BANK INDONESIA
Bank Sentral Republik Indonesia

Perbankan

Lampiran Surat Edaran Bank Indonesia Nomor 6/ 18 /DPNP tanggal 20 April 2004

# Pedoman Penerapan Manajemen Risiko pada Aktivitas Pelayanan Jasa Bank melalui Internet (*Internet Banking*)

Direktorat Penelitian dan Pengaturan Perbankan
2004

# DAFTAR ISI

# I. PENDAHULUAN

Perkembangan teknologi informasi telah mempengaruhi kebijakan dan strategi dunia usaha perbankan yang selanjutnya lebih mendorong inovasi dan persaingan di bidang layanan terutama jasa layanan pembayaran melalui Bank. Inovasi jasa layanan perbankan yang berbasis teknologi tersebut terus berkembang mengikuti pola kebutuhan nasabah Bank. Transaksi perbankan berbasis elektronis, termasuk internet merupakan salah satu bentuk pengembangan penyediaan jasa layanan Bank yang memberikan peluang usaha baru bagi Bank yang berakibat kepada perubahan strategi usaha perbankan, dari berbasis manusia (tradisional) menjadi berbasis teknologi informasi yang lebih efisien bagi Bank dan praktis bagi nasabah.

Namun demikian, disamping Bank memperoleh manfaat signifikan dari inovasi teknologi melalui transaksi perbankan berbasis internet tersebut, Bank juga menghadapi risiko yang melekat pada kegiatan dimaksud, antara lain risiko strategik, risiko reputasi, risiko operasional termasuk risiko keamanan dan risiko hukum, risiko kredit, risiko pasar dan risiko likuiditas. *Internet banking* pada dasarnya tidak menimbulkan risiko baru yang berbeda dari produk layanan jasa perbankan melalui media lain, tetapi disadari bahwa *internet banking* meningkatkan risiko tersebut. Secara khusus *internet banking* meningkatkan risiko strategik, risiko operasional termasuk risiko keamanan dan risiko hukum serta risiko reputasi. Oleh karena itu, disamping memanfaatkan peluang baru tersebut, Bank harus mengidentifikasi, mengukur, memantau dan mengendalikan risiko-risiko tersebut dengan prinsip kehati-hatian.

Pada dasarnya prinsip-prinsip yang diterapkan dalam manajemen risiko Bank secara umum berlaku pula untuk aktivitas *internet banking*, namun prinsip-prinsip tersebut perlu disesuaikan dengan memperhatikan risiko-risiko spesifik yang melekat pada aktivitas tersebut. Berdasarkan hal tersebut, prinsip manajemen risiko *internet banking* dibagi dalam tiga bagian yang tidak terpisahkan dan saling melengkapi yaitu pengawasan aktif komisaris dan direksi Bank, pengendalian pengamanan, serta manajemen risiko hukum dan risiko reputasi sebagai berikut:

## 1. Pengawasan Aktif Komisaris dan Direksi Bank

Mengingat Komisaris dan Direksi Bank bertanggung jawab dalam mengembangkan strategi bisnis Bank serta menetapkan pengawasan manajemen yang efektif atas risiko maka penyelenggaraan aktivitas *internet banking* harus didasarkan atas kebijakan tertulis yang informatif dan jelas yang ditetapkan oleh Komisaris dan Direksi Bank. Pengawasan manajemen yang efektif meliputi antara lain persetujuan dan kaji ulang terhadap aspek utama dari proses pengendalian pengamanan Bank.

### 2. Pengendalian Pengamanan

Proses pengendalian pengamanan memerlukan perhatian khusus dari manajemen karena adanya risiko pengamanan yang meningkat yang ditimbulkan oleh aktivitas *internet banking*. Sehubungan dengan itu, Bank perlu melakukan pengujian identitas nasabah, pengujian keaslian transaksi, penerapan prinsip pemisahan tugas, pengendalian terhadap penggunaan hak akses terhadap sistem, dan perlindungan terhadap integritas data maupun kerahasiaan informasi penting pada *internet banking*.

