H. Risiko Operasional

38. Perhitungan Risiko Operasional

a. Bank Secara Individu

dalam juta rupiah

No	Pendekatan yang digunakan	31 Desember 2023				31 Desember 2022		
		Komponen Indikator Bisnis (KIB)	Faktor Pengali Kerugian Intern (FPKI)	Modal Minimum Risiko Operasional (MMRO)	ATMR	Pendapatan bruto (rata-rata 3 tahun terakhir)	Beban Modal	ATMR
1	Pendekatan Indikator Dasar	-	-	-	-	49.599.197	7.439.879	92.998.494
2	Pendakatan Standar	4.450.593	0,62853430	2.797.350	34.966.876	-	-	-

b. Bank Secara Konsolidasi

dalam juta rupiah

No	Pendekatan yang digunakan	31 Desember 2023				31 Desember 2022		
		Komponen Indikator Bisnis (KIB)	Faktor Pengali Kerugian Intern (FPKI)	Modal Minimum Risiko Operasional (MMRO)	ATMR	Pendapatan bruto (rata-rata 3 tahun terakhir)	Beban Modal	ATMR
1	Pendekatan Indikator Dasar	-	-	-	-	51.500.813	7.725.122	96.564.025
2	Pendakatan Standar	4.515.914	0.63376978	2.862.050	35.775.625	-	-	-

39. Pengungkapan Kualitatif Umum

Pengelolaan Risiko Operasional

Risiko Operasional terjadi karena adanya ketidakcukupan atau tidak berfungsinya proses internal, kesalahan manusia, kegagalan sistem, atau adanya gangguan eksternal yang memengaruhi operasional Bank. Kejadian Risiko Operasional merupakan kejadian risiko yang melekat pada setiap proses bisnis dan operasional yang dijalankan Bank dan dapat memicu terjadinya Risiko Reputasi, Risiko Hukum, Risiko Kepatuhan, serta Risiko lainnya apabila tidak dikelola dengan baik.

Dengan meningkatnya keragaman dan kompleksitas produk serta aktivitas perbankan yang ditawarkan kepada nasabah, perkembangan sistem dan teknologi pendukung yang sangat cepat, serta meningkatnya ekspektasi nasabah akan pelayanan yang diberikan oleh Bank, maka pengelolaan risiko operasional menjadi hal yang sangat penting.

Dalam rangka menerapkan manajemen risiko operasional, BNI mengacu pada ketentuan Bank Indonesia atau Otoritas Jasa Keuangan, serta *International Best Practices*. Agar pengelolaan manajemen risiko operasional berjalan dengan baik, BNI memiliki Kerangka Kerja Manajemen Risiko Operasional yang terdiri dari 6 (enam) komponen utama, yaitu:

1. Strategi dan Tujuan Bisnis

   Strategi dan tujuan bisnis BNI sebagai acuan dalam penerapan manajemen risiko operasional.

2. Strategi Manajemen Risiko Operasional

   Strategi Manajemen Risiko Operasional dirumuskan sesuai strategi dan tujuan bisnis secara keseluruhan dengan memperhatikan tingkat Risiko yang akan diambil (*risk*

appetite) dan toleransi Risiko (*risk tolerance*). Tujuan penetapan strategi manajemen risiko operasional adalah untuk memastikan bahwa eksposur risiko operasional telah dikelola secara terkendali sesuai dengan kebijakan dan prosedur intern serta peraturan perundang-undangan dan ketentuan lain yang berlaku.

