PENJELASAN

ATAS

PERATURAN BANK INDONESIA

NOMOR: 9/15/PBI/2007

TENTANG

PENERAPAN MANAJEMEN RISIKO DALAM PENGGUNAAN TEKNOLOGI INFORMASI OLEH BANK UMUM

UMUM

Dalam rangka meningkatkan efisiensi kegiatan operasional dan mutu pelayanan Bank kepada nasabahnya, Bank dituntut untuk mengembangkan strategi bisnis Bank dengan lebih banyak memanfaatkan kemajuan Teknologi Informasi untuk meningkatkan daya saing Bank.

Penerapan Teknologi Informasi telah membawa perubahan dalam kegiatan operasional serta pengelolaan data Bank sehingga dapat dilakukan secara lebih efisien dan efektif serta memberikan informasi secara lebih akurat dan cepat. Perkembangan produk perbankan berbasis teknologi diantaranya berupa *Electronic Banking* memudahkan nasabah untuk melakukan transaksi perbankan secara *non cash* setiap saat melalui jaringan elektronik. Selain itu penggunaan jasa pihak ketiga dalam penyediaan sistem dan pelayanan Bank semakin meningkat pula.

Disamping berbagai manfaat dan keunggulan yang diperoleh dari penggunaan Teknologi Informasi dalam pelaksanaan kegiatan operasional Bank, terdapat pula risiko yang dapat merugikan Bank serta nasabah seperti risiko operasional, risiko hukum, dan risiko reputasi selain risiko perbankan lainnya seperti risiko likuiditas dan risiko kredit.

Mengingat …

Mengingat bahwa Teknologi Informasi merupakan aset penting dalam operasional yang dapat meningkatkan nilai tambah dan daya saing Bank sementara dalam penyelenggaraannya mengandung berbagai risiko, maka Bank perlu menerapkan *IT Governance.* Keberhasilan penerapan *IT Governance* tersebut sangat tergantung pada komitmen seluruh unit kerja di Bank, baik penyelenggara maupun pengguna Teknologi Informasi. Penerapan *IT Governance* dilakukan melalui penyelarasan Rencana Strategis Teknologi Informasi dengan strategi bisnis Bank, optimalisasi pengelolaan sumber daya, pemanfaatan Teknologi Informasi (*IT value delivery),* pengukuran kinerja dan penerapan manajemen risiko yang efektif.

Untuk dapat menerapkan manajemen risiko yang efektif, diperlukan keterlibatan dan pengawasan Dewan Komisaris dan Direksi; penyusunan dan penerapan kebijakan dan prosedur terkait Teknologi Informasi; serta proses identifikasi, pengukuran, pemantauan dan pengendalian risiko yang berkesinambungan.

Selain itu, kedepan Bank dituntut pula untuk mengantisipasi kebutuhan akan infrastruktur Teknologi Informasi yang memadai dalam rangka menghadapi implementasi *Basel II.*

Dengan ketentuan ini, Bank diharapkan mampu mengelola risiko yang dihadapi secara efektif dalam seluruh aktivitas operasional yang didukung dengan pemanfaatan Teknologi Informasi.

PASAL DEMI PASAL

Pasal 1

Cukup jelas.

Pasal 2 …

Pasal 2

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Sumber daya Teknologi Informasi mencakup antara lain perangkat keras, perangkat lunak, jaringan, sumber daya manusia dan data/informasi.

Pasal 3

Kompleksitas usaha meliputi antara lain keragaman dalam jenis transaksi/produk/jasa dan jaringan kantor serta teknologi pendukung yang digunakan.

Pasal 4

Dalam menetapkan wewenang dan tanggung jawab tersebut perlu memperhatikan antara lain prinsip pemisahan tugas dan tanggung jawab (*segregation of duties)*, misalnya pihak yang melakukan input data berbeda dari pihak yang melakukan validasi data.

Pasal 5

Cukup jelas.

Pasal 6 …

Pasal 6

Huruf a

Cukup jelas.

Huruf b

Angka 1

Cukup jelas.

Angka 2

Upaya peningkatan kompetensi sumber daya manusia dilakukan antara lain melalui penyelenggaraan pendidikan atau pelatihan.

Angka 3

Cukup jelas.

Angka 4

Cukup jelas.

Angka 5

Cukup jelas.

Pasal 7

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Struktur komite dapat disesuaikan dengan ukuran dan kompleksitas kegiatan Bank serta struktur kepemilikan/*legal entity* Bank.