### 3. Manajemen Risiko Hukum dan Risiko Reputasi

Untuk melindungi Bank dari risiko hukum dan risiko reputasi, pelayanan jasa *internet banking* harus dilaksanakan secara konsisten dan tepat waktu sesuai dengan harapan nasabah. Agar dapat memenuhi harapan nasabah, Bank harus memiliki kapasitas, kontinuitas usaha dan perencanaan darurat yang efektif. Mekanisme penanganan kejadian (*incident response mechanism*) yang efektif juga sangat penting untuk meminimalkan risiko operasional, risiko hukum dan risiko reputasi yang timbul dari kejadian yang tidak diharapkan. Selain itu Bank perlu memahami dan mengelola risiko yang timbul dari hubungan Bank dengan pihak ketiga dalam menyelenggarakan *internet banking*.

## II. POKOK-POKOK PENERAPAN MANAJEMEN RISIKO – *INTERNET BANKING*

### 1. Pengawasan Aktif Komisaris dan Direksi Bank

a. Komisaris dan Direksi harus melakukan pengawasan yang efektif terhadap risiko yang terkait dengan aktivitas *internet banking*, termasuk penetapan akuntabilitas, kebijakan, dan proses pengendalian untuk mengelola risiko tersebut.

   1) Komisaris harus menyetujui kebijakan yang terkait dengan aktivitas *internet banking* dan mengevaluasi pelaksanaan kebijakan *internet banking* yang disampaikan oleh Direksi.

   2) Direksi harus melakukan kaji ulang terhadap rencana pelaksanaan *internet banking* yang berpotensi memiliki dampak yang signifikan terhadap strategi dan profil risiko Bank termasuk analisa *cost and benefit* dari rencana *internet banking* tersebut.

   3) Direksi harus memastikan bahwa Bank pada saat memasuki aktivitas *internet banking* telah memiliki manajemen risiko yang memadai. Selain itu Direksi harus memastikan bahwa pejabat atau pegawai yang terkait dengan aktivitas *internet banking* memiliki kompetensi dalam aplikasi dan teknologi pendukung

*internet banking* Bank.

4) Direksi harus melakukan pemantauan secara berkala terhadap risiko reputasi yang melekat pada *internet banking*, dan melaporkan hasil pemantauan tersebut kepada Komisaris.

5) Direksi harus memastikan bahwa proses manajemen risiko aktivitas *internet banking* Bank terintegrasi ke dalam manajemen risiko Bank secara keseluruhan.

6) Dalam melakukan pengawasan manajemen risiko Direksi harus:

   a) menetapkan limit risiko dalam kaitannya dengan *internet banking* dengan memperhatikan *risk appetite* Bank;

   b) menetapkan delegasi wewenang dan mekanisme pelaporan, termasuk prosedur yang diperlukan untuk kejadian yang berdampak pada kondisi keuangan dan reputasi Bank;

   c) memperhatikan faktor-faktor risiko yang secara khusus berhubungan dengan keamanan, integritas dan ketersediaan jasa *internet banking*;

   d) memastikan bahwa uji tuntas (*due dilligence*) dan analisis risiko yang memadai telah dilaksanakan sebelum Bank melakukan aktivitas *internet banking* secara *cross-border*.

b. Direksi harus menyetujui dan melakukan kaji ulang terhadap aspek utama dari prosedur pengendalian pengamanan Bank.

1) Direksi harus mengawasi pengembangan dan pemeliharaan secara kontinyu terhadap infrastruktur pengendalian pengamanan yang melindungi sistem dan data *internet banking* dari gangguan internal dan eksternal.

2) Direksi harus memastikan bahwa Bank memiliki kebijakan dan prosedur pengamanan yang menyeluruh untuk menangani potensi gangguan pengamanan internal dan eksternal, baik dalam bentuk tindakan pencegahan maupun penanganan kejadian (gangguan) tersebut. Prosedur pengamanan tersebut antara lain meliputi:

   a) penugasan tanggung jawab kepada pejabat atau pegawai Bank untuk mengawasi penyusunan kebijakan pengamanan Bank;

   b) pengendalian fisik yang memadai untuk mencegah *unauthorized physical access* terhadap ruang computer;

c) prosedur pengendalian logik dan pemantauan yang memadai untuk mencegah *unauthorized access* internal dan eksternal terhadap aplikasi dan *database internet banking*;

d) kaji ulang dan pengujian secara berkala terhadap langkah-langkah pengendalian pengamanan.