3. Model Manajemen Risiko Operasional

   a. Tata Kelola Manajemen Risiko Operasional

      Tata kelola manajemen risiko operasional diimplementasikan berdasarkan konsep *Three Lines Model* yang membedakan antara Satuan Kerja Operasional (*Risk Taking Unit*) yang merupakan *Risk and Control Owner*, Satuan Kerja Manajemen Risiko yang independen, dan Satuan Kerja Audit Intern. Fungsi *Risk Taking Unit* dijalankan oleh Satuan Kerja Operasional dan spesifik untuk konteks risiko operasional bermitra dengan *Senior Operational Risk Executive* (SORX) dalam memitigasi risiko yang dihadapi. Satuan Kerja Manajemen Risiko bersama dengan Satuan Kerja Kepatuhan bertugas memantau risiko dan menyediakan kebijakan/ prosedur terkait manajemen risiko untuk meminimalisir risiko, serta me-*review* produk bank baru. Satuan Kerja Audit Intern bertugas memastikan efektivitas pengelolaan risiko dan pengendalian intern.

   b. Proses Manajemen Risiko Operasional

      Proses manajemen risiko operasional meliputi identifikasi, pengukuran, pemantauan dan pengendalian terhadap risiko operasional, yang dijabarkan sebagai berikut:

      1) Identifikasi

         Identifikasi risiko dilakukan secara proaktif terhadap seluruh aktivitas, proses, dan produk dalam rangka menganalisis sumber, tingkat kemungkinan timbulnya risiko operasional serta dampak yang ditimbulkannya.
         Mekanisme identifikasi risiko operasional dilakukan dengan menerapkan *process mapping* atas proses kerja/ aktivitas masing-masing unit untuk menangkap potensi risiko operasional.

      2) Pengukuran

         Pengukuran risiko dilakukan dalam rangka mengetahui perkembangan dan besarnya eksposur risiko operasional sebagai acuan untuk melakukan pengendalian serta untuk keperluan perhitungan kewajiban penyediaan modal minimum. Dalam rangka perhitungan beban modal dan ATMR risiko operasional, saat ini Bank menggunakan metode *Standardized Approach* (SA) sesuai dengan Surat Edaran Otoritas Jasa Keuangan No. 6/SEOJK.03/2020 tanggal 29 April 2020 tentang Perhitungan Aset Tertimbang Menurut Risiko untuk Risiko Operasional dengan Menggunakan Pendekatan Standar Bagi Bank Umum.

      3) Pemantauan

         Pemantauan risiko dilakukan oleh seluruh unit sebagai *first line roles* terhadap risiko utama pada saat aktivitas sedang berlangsung. Sedangkan *second line* melakukan evaluasi dan laporan/ *feedback* atas penilaian risiko berdasarkan hasil *self assessment* serta realisasi atas kerugian risiko operasional yang terjadi, meliputi:
         - *Feedback report* untuk seluruh Divisi/ Satuan/ Wilayah/ Cabang
         - Laporan bulanan Pemantauan Kerugian Risiko Operasional kepada Direksi
         - Laporan Profil Risiko Operasional

      4) Pengendalian

         Pengendalian risiko dilakukan untuk mengurangi dan mengendalikan dampak dan frekuensi risiko operasional yang teridentifikasi selama tahap penilaian dan

pengukuran. Proses pengendalian risiko disesuaikan dengan eksposur risiko maupun tingkat dan toleransi risiko yang akan diambil.

c. Kebijakan dan Permodalan Risiko Operasional

Bank telah memiliki Pedoman Penerapan Manajemen Risiko Operasional untuk mendukung implementasi manajemen risiko operasional pada segenap unit baik di dalam maupun di luar negeri. Kebijakan tersebut dijabarkan lebih rinci dalam Prosedur atau *Standard Operating Procedure* serta Petunjuk Teknis transaksi dan operasional yang *prudent* untuk menjalankan aktivitas bisnis sehari-hari seperti:

1) Prosedur Manajemen Risiko Operasional
2) Petunjuk Teknis Manajemen Risiko Operasional
3) Petunjuk Teknis SORX

Bank melakukan perhitungan modal risiko operasional untuk memastikan BNI memiliki modal yang cukup dalam rangka menyerap risiko operasional yang dihadapi.

d. *Tools* dan *Method*

Dalam menerapkan manajemen risiko operasional juga perlu diperlengkapi dengan *tools* dan metodologi. *Tools* yang diterapkan dalam manajemen risiko operasional antara lain *Risk Control Self Assessment* (RCSA), *Loss Event Database* (LED), *Key Risk Indicator* (KRI) dan *Business Continuity Management* (BCM).