Huruf a sampai dengan huruf d

Cukup jelas.

Pasal 8 …

Pasal 8

Ayat (1)

Cukup jelas.

Ayat (2)

Kedalaman kebijakan dan prosedur selain disesuaikan dengan tujuan, kebijakan usaha, ukuran dan kompleksitas usaha Bank, juga memperhatikan profil risiko Bank.

Huruf a sampai dengan huruf i

Cukup jelas.

Ayat (3)

Limit risiko merupakan tingkat kesalahan yang masih bisa ditoleransi oleh sistem (*risk tolerance*) atau standar pengamanan yang ditetapkan atau disetujui untuk tidak dilampaui. Standar pengamanan ini disesuaikan dengan *risk appetite* yang dimiliki Bank.

Pasal 9

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Pasal 10

Cukup jelas.

Pasal 11

Cukup jelas.

Pasal 12 …

Pasal 12

Ayat (1)

Aktivitas operasional Teknologi Informasi mencakup aktivitas pada Pusat Data (*Data Center*), *Disaster Recovery Center* maupun pada pengguna Teknologi Informasi.

Huruf a sampai dengan huruf g

Cukup jelas.

Ayat (2)

Yang dimaksud memiliki sistem yang dapat menghasilkan laporan yang terpisah adalah yang dapat mengidentifikasikan input dan proses serta output dari transaksi berdasarkan prinsip syariah.

Pasal 13

Ayat (1)

Business Continuity Plan dan *Disaster Recovery Plan* disusun selain mencakup rencana pemulihan pada situasi *total disaster* juga pada berbagai tingkat gangguan dan bencana misalnya *minor* (berdampak kecil dan tidak memerlukan biaya besar serta dapat diselesaikan dalam jangka waktu pendek), *major* (berdampak besar dan dapat menjadi lebih parah apabila tidak diatasi segera) dan *catastrophic* (berdampak terjadi kerusakan yang bersifat permanen sehingga memerlukan relokasi/penggantian dengan biaya yang besar).

Yang dimaksud dengan dapat dilaksanakan secara efektif adalah operasional Teknologi Informasi dapat berjalan kembali segera setelah gangguan terjadi sehingga tidak mengganggu pelayanan kepada nasabah.

Ayat (2) …

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Pasal 14

Cukup jelas.

Pasal 15

Ayat (1)

Dalam melaksanakan sistem pengendalian intern Teknologi Informasi Bank mengacu pada prinsip-prinsip umum sebagaimana diatur dalam ketentuan mengenai pedoman standar sistem pengendalian intern.

Ayat (2)

Cukup jelas.

Ayat (3)

Yang dimaksud dengan memadai antara lain teknologi yang sesuai dengan kegiatan operasional Bank, sumber daya manusia yang kompeten dan struktur organisasi yang tidak memberikan peluang kepada siapapun untuk melakukan dan menyembunyikan kesalahan atau penyimpangan dalam pelaksanaan tugasnya.

Ayat (4)

Cukup jelas.

Pasal 16 …

Pasal 16

Ayat (1)

Ketentuan yang berlaku antara lain ketentuan mengenai standar pelaksanaan fungsi audit intern.

Ayat (2)

Penggunaan auditor ekstern untuk melaksanakan fungsi audit intern atas Teknologi Informasi tidak mengurangi tanggung jawab pimpinan Satuan Kerja Audit Intern Bank. Selain itu penggunaan auditor ekstern harus telah mempertimbangkan ukuran dan kompleksitas usaha Bank.

Ayat (3)

Cukup jelas.

Pasal 17

Cukup jelas.

Pasal 18

Ayat (1)

Yang dimaksud dengan menggunakan pihak penyedia jasa Teknologi Informasi adalah penggunaan jasa pihak lain dalam penyelenggaraan Teknologi Informasi Bank secara berkesinambungan dan/atau dalam periode tertentu. Yang dimaksud dengan pihak lain bagi kantor cabang bank asing termasuk kantor pusat dan kantor bank lainnya di luar negeri maupun kelompok usaha Bank. Yang dimaksud pihak lain bagi bank yang dimiliki pihak asing termasuk kantor induk dan kelompok usaha Bank.