3) Untuk mendukung prosedur pengendalian pengamanan pada penyelenggaraan *internet banking*, maka Bank harus memperhatikan hal-hal sebagai berikut:

a) Bank harus menyusun dan memelihara profil pengamanan serta menetapkan hak otorisasi yang specifik (*specific authorization privileges*) bagi para pengguna sistem dan aplikasi *internet banking* seperti nasabah, satuan kerja/petugas Bank dan penyedia jasa (*outsourcing*);

b) Bank harus mengklasifikasikan data dan sistem *internet banking* berdasarkan sensitivitas, kepentingan dan tingkat perlindungannya, antara lain dengan menetapkan mekanisme yang tepat seperti enkripsi, pengendalian terhadap akses, dan rencana pemulihan data guna melindungi seluruh sistem, *server*, *database* dan aplikasi *internet banking* yang sensitif dan berisiko tinggi;

c) penyimpanan data yang sensitif atau berisiko tinggi pada sistem komputer Bank (*desktop* dan *laptop*) harus diminimalkan dan dilindungi oleh enkripsi, pengendalian terhadap akses, dan rencana pemulihan data;

d) kunci-kunci (*keys*) yang digunakan untuk keperluan enkripsi harus disimpan secara aman sehingga tidak ada satu orang pun yang secara utuh mengetahui kombinasi kunci-kunci tersebut;

e) Bank harus memiliki pengendalian fisik yang memadai guna mencegah (*unauthorized access*) terhadap sistem, *server*, *database* dan aplikasi *internet banking*;

f) Bank harus menerapkan berbagai metode dan teknik yang tepat untuk mengurangi ancaman eksternal terhadap sistem *internet banking*, seperti:

i. perangkat lunak *virus scanning* untuk seluruh *entry point* dan masing-masing sistem komputer (*desktop*);

ii. perangkat lunak dan perangkat penilaian sistem pengamanan lain secara berkala untuk mendeteksi penyusupan;

iii. pengujian penetrasi (*penetration testing*) terhadap jaringan internal dan eksternal harus dilakukan secara berkala sekurang-kurangnya 1 (satu) tahun sekali.

**2. Pengendalian Pengamanan (*Security Control*)**

a. Bank harus melakukan langkah-langkah yang memadai untuk menguji keaslian (otentikasi) identitas dan otorisasi terhadap nasabah yang melakukan transaksi melalui *internet banking*.

1) Bank harus menggunakan metode yang dapat diandalkan (*reliable)* untuk proses verifikasi identitas dan otorisasi nasabah baru serta proses pengujian keaslian identitas dan otorisasi nasabah lama.

2) Bank harus memiliki kebijakan dan prosedur tertulis untuk memastikan bahwa Bank mampu menguji keaslian identitas dan otorisasi dari nasabah. Bank dapat menggunakan berbagai metode untuk pengujian keaslian seperti *personal identification number* (PIN), *password,* dan sertifikat digital.

3) Bank harus menetapkan metode pengujian keaslian yang didasarkan atas penilaian manajemen terhadap risiko yang dihadapi oleh aktivitas *internet banking*. Penilaian risiko ini juga harus mengevaluasi kemampuan transaksi pada sistem *internet banking* seperti transfer dana, pembayaran tagihan, dan penarikan kredit, serta menilai sensitivitas dan nilai data yang disimpan, dan kemudahan nasabah untuk menggunakan metode pengujian keaslian.