New Periskop	
Modul *Risk and Control Self Assessment* (RCSA)	*Risk and Control Self Assessment* (RCSA) merupakan suatu rangkaian kegiatan yang dilakukan secara independen oleh setiap unit (*risk owner*) dalam rangka mengidentifikasi potensi risiko operasional yang terdapat di unitnya, mencari penyebabnya, mengukur potensi kerugian (dampak dan frekuensi) yang mungkin timbul serta mencarikan solusi untuk mengatasinya. Selain itu, dilakukan penilaian kontrol untuk masing-masing risiko yang akan memengaruhi skor risiko yang melekat (*Inherent Risk*).
Modul *Loss Event Database* (LED)	Merupakan *database event* sejak *event* terjadi hingga penyelesaiannya akibat risiko operasional yang terjadi di seluruh unit di Bank. Data *event* yang terkumpul melalui modul LED, selain digunakan untuk pengelolaan risiko operasional yang lebih baik serta mencegah terjadinya kasus serupa juga sebagai dasar pada perhitungan ATMR risiko operasional dalam rangka menghitung kebutuhan modal untuk menutup risiko operasional dengan menggunakan metode *Standardized Approach* yang mulai diimplementasikan tahun 2023.
Modul *Key Risk Indicator* (KRI)	*Key Risk indicators* merupakan alat ukur untuk mengidentifikasi potensi kerugian risiko operasional yang melekat pada produk dan aktivitas secara dini dan memberikan tanda (*early warning signal*) jika melebihi suatu *threshold* tertentu yang telah ditetapkan sebelumnya untuk memonitor eksposur risiko operasional dan efektivitas kontrol Bank.
Modul *Business Continuity Management* (BCM)	Merupakan salah satu upaya untuk mendukung pengelolaan dokumentasi langkah penanganan dampak gangguan/ bencana dan proses pemulihan agar kegiatan operasional bank dan pelayanan nasabah dapat tetap berjalan pada kondisi bencana. Modul ini terdiri dari penyusunan *call tree*, pembentukan Oganisasi *Crisis Management Team* (CMT) / *Emergency Task Force* (ETF), penyusunan *Business Impact Analysis* (BIA), *Threat and Risk Assessment* (TRA) dan pemeliharaan sarana prasarana BCM serta pencatatan *monitoring* kejadian dan potensi bencana.

4. Teknologi Informasi dan Data

Penggunaan dan penerapan teknologi informasi dan data yang terintegrasi untuk risiko operasional mampu menghasilkan laporan yang lengkap dan akurat dalam rangka mendeteksi dan mengoreksi penyimpangan atas proses bisnis secara tepat waktu. Pemanfaatan data yang berkualitas menghasilkan analisis yang dapat digunakan dalam pengelolaan risiko operasional serta sebagai bahan pendukung dalam pengambilan keputusan oleh manajemen.

5. Sumber Daya Manusia (SDM) dan Budaya Risiko

Penerapan budaya risiko (*risk culture*) yang efektif di BNI dapat menciptakan mekanisme yang melibatkan seluruh pegawai untuk mengidentifikasi dan mencegah kelemahan dan penyimpangan secara dini dengan efisien dan efektif.

6. *Assurance*

Assurance adalah aktivitas penilaian independen oleh pihak ketiga atas implementasi kerangka kerja manajemen risiko operasional. Penilaian ini dilakukan oleh Satuan Audit Internal (IAD) maupun pihak eksternal bank.

Business Continuity Management

Merupakan rangkaian proses sistem manajemen terencana untuk menjamin kelangsungan usaha akibat adanya gangguan atau bencana baik oleh faktor alam, perbuatan manusia, maupun sistem yang dapat terjadi pada fungsi-fungsi usaha BNI yang kritikal sehingga menyebabkan terganggunya aktivitas bisnis dan layanan BNI.