Ayat (2) …

Ayat (2)

Huruf a

Angka 1

Yang dimaksud tanggung jawab Bank dalam menerapkan manajemen risiko antara lain dengan memastikan bahwa penyedia jasa menerapkan manajemen risiko secara memadai pada kegiatan Bank yang diselenggarakan oleh pihak penyedia jasa Teknologi Informasi sesuai yang dipersyaratkan dalam Peraturan Bank Indonesia ini.

Angka 2

Cukup jelas.

Angka 3

Cukup jelas.

Angka 4

Cukup jelas.

Angka 5

Akses untuk memperoleh data dan informasi dimaksudkan agar pemeriksaan dapat dilaksanakan secara efektif.

Angka 6

Akses terhadap *database* tersebut meliputi namun tidak terbatas pada penyediaan terminal, *user id* untuk melakukan *query*, dan *download* data.

Huruf b

Angka 1

Syarat ini dimaksudkan untuk meyakini bahwa Pusat Data (*Data Center*), *Disaster Recovery Center* dan/atau

Pemrosesan Transaksi Berbasis Teknologi yang digunakan oleh Bank memiliki pengendalian Teknologi Informasi yang memadai paling kurang mencakup *physical security* dan *logical security*.

Angka 2

Akses tersebut diperlukan untuk memperoleh data dan informasi yang diperlukan dalam rangka audit baik audit Teknologi Informasi maupun audit lainnya.

Angka 3

Pernyataan tersebut dibuktikan dengan dokumen berupa "Surat Pernyataan" yang harus dibuat oleh pihak penyedia jasa yang menyelenggarakan Pusat Data (*Data Center*), *Disaster Recovery Center,* dan/atau Pemrosesan Transaksi Berbasis Teknologi.

Angka 4

Yang dimaksud keamanan seluruh informasi adalah terpenuhinya prinsip kerahasiaan (*confidentiality*), integritas (*integrity*), dan keaslian (*authentication*).

Angka 5

Cukup jelas.

Angka 6

Cukup jelas.

Angka 7

Cakupan audit yang dilakukan oleh auditor independen termasuk sistem aplikasi yang digunakan untuk memproses data Bank.

Angka 8 …

Angka 8

Cukup jelas.

Angka 9

Cukup jelas

Ayat (3)

Cukup jelas.

Ayat (4)

Yang dimaksud dengan pihak terkait dengan Bank adalah pihak terkait sebagaimana diatur dalam ketentuan Bank Indonesia mengenai Batas Maksimum Pemberian Kredit Bank Umum.

Yang dimaksud dengan hubungan kerja sama secara wajar *(arm's length principle)* adalah kondisi dimana transaksi antar pihak bersifat independen sebagaimana pihak yang tidak terkait, antara lain memiliki kesetaraan dan didasarkan pada harga pasar yang wajar sehingga meminimalisasi terjadinya konflik kepentingan (*conflict of interest*).

Ayat (5)

Cukup jelas.

Ayat (6)

Indikasi kesulitan pengawasan antara lain:

a. kesulitan otoritas pengawas dalam akses terhadap data dan informasi;
b. kesulitan dalam pelaksanaan pemeriksaan terhadap pihak penyedia jasa;
c. pihak penyedia jasa digunakan sebagai media untuk melakukan rekayasa data Bank dan atau rekayasa keuangan Bank.

Pasal 19 …

Pasal 19

Ayat (1)

Cukup jelas.

Ayat (2)

Penyelenggaraan Pusat Data (*Data Center*) dan/atau *Disaster Recovery Center* di luar negeri yang harus mendapat persetujuan dari Bank Indonesia terlebih dahulu, termasuk penyelenggaraan pada kantor Bank, kantor induk maupun kelompok usaha Bank di luar negeri.

Penyelenggaraan Pusat Data (*Data Center*) dan/atau *Disaster Recovery Center* oleh kantor cabang dari Bank yang kantor pusatnya berkedudukan di Indonesia yang beroperasi di luar negeri pada kantor cabang tersebut tidak termasuk dalam ketentuan pada ayat (2).

Ayat (3)

Huruf a

Cukup jelas.

Huruf b

Yang dimaksud dengan "tidak mengurangi efektifitas pengawasan Bank Indonesia" adalah tidak menimbulkan kesulitan pengawas dalam memperoleh data dan informasi yang diperlukan seperti adanya akses terhadap database dan memiliki struktur database dari setiap aplikasi yang digunakan.

Huruf c

Ketentuan perundang-undangan yang berlaku di Indonesia antara lain ketentuan Bank Indonesia tentang tata cara pemberian perintah atau izin tertulis membuka rahasia Bank.