4) Bank harus memantau dan menerapkan praktek *internet banking* yang sehat untuk memastikan bahwa:

a) *database* pengujian keaslian yang menyediakan akses kepada rekening nasabah pada *internet banking* dilindungi dari gangguan dan perusakan;

b) setiap penambahan, penghapusan atau perubahan *database* pengujian keaslian telah dengan tepat diotorisasi oleh pihak yang berwenang;

c) terdapat sarana pengendalian yang tepat terhadap sistem *internet banking* sehingga pihak ketiga yang tak dikenal tidak bisa menggantikan nasabah yang telah dikenal.

b. Bank harus menggunakan metode pengujian keaslian transaksi untuk menjamin bahwa transaksi tidak dapat diingkari oleh nasabah (*non repudiation*) dan menetapkan tanggung jawab dalam transaksi *internet banking*.

   Bank harus menyusun dan menetapkan prosedur yang tepat sesuai dengan signifikansi dan jenis transaksi *internet banking* untuk memastikan bahwa:

   1) sistem *internet banking* telah dirancang untuk mengurangi kemungkinan dilakukannya transaksi secara tidak sengaja (*unintended*) oleh para pengguna yang berhak;

   2) seluruh pihak yang melakukan transaksi telah diuji keasliannya;

   3) data transaksi keuangan dilindungi dari kemungkinan pengubahan dan setiap pengubahan dapat dideteksi.

c. Bank harus memastikan adanya pemisahan tugas dalam sistem *internet banking*, *database* dan aplikasi lainnya.

   Penetapan pemisahan tugas dalam sistem *internet banking* hendaknya memperhatikan hal-hal sebagai berikut:

   1) sistem dan proses transaksi harus dirancang untuk memastikan bahwa tidak ada karyawan/pihak ketiga yang dapat memasuki, melakukan otorisasi dan menyelesaikan suatu transaksi;

   2) adanya pemisahan tugas antara pihak yang menginisiasi data statik dan pihak yang bertanggung jawab untuk memverifikasi kebenaran data statik;

   3) perlu pengujian untuk memastikan bahwa penerapan pemisahan tugas tidak dapat dilampaui (di-*by pass*);

   4) adanya pemisahan tugas antara pihak yang mengembangkan dengan pihak yang menatausahakan sistem *internet banking*.

d. Bank harus memastikan adanya pengendalian terhadap otorisasi dan hak akses (*privileges*) yang tepat terhadap sistem *internet banking*, *database*, dan aplikasi lainnya.

   Dalam rangka memelihara pemisahan tugas, Bank harus mengendalikan secara ketat otorisasi dan penggunaan hak akses. Kegagalan untuk menyediakan dan menerapkan pengendalian otorisasi tersebut dapat memberikan kesempatan kepada pihak lain yang tidak memiliki hak akses untuk dapat melakukan hal-hal di luar kewenangannya.

Hal-hal yang perlu diperhatikan antara lain:

1) perlu adanya otorisasi dan hak akses yang spesifik kepada pihak-pihak yang berkaitan dengan aktivitas *internet banking*;

2) sistem *internet banking* dirancang dengan memperhatikan bahwa setiap sub sistem saling berinteraksi dalam suatu *database* otorisasi yang telah ditetapkan Bank;

3) pihak-pihak yang berkaitan dengan aktivitas *internet banking* tidak memiliki wewenang untuk mengubah otoritas atau hak akses terhadap *database* otorisasi *internet banking*;

4) penambahan atau perubahan dari pihak-pihak yang memiliki akses terhadap suatu *database* otorisasi *internet banking* harus diotorisasi oleh pihak yang memiliki kewenangan;

5) tersedianya langkah yang tepat untuk memastikan bahwa *database* otorisasi internet banking tahan terhadap gangguan, antara lain melalui pemantauan yang berkelanjutan, dan adanya jejak audit untuk mendokumentasikan gangguan tersebut;

6) setiap *database* otorisasi *internet banking* yang telah terganggu hendaknya tidak digunakan sampai dengan digantikan oleh suatu *database* yang valid;

7) terdapat pengendalian untuk mencegah setiap perubahan tingkat otorisasi selama terjadinya transaksi *internet banking* dan setiap upaya untuk mengubah otorisasi tersebut harus dicatat (*logged*) dan menjadi perhatian manajemen Bank.

e. Bank harus memastikan tersedianya prosedur yang memadai untuk melindungi integritas data, catatan/arsip, dan informasi pada transaksi *internet banking*.