Untuk mengantisipasi kejadian tersebut maka BNI telah menerapkan Manajemen Keberlangsungan Usaha/ *Business Continuity Management* (BCM) di segenap unit baik di dalam maupun di luar negeri, yang diharapkan dapat meminimalisir risiko operasional pada saat terjadinya kondisi darurat atau bencana.

Penerapan kebijakan tersebut sejalan dengan peraturan Regulator yang mewajibkan Bank untuk melaksanakan proses pengendalian risiko yang dapat membahayakan kelangsungan usaha Bank, serta selaras dengan persyaratan pada dokumen Basel II yang mewajibkan Bank untuk memiliki pengelolaan keberlangsungan usaha dan rencana darurat (*Business Continuity Management* dan *Contingency Plan*) guna memastikan kemampuan Bank agar tetap dapat beroperasi dan meminimalisir kerugian jika terjadi gangguan terhadap aktivitas bisnisnya. Selain peraturan Regulator dan Basel II, untuk Kantor Luar Negeri, BCM diimplementasikan sesuai dengan regulasi BCM di negara setempat.

Tata Kelola dan Organisasi

Dalam kondisi bencana (*disaster*), BNI telah menyiapkan organisasi spesifik berupa *Crisis Management Team* (CMT) dan *Emergency Task Force* (ETF) yang dipimpin oleh *Executive Management Team* (EMT)/ Pimpinan Tertinggi Unit sebagai koordinator yang memiliki level kewenangan tertinggi. CMT/ETF akan aktif apabila *Executive Management Team* (EMT) selaku pimpinan tertinggi dari CMT/ETF menyatakan deklarasi kondisi status darurat/bencana.

BNI telah memiliki infrastruktur yang dibutuhkan dalam implementasi BCM seperti *Disaster Recovery Center* (DRC), *Data Center* (DC), lokasi alternatif Gedung BCM dan BCM *Center* yang secara rutin dikelola kesiapannya.

Prosedur dan Petunjuk Teknis

Terkait dengan implementasi *Business Continuity Management* (BCM), BNI telah menetapkan:

1. Kebijakan *Business Continuity Management* (BCM) Dalam Negeri
2. Prosedur *Business Continuity Management* (BCM) Dalam Negeri
3. *Business Continuity Management* (BCM) *Policy for Overseas Branches*
4. *Business Continuity Management* (BCM) *Procedure for Overseas Branches*
5. Kebijakan *Crisis Management Protocol* (CMP)
6. Prosedur Tata Kelola Gedung *Business Continuity Management* (BCM)

Proses

Setiap langkah *Recovery Strategy* dan *Restoration Strategy* yang dilaksanakan dipantau dan dilaporkan kepada *Crisis Management Team* (CMT) sampai kondisi dinyatakan normal kembali. Untuk memastikan tingkat kesiapan dan evaluasi *Business Continuity Management* (BCM), BNI melakukan pengujian sistem pada divisi/ unit kritikal setiap 3 (tiga) bulan sekali, melakukan *site visit*, sosialisasi dan simulasi penanganan bencana terkait implementasi BCM di seluruh unit operasional yang dilakukan secara rutin tiap tahun untuk mengetahui tingkat kesiapan masing-masing unit, ditinjau dari segi organisasi maupun infrastruktur BCM yang dimilikinya.

Hasil evaluasi dan pengujian rutin tersebut terlihat dari penanganan yang sistematis dan terarah dalam menghadapi bencana baik yang disebabkan oleh manusia, alam, maupun oleh sistem sehingga aktivitas operasional BNI di lokasi bencana dapat tetap berjalan pada tingkatan tertentu walaupun beberapa sarana dan prasarana penunjang aktivitas bisnis mengalami gangguan.