Huruf d …

Huruf d

Cukup jelas.

Huruf e

Cukup jelas.

Angka 1)

Cukup jelas.

Angka 2)

Cukup jelas.

Angka 3)

Yang dimaksud dengan kantor bank di luar negeri bagi kantor cabang bank asing adalah kantor pusat atau kantor lainnya. Sedangkan bagi Bank yang dimiliki lembaga keuangan asing yang dimaksud dengan kantor bank di luar negeri adalah kantor induk Bank tersebut.

Huruf f

Angka 1)

Manfaat yang diharapkan antara lain peningkatan kualitas layanan kepada nasabah.

Angka 2)

Cukup jelas.

Pasal 20

Ayat (1)

Yang dimaksud dengan prinsip kehati-hatian dalam ayat ini antara lain mengenai pengelolaan risiko atas produk dan aktivitas baru sebagaimana diatur dalam ketentuan mengenai manajemen risiko.

Yang dimaksud dengan produk dan aktivitas baru antara lain produk dan aktivitas yang menambah atau meningkatkan risiko pada Bank termasuk pengembangan pelayanan seperti pemasaran kredit.

Ayat (2)

Cukup jelas.

Ayat (3)

Penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi di luar negeri dalam ayat ini termasuk yang dilakukan pada kantor pusat atau kantor lainnya bagi kantor cabang bank asing atau kantor induk bagi bank yang dimiliki lembaga keuangan asing.

Ayat (4)

Cukup jelas.

Huruf a

Hubungan Bank dengan nasabah didasarkan atas perjanjian yang jelas dan memperhatikan ketentuan mengenai transparansi informasi produk dan penggunaan data pribadi nasabah serta ketentuan mengenai penyelesaian pengaduan nasabah. Bank tetap bertanggungjawab atas setiap transaksi yang pemrosesannya diserahkan kepada pihak penyedia jasa.

Huruf b

Yang dimaksud dengan "aktivitas *inherent banking functions*" adalah aktivitas yang terkait dengan tabungan, giro, deposito berjangka, dan kredit kecuali kartu kredit. Yang termasuk aktifitas terkait antara lain aktifitas pemeliharaan *master file* data pribadi nasabah.

Huruf c …

Huruf c

Yang dimaksud dengan dokumen pendukung administrasi keuangan adalah data yang merupakan bukti adanya hak dan kewajiban serta kegiatan usaha suatu perusahaan dan digunakan sebagai pendukung penyusunan laporan keuangan. Contoh: akad kredit dan dokumen pencairan kredit, *deal slip* dan *deal confirmation* transaksi *treasury* serta dokumen perintah transfer dana melalui SWIFT.

Huruf d

Upaya untuk meningkatkan peran Bank bagi perkembangan perekonomian Indonesia antara lain tercermin pada rencana peningkatan pemberian kredit, peningkatan pembiayaan ekspor impor.

Pasal 21

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Cukup jelas.

Ayat (4)

Laporan tersebut mencakup kajian paska implementasi (*post implemention review*).

Ayat (5)

Cukup jelas.

Ayat (6)

Yang dimaksud dokumen permohonan diterima secara lengkap adalah diterimanya dokumen yang dipersyaratkan dalam ketentuan ini serta diterimanya data tambahan apabila diperlukan.

Pasal 22

Ayat (1)

Ketentuan Bank Indonesia yang berlaku meliputi ketentuan yang mengatur mengenai produk, seperti ketentuan tentang Penyelenggaraan Kegiatan Alat Pembayaran dengan Menggunakan Kartu dan ketentuan lainnya seperti ketentuan tentang Penerapan Prinsip Mengenal Nasabah *(Know Your Customer)* dan ketentuan tentang Penerapan Manajemen Risiko serta ketentuan-ketentuan lain yang mengatur prinsip kehati-hatian dalam kegiatan usaha Bank.

Ayat (2)

Edukasi yang diberikan oleh Bank kepada nasabah dimaksudkan sebagai upaya meningkatkan pemahaman nasabah atas karakteristik produk *Electronic Banking,* baik dari aspek manfaat, risiko, pengamanan dan kemungkinan penyalahgunaan oleh pihak lain yang mengakibatkan kerugian nasabah.

Pasal 23

Ayat (1)

Cukup jelas.