Beberapa langkah yang dapat digunakan oleh Bank untuk memelihara integritas data di dalam sistem *internet banking* antara lain meliputi:

1) transaksi *internet banking* harus sangat resisten terhadap gangguan pada setiap proses transaksi;

2) arsip *internet banking* harus disimpan, diakses dan dimodifikasi sedemikian rupa sehingga resisten terhadap gangguan;

3) transaksi dan proses pencatatan *internet banking* harus dirancang sedemikian rupa sehingga tidak memungkinkan pengubahan yang tidak sah;

4) terdapat prosedur pemantauan dan pengujian yang memadai sehingga setiap perubahan pada sistem *internet banking* tidak mengurangi kehandalan data;

5) setiap gangguan pada transaksi atau pencatatan *internet banking* harus dapat dideteksi melalui pemrosesan transaksi, pemantauan dan pemeliharaan pencatatan.

f. Bank harus memastikan tersedianya mekanisme penelusuran (*audit trail)* yang jelas untuk seluruh transaksi *internet banking*.

1) Untuk memastikan tersedianya jejak audit yang jelas maka jenis transaksi *internet banking* yang harus diperhatilkan meliputi antara lain:

a) pembukaan, modifikasi atau penutupan suatu rekening nasabah;

b) setiap transaksi yang mengandung dampak keuangan;

c) setiap otorisasi yang memperbolehkan nasabah untuk melampaui batasan tertentu yang telah ditetapkan;

d) setiap pemberian, modifikasi dan pencabutan hak dan kewenangan untuk mengakses sistem.

2) Hal-hal yang harus diperhatikan untuk memastikan tersedianya *audit trail* yang jelas antara lain:

a) catatan/*log* harus dipelihara untuk semua transaksi *internet banking* guna tersedianya jejak audit yang jelas dan membantu penyelesaian perselisihan;

b) jejak audit maupun log-log lainnya, misalnya log tools pendeteksian penyusupan harus di*review*/evaluasi secara berkala;

c) sistem *internet banking* harus dirancang guna memperoleh bukti forensik dan mencegah timbulnya gangguan dan pengumpulan bukti yang tidak tepat;

d) apabila sistem pemrosesan dan jejak audit merupakan tanggung jawab dari pihak ketiga maka Bank harus mempunyai akses kepada jejak audit yang dipelihara oleh pihak ketiga tersebut dan jejak audit tersebut harus sesuai dengan standar yang ditetapkan Bank.

g. Bank harus mengambil langkah-langkah untuk melindungi kerahasiaan informasi penting pada *internet banking*. Langkah tersebut harus sesuai dengan sensitivitas informasi yang dikeluarkan dan/atau disimpan dalam *database*.

Untuk melindungi kerahasiaan dari informasi-informasi penting yang ada pada *internet banking*, Bank harus memastikan bahwa:

1) seluruh arsip dan data Bank yang bersifat rahasia hanya dapat diakses oleh pihak-pihak yang telah diotorisasi dan dibuktikan keasliannya;

2) semua data Bank yang bersifat rahasia harus dipelihara secara aman dan dilindungi dari kemungkinan diketahui atau dimodifikasi secara transmisi melalui jaringan publik, pribadi atau internal;

3) Bank harus memiliki standar dan pengendalian atas penggunaan dan perlindungan data apabila pihak ketiga/*outsourcing* memiliki akses terhadap data tersebut;

4) seluruh akses terhadap data yang sifatnya terbatas harus disimpan (*logged*) dan langkah yang tepat perlu dilakukan untuk memastikan bahwa data resisten terhadap gangguan.

**3. Manajemen Risiko Hukum dan Risiko Reputasi**

a. Bank harus memastikan bahwa *website* Bank menyediakan informasi yang memungkinkan calon nasabah untuk memperoleh informasi yang tepat mengenai identitas dan status hukum Bank sebelum melakukan transaksi melalui *internet banking*.

