan ketentuan internal dan eksternal. Penilaian mandiri tersebut wajib didokumentasikan dan dilakukan secara reguler.
- 4.50. Dokumentasi tersebut dapat berbentuk laporan tetapi tidak ada *template* laporan khusus yang ditentukan untuk diisi oleh bank untuk memberikan fleksibilitas terhadap setiap bank dalam penyusunannya sesuai dengan konsep proporsionalitas. Dokumentasi tersebut tidak wajib disampaikan kepada otoritas tetapi apabila diminta oleh pengawas sewaktu-waktu, bank harus dapat menyampaikannya, khususnya dalam rangka penilaian ketahanan operasional oleh pengawas.
- 4.51. Dokumentasi terhadap penilaian mandiri wajib memuat sedikitnya:
 - a. Layanan Bisnis Kritis dan pertimbangan penentuannya.
 - b. Toleransi atas disrupsi dan pertimbangan penentuannya.
 - c. Pemetaan keterkaitan antara sumber daya manusia, teknologi, proses, informasi, fasilitas, serta interkoneksi dan interdependensi dari hal tersebut terhadap Layanan Bisnis Kritis
 - d. Strategi agar Layanan Bisnis Kritis tetap berada pada Toleransi atas disrupsi.
 - e. Implementasi manajemen insiden
 - f. Metode dan asumsi yang digunakan dalam Uji Skenario
 - g. Hasil Uji Skenario Ketahanan Operasional dan tindak lanjut yang diambil.

- 4.52. Bank mengidentifikasi dan memantau eksposur berkelanjutan terhadap risiko operasional relatif terhadap selera risiko dan toleransi disrupsi. Bank mendirikan dan mempertahankan prosedur komunikasi dan koordinasi untuk menginformasikan seluruh area terkait tentang eksposur yang ada.
- 4.53. Bank mendeteksi secara tepat waktu aktivitas anomali yang dapat menyebabkan disrupsi yang mempengaruhi operasi kritikal dan lini bisnis inti dan hal tersebut menilai dampak potensial dari aktivitas bersamaan dengan efektivitas dari kebijakan perlindungan.
- 4.54. Bank melaporkan kepada otoritas apabila terdapat keadaan atau perkiraan keadaan yang dapat membahayakan kelangsungan usaha bank. Dewan Komisaris wajib melaporkan kepada Otoritas Jasa Keuangan segera setelah ditemukan keadaan atau perkiraan keadaan yang dapat membahayakan kelangsungan usaha bank.
- 4.55. Bank merinci dan mendokumentasikan secara detail terkait ketergantungan layanan operasional pada pihak entitas grup lain dan pihak ketiga dengan melakukan pemetaan aplikasi TI yang dinilai penting ke dalam Layanan Bisnis Kritikal sehingga dapat dilakukan pemeliharaan dan perawatan.
- 4.56. Bank menyelenggarakan pengawasan kontinu dan pelaporan kepada Pejabat Eksekutif dan Direksi yang menyediakan data yang cukup dan informasi untuk pengambilan keputusan yang tepat waktu dan cocok terkait dengan kebijakan untuk menanggapi suatu disrupsi.