Ayat (2)

Yang dimaksud dengan "produk *Electronic Banking*" adalah produk baru yang karakteristiknya berbeda dengan produk yang telah ada di Bank dan/atau menambah atau meningkatkan eksposur risiko tertentu pada Bank.

Ayat (3)

Cukup jelas.

Ayat (4)

Cukup jelas.

Ayat 5

Hasil pemeriksaan dari pihak independen di luar Bank diperlukan untuk produk *Electronic Banking* yang baru pertama kali diterbitkan oleh Bank seperti *internet banking* yang bersifat transaksional dan *sms banking*.

Sedangkan untuk penambahan fitur layanan produk *Electronic Banking* yang telah ada yang dapat menambah atau meningkatkan eksposur risiko, Bank dapat menyampaikan hasil pemeriksaan yang dilakukan oleh pihak internal Bank yang tidak terlibat dalam perancangan dan pengembangan sistem aplikasi serta pengambilan keputusan dalam implementasi aktivitas *Electronic Banking.*

Ayat (6)

Cukup jelas.

Ayat (7)

Laporan realisasi rencana penerbitan produk *Electronic Banking* mencakup kajian paska implementasi (*post implementation review)*.

Pasal 24

Ayat (1)

Cukup jelas.

Ayat (2)

Laporan ini berisi perubahan yang telah dilakukan selama satu tahun pelaporan atas data yang telah disampaikan dalam Laporan Penggunaan Teknologi Informasi, diluar perubahan yang telah dilaporkan dalam Laporan Perubahan Mendasar. Hal-hal yang perlu dilaporkan antara lain perubahan pejabat penentu dalam struktur organisasi Teknologi Informasi serta perubahan rencana jangka panjang (*IT Strategic Plan*).

Ayat (3)

Cukup jelas.

Pasal 25

Ayat (1)

Perubahan mendasar yang dilaporkan antara lain perubahan terhadap konfigurasi, aplikasi *core banking*, produk *Electronic Banking,* penggunaan pihak penyedia jasa di dalam negeri, dan perubahan mendasar lainnya yang dapat menambah atau meningkatkan risiko Bank.

Ayat (2)

Cukup jelas.

Ayat (3)

Dengan berlakunya ketentuan dalam ayat ini maka kewajiban menyampaikan laporan produk dan aktivitas baru sebagaimana diatur

dalam ketentuan manajemen risiko menjadi tidak berlaku untuk produk yang dilaporkan dengan format laporan realisasi ini.

Pasal 26

Ayat (1)

Cukup jelas.

Ayat (2)

Cukup jelas.

Ayat (3)

Yang termasuk dalam kejadian kritis adalah kegagalan sistem yang serius, *system down time* dan degradasi kinerja sistem yang mempengaruhi kinerja Bank dalam memberikan pelayanan kepada nasabah.

Ayat (4)

Laporan melalui e-mail atau telepon kepada pengawas Bank berdasarkan informasi awal yang tersedia.

Ayat (5)

Cukup jelas.

Pasal 27

Cukup jelas.

Pasal 28

Cukup jelas.

Pasal 29

Ayat (1)

Cukup jelas.

Ayat (2)

Penyediaan akses kepada Bank Indonesia dimaksudkan agar pengawasan oleh Bank Indonesia dapat dilaksanakan secara efektif antara lain memastikan integritas, validitas, ketersediaan dan keaslian data setiap transaksi yang dilakukan oleh Bank.

Akses tersebut termasuk :

a. akses terhadap *database* baik untuk data terkini maupun untuk data yang telah lalu;
b. akses terhadap infrastruktur pendukung seperti jaringan komunikasi.

Pasal 30

Cukup jelas.

Pasal 31

Cukup jelas.

Pasal 32

Cukup jelas.

Pasal 33

Cukup jelas.

Pasal 34

Cukup jelas.

Pasal 35

Ayat (1)

Permohonan persetujuan ulang disampaikan menggunakan format Laporan Rencana Perubahan Mendasar sebagaimana diatur dalam Surat Edaran Bank Indonesia.

Ayat (2)

Action plan antara lain berisi rencana pengembalian Pusat Data (*Data Center*), *Disaster Recovery Center* dan atau Pemrosesan Transaksi Berbasis Teknologi ke dalam negeri dan jangka waktu penyelesaian *action plan*.

Ayat (3)

Cukup jelas.

Pasal 36

Cukup jelas.

Pasal 37

Cukup jelas.

Pasal 38

Cukup jelas.

Pasal 39 …

Pasal 39

Cukup jelas.