Informasi yang disediakan dalam *website* Bank antara lain:

1) nama dan tempat kedudukan Bank;

2) identitas otoritas pengawasan Bank;

3) tata cara bagi nasabah untuk mengakses unit pelayanan nasabah apabila terdapat masalah, pengaduan, penyalahgunaan rekening dan sebagainya;

4) tata cara bagi nasabah untuk mengakses program keluhan nasabah;

5) tata cara bagi nasabah untuk memperoleh informasi mengenai penjaminan simpanan dan perlindungan nasabah lainnya;

6) informasi relevan lainnya.

b. Bank harus mengambil langkah-langkah untuk memastikan bahwa ketentuan kerahasiaan nasabah diterapkan sesuai dengan yang berlaku di negara tempat kedudukan Bank menyediakan produk dan jasa *internet banking*.

1) Penyalahgunaan pengungkapan kerahasiaan data nasabah dapat menyebabkan Bank terekspos risiko hukum dan risiko reputasi. Oleh karena itu Bank harus melakukan tindakan yang memastikan bahwa:

a) kebijakan dan standar kerahasiaan nasabah sesuai dengan peraturan perundang-undangan yang berlaku tentang kerahasiaan nasabah/rahasia Bank;

b) nasabah diberikan pemahaman tentang kebijakan kerahasiaan nasabah Bank dan isu kerahasiaan terkait lainnya yang berkaitan dengan penggunaan produk dan jasa *internet banking*;

c) data nasabah tidak digunakan untuk tujuan di luar yang secara umum diperkenankan atau di luar otorisasi yang diberikan oleh nasabah;

d) standar penggunaan data nasabah wajib dipenuhi dalam hal pihak ketiga (*outsourcing*) mempunyai akses terhadap data nasabah;

2) Dalam rangka mendukung penerapan kerahasiaan informasi nasabah yang melakukan transaksi melalui *internet banking*, Bank harus memperhatikan hal-hal sebagai berikut:

a) penggunaan teknik enkripsi, prosedur khusus dan pengendalian pengamanan lainnya untuk memastikan kerahasiaan data nasabah *internet banking*;

b) pengembangan prosedur dan pengendalian yang memadai untuk menilai infrastruktur dan prosedur pengamanan nasabah *internet banking* secara berkala;

c) kepastian bahwa bahwa pihak ketiga (*outsourcing*) yang digunakan oleh Bank mempunyai kebijakan kerahasiaan yang konsisten dengan yang dimiliki Bank;

d) pengambilan langkah-langkah untuk menginformasikan nasabah *internet banking* tentang kebijakan kerahasiaan informasi nasabah tersebut, yang meliputi:

(1) pemberian informasi yang singkat dan jelas kepada nasabah mengenai kebijakan kerahasiaan yang dimiliki Bank, antara lain melalui *website* Bank;

(2) pemberian petunjuk kepada nasabah mengenai pentingnya untuk menjaga *password*, nomor identifikasi pribadi (PINs) dan data perbankan dan/atau data pribadi lainnya;

(3) penyediaan informasi kepada nasabah mengenai teknik pengamanan komputer pribadi nasabah, termasuk keuntungan dalam menggunakan perangkat lunak pengamanan virus, pengendalian terhadap akses fisik dan *firewall personal* untuk koneksi terhadap internet.

c. Bank harus memiliki prosedur perencanaan darurat dan kesinambungan usaha yang efektif untuk memastikan tersedianya sistem dan jasa *internet banking*.

1) Bank harus mampu menyediakan jasa *internet banking* melalui sistem dan aplikasi secara *in-house* maupun *outsourcing* kepada nasabah secara konsisten dan tepat waktu.

2) Untuk menjamin kesinambungan usaha jasa *internet banking*, Bank harus memastikan bahwa:

a) kapasitas sistem *internet banking* yang tersedia maupun peningkatan volume transaksi di masa depan telah dianalisis berdasarkan perkembangan eksternal dan proyeksi tingkat penerimaan produk dan jasa *internet banking* oleh nasabah;

b) pengujian dan kaji ulang berkala terhadap kapasitas pemrosesan transaksi *internet banking*;

c) pengujian secara berkala terhadap kesinambungan usaha dan perencanaan darurat untuk pemrosesan dan sistem penyampaian jasa *internet banking*.

3) Beberapa langkah yang perlu diperhatikan Bank dalam rangka penerapan rencana darurat, kesinambungan usaha dan peningkatan kualitas kapasitas *internet banking*, antara lain:

a) Bank harus mengidentifikasi dan mereview seluruh aplikasi dan jasa *internet banking*, termasuk yang disediakan oleh penyedia jasa/pihak ketiga;

b) Bank harus melakukan penilaian risiko pada setiap jasa dan aplikasi internet, termasuk implikasi yang mungkin timbul seperti risiko kredit, pasar, likuiditas, hukum, operasional dan reputasi yang dapat mengganggu kegiatan usaha Bank;

c) Bank harus menetapkan kriteria kinerja untuk setiap jasa dan aplikasi *internet banking* dan memantau pelaksanaannya dibandingkan dengan kriteria kinerja tersebut;

d) Bank harus mengambil langkah-langkah yang tepat untuk memastikan bahwa sistem *internet banking* mampu mengatasi volume transaksi yang besar maupun kecil, dan kinerja maupun kapasitas sistem tersebut konsisten dengan rencana Bank untuk pengembangan *internet banking* di masa datang;

e) Bank harus mengembangkan beberapa prosedur alternatif apabila sistem *internet banking* akan mencapai limit kapasitas tertentu;

f) Bank harus memiliki prosedur pemulihan sistem *internet banking* untuk menjaga kelangsungan usaha guna mengurangi ketergantungan kepada penyedia jasa/pihak ketiga maupun pihak eksternal lainnya;

g) rencana darurat *internet banking* meliputi suatu prosedur untuk memulihkan atau mengganti kemampuan pemrosesan *internet banking*, merekonstruksi informasi transaksi pendukung, dan untuk memulihkan keberadaan sistem dan aplikasi *internet banking* dalam hal terjadi gangguan kegiatan usaha.

d. Bank harus mengembangkan rencana penanganan yang memadai untuk mengelola, mengatasi, dan meminimalkan permasalahan yang timbul dari kejadian yang tidak diperkirakan (internal dan eksternal), yang dapat menghambat penyediaan sistem dan jasa *internet banking*.

1) Bank harus mengembangkan strategi komunikasi, yang dapat memastikan kesinambungan usaha, mengendalikan risiko reputasi, dan membatasi kewajiban Bank yang terkait dengan terganggunya jasa *internet banking*, termasuk yang berasal dari sistem dan operasional yang ditangani oleh pihak ketiga.

2) Untuk memastikan penanganan yang efektif terhadap kejadian yang tak diperkirakan, Bank harus mengembangkan:

a) rencana penanganan kejadian untuk mengatasi pemulihan sistem dan jasa *internet banking* dengan berbagai skenario;

b) mekanisme untuk mengidentifikasi suatu kejadian, menilai materialitasnya, dan mengendalikan risiko reputasi yang terkait dengan gangguan dalam pemberian jasa *internet banking*;

c) strategi komunikasi dengan pihak eksternal dan media untuk mengatasi permasalahan yang mungkin timbul sebagai akibat kegagalan pengamanan, gangguan sistem *on-line* dan sistem *internet banking*;

d) tim penanganan kejadian yang memiliki kewenangan untuk bertindak dalam keadaan darurat dan yang memiliki kompetensi dalam melakukan analisa sistem deteksi maupun menilai hasil/output dari sistem deteksi tersebut;

e) mekanisme instruksi yang jelas untuk memastikan bahwa tindakan yang diambil merupakan tindakan korektif yang tepat;

f) prosedur penyampaian informasi secara cepat dan tepat kepada nasabah Bank, *counterparty*, dan media mengenai penyebab terjadinya gangguan *internet banking* dan perkembangan penanganannya;

g) prosedur pengumpulan