Proses penerapan BCM dilakukan sebagai berikut:

1. Pembentukan struktur organisasi BCM di segenap unit kerja BNI
2. Menilai potensi risiko dan ancaman untuk mendapatkan gambaran atas kejadian bencana yang memiliki kemungkinan terjadinya (*likelihood*) paling tinggi dan dampak (*impact*) paling besar, serta memperkirakan tindakan maupun fasilitas yang harus dipersiapkan
3. Mengidentifikasi proses bisnis yang kritikal (*Business Impact Analysis*–BIA) bagi kelangsungan bisnis BNI bilamana terjadi kondisi darurat/bencana. BIA merupakan acuan bagi unit dalam menyusun prioritas dan strategi pemulihan (*recovery*) serta kerangka waktu pemulihan untuk aktivitas bisnis utamanya
4. Membuat rencana penanganan kondisi darurat sebagai acuan bagi unit dalam pencegahan dan penanganan kondisi darurat serta sebagai dasar implementasi standar keamanan dan keselamatan gedung
5. Membuat Strategi Pemulihan (*Recovery Strategy*) dengan tujuan mempersiapkan cara yang terorganisir untuk membuat keputusan jika terjadi kondisi darurat yang mengganggu aktivitas bisnis Bank
6. Membuat Strategi Pengembalian (*Resumption Strategy*) dengan tujuan menyediakan cara mengembalikan fungsi dan aktivitas ke tingkat layanan sebelum terjadi bencana

Manajemen Risiko Digital

Seiring dengan perkembangan inovasi bisnis perbankan yang mengutamakan *platform-based* dan *fully* digital melalui pengembangan *advanced digital capabilty* dengan bisnis model berbasis data, Bank melakukan penguatan manajemen risiko khususnya terkait dengan risiko digital serta meningkatkan ketahanan siber (*cyber resilience*) melalui penguatan keamanan siber (*cyber security*). Standar penerapan manajemen risiko digital dan keamanan siber juga dilengkapi pengujian ketahanan dan keamanan siber, serta didukung pelaporan efektif terhadap penerapan manajemen risiko digital dan keamanan siber sehingga tercipta layanan yang efektif, efisien dan aman.

Tata Kelola dan Kebijakan

Strategi manajemen risiko digital dan keamanan siber diimplementasikan dalam koridor tata kelola yang efektif dan menyeluruh, sehingga menciptakan pengelolaan manajemen risiko yang bersifat proaktif dan *forward looking*. Penerapan tata kelola menajemen risiko di BNI dilakukan melalui Kebijakan Umum Manajemen Risiko (KUMR), *framework*, dan prosedur yang diterapkan secara konsisten dan berkesinambungan sesuai ketentuan regulasi. Penerapan tata kelola manajemen risiko yang berbasis *People*, *Process*, dan *Technology*, menjadi pondasi utama penyelenggaraan manajemen risiko digital dan keamanan siber Bank dalam memenuhi ekspektasi nasabah, *stakeholder* dan regulator.

Proses dan Metode

Dalam mengelola manajemen risiko digital dan keamanan siber, BNI menerapkan proses terstruktur yang melibatkan serangkaian aktivitas melalui identifikasi, penilaian, pengukuran, pemantauan dan pengendalian risiko produk dan aktivitas digital atas 8 (delapan) aspek risiko digital antara lain:

1. *Data privacy risk*

2. *Cybersecurity risk*
3. *Process automation risk*
4. *Third party risk*
5. *Compliance risk*
6. *Resiliency risk*
7. *Workforce risk*
8. *Cloud related risk*

Dalam pengelolaan risiko Bank menggunakan 2 (dua) pendekatan metode analitik dan prediksi pemodelan dari data-data yang didapatkan. Metode ini dilakukan secara berkelanjutan melalui kolaborasi antara *first line* dan *second line*, serta *third line* sebagai *evaluator* dan *reviewer* implementasi manajemen risiko. Bank juga memiliki beberapa program penguatan risiko digital dan keamanan siber antara lain *digital product assessment*, *thematic review*, *Cyber Security Incident Response Team*, *Social Engineering Technique Program* (SETP), dan lain-lain, sehingga menghasilkan suatu *risk reponse* yang efektif, cepat dan efisien.