H. Risiko Operasional

40. Perhitungan Risiko Operasional

a. Bank Secara Individu

(dalam juta rupiah)

Tabel Pengungkapan Kuantitatif Risiko Operasional Bank secara Individu

Pendekatan yang digunakan	31 Desember 2022			31 Desember 2021		
	Pendapatan bruto (rata-rata 3 tahun terakhir)	Beban Modal	ATMR	Pendapatan bruto (rata-rata 3 tahun terakhir)	Beban Modal	ATMR
Pendekatan Indikator Dasar	49.599.197	7.439.879	92.998.494	46.538.345	6.980.752	87.259.398
Total	49.599.197	7.439.879	92.998.494	46.538.345	6.980.752	87.259.398

b. Bank Secara Konsolidasi

(dalam juta rupiah)

Tabel Pengungkapan Kuantitatif Risiko Operasional Bank secara Konsolidasi dengan Entitas Anak

Pendekatan yang digunakan	31 Desember 2022			31 Desember 2021		
	Pendapatan bruto (rata-rata 3 tahun terakhir)	Beban Modal	ATMR	Pendapatan bruto (rata-rata 3 tahun terakhir)	Beban Modal	ATMR
Pendekatan Indikator Dasar	51.500.813	7.725.122	96.564.025	49.063.444	7.359.517	91.993.958
Total	51.500.813	7.725.122	96.564.025	49.063.444	7.359.517	91.993.958

41. Pengungkapan Kualitatif Umum 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.

Tata Kelola dan Organisasi

Tata kelola Manajemen Risiko Operasional telah diimplementasikan BNI dimana segenap unit bisnis dan unit pendukung baik di dalam maupun di luar negeri, berperan sebagai *Risk Owner* atau *Risk Taker* yang merupakan *first line of defense*. Implementasi tersebut didukung dengan *second line of defense* yang dijalankan oleh Divisi Enterprise Risk Management, Divisi Compliance, serta Divisi Policy Governance sebagai *Risk Control Unit* dan *third line of defense* yaitu Satuan Internal Audit sebagai *Risk Assurance Unit*. Selain itu, adanya Forum Komunikasi Kontrol Internal diharapkan dapat meningkatkan efektivitas komunikasi *first line of defense* dan *second line of defense* yang nantinya dapat meningkatkan kualitas identifikasi *Risk Exposure*.

Kebijakan dan Prosedur

Divisi Enterprise Risk Management telah memiliki Pedoman Penerapan Manajemen Risiko Operasional untuk mendukung implementasi Manajemen Risiko Operasional pada segenap unit baik di dalam maupun di luar negeri, yaitu:

1. Kebijakan Manajemen Risiko Operasional Dalam Negeri;
2. *Operational Risk Management Policy for Overseas Branches*.

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 Dalam Negeri;
2. Prosedur Pelaksanaan *Self Assessment* (SA) Risiko Operasional;
3. *Operational Risk Self Assessment Manual for Overseas Branches*;
4. Prosedur Pelaksanaan *Loss Event Database* (LED);
5. Prosedur Pelaksanaan *Key Risk Indicators* (KRI);
6. Pedoman Pelaksanaan Pembukuan Rekening Beban Risiko Operasional (BRO).

Proses

Manajemen Risiko Operasional BNI terdiri dari 5 (lima) proses utama yang berkesinambungan yaitu identifikasi, penilaian, pengukuran, pemantauan dan pengendalian risiko.

1. Identifikasi Risiko
   Mekanisme identifikasi Risiko Operasional dilakukan dengan menerapkan Macro Process Mapping Assessment atas proses kerja/ aktivitas masing-masing unit untuk menangkap potensi Risiko Operasional termasuk Risiko Digital dan risiko ahli daya yang dilakukan dengan metode *interview* (*one-on-one meeting*).
2. Penilaian Risiko
   Dilakukan oleh masing-masing unit pemilik risiko melalui metode *operational risk self assessment*, mencakup penilaian atas dampak, frekuensi, penyebab risiko dan mekanisme kontrol.
3. Pengukuran Risiko
   Dalam rangka perhitungan beban modal dan ATMR risiko operasional, saat ini Bank menggunakan metode *Basic Indicator Approach* (BIA) sesuai dengan Surat Edaran OJK No. 24/SEOJK.03/2016 perihal Perhitungan ATMR untuk Risiko Operasional dengan menggunakan Pendekatan Indikator Dasar (PID).
4. Pemantauan Risiko
   Dilakukan oleh seluruh unit sebagai *first line of defense* terhadap risiko utama pada saat aktivitas sedang berlangsung. Sedangkan Divisi Enterprise Risk Management melakukan evaluasi dan laporan/ *feedback* atas penilaian risiko berdasarkan hasil self assessment serta realisasi atas kerugian Risiko Operasional yang terjadi, meliputi:
   a. *Feedback report* untuk seluruh Divisi/ Satuan/ Wilayah/ Cabang;
   b. Laporan bulanan Pemantauan Beban Risiko Operasional kepada Direksi;
   c. Laporan Profil Risiko Operasional..
5. Pengendalian Risiko
   Mekanisme mitigasi Risiko Operasional tergambar pada proses pengendalian *intern* dengan menerapkan 4 (empat) strategi mitigasi, yaitu hindari, kurangi, transfer dan terima, dengan tujuan untuk meminimalkan kerugian akibat tidak berfungsinya proses internal, faktor manusia, sistem dan teknologi, serta kejadian eksternal. Keempat strategi mitigasi tersebut tertuang dalam prosedur mitigasi Risiko Operasional yang meliputi prosedur pengendalian, prosedur penyelesaian transaksi, prosedur akuntansi, prosedur penyimpanan aset dan kustodian, prosedur penyediaan produk dan prosedur pencegahan *fraud*.

Perangkat dan Metode

Untuk membantu proses pengelolaan Risiko Operasional yang dilakukan oleh setiap unit kerja, BNI telah mengembangkan perangkat Manajemen Risiko Operasional (*operational risk management tool*) berbasis situs *web* yang diberi nama *New* PERISKOP (Perangkat Risiko Operasional). *New* PERISKOP mempunyai peranan yang sangat penting, yaitu mensosialisasikan budaya risiko serta meningkatkan kesadaran risiko karena terdapat 4 (empat) proses utama dalam pengelolaan risiko operasional yang menggunakan perangkat ini, yaitu *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*). Hasil RCSA memberikan gambaran potensi risiko yang dihadapi unit untuk 6 (enam) bulan ke depan yang didasarkan pada data historis 6 (enam) bulan sebelumnya.
Modul *Loss Event Database* (LED)	Merupakan *database* atas seluruh kerugian finansial yang meliputi *actual loss* dan *near miss* sejak *event* terjadi hingga penyelesaiannya akibat risiko operasional yang terjadi di seluruh unit di Bank. Data kerugian 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 *Revised 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.

Business Continuity Management

Merupakan gangguan atau bencana yang diakibatkan 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 Cabang 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.

Kebijakan dan Prosedur

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 atas 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 acuan 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 (*Return Strategy*) dengan tujuan menyediakan cara mengembalikan fungsi dan aktivitas ke tingkat layanan sebelum terjadi bencana;

Pengembangan perangkat tersebut sejalan dengan peraturan regulator yang mewajibkan Bank untuk melaksanakan proses pengendalian risiko dalam mengelola 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 untuk dapat tetap beroperasi dan membatasi kerugian jika terjadi gangguan terhadap aktivitas bisnisnya. Selain peraturan regulator dan Basel II, untuk Kantor Cabang Luar Negeri, BCM diimplementasikan dengan memenuhi regulasi BCM di negara setempat.

MANAJEMEN RISIKO DIGITAL

Untuk mendukung pertumbuhan produk-produk digital, BNI telah menerapkan Manajemen Risiko Digital yang efektif melalui proses identifikasi, penilaian, pengukuran, pemantauan dan pengendalian risiko produk-produk digital atas 8 (delapan) aspek Risiko Digital yaitu *cybersecurity risk*, *third party risk*, *process automation risk*, *data privacy risk*, *resilience risk*, *compliance risk*, *cloud related risk* dan *workforce risk*.

BNI juga menerapkan pengendalian risiko digital melalui penguatan tata kelola/ *governance* manajemen risiko digital melalui Kebijakan/ Prosedur terkait *technology risk*, *information risk* dan *cybersecurity risk.*

Sejalan dengan pertumbuhan produk digital dan inovasi di bidang Teknologi Informasi (TI) akan berdampak peningkatan risiko ancaman keamanan siber. Untuk itu, BNI secara khusus melakukan beberapa penguatan Manajemen Risiko keamanan siber dengan standar penerapan Manajemen Risiko keamanan siber, pengujian keamanan ketahanan siber dan pelaporan penerapan Manajemen Risiko keamanan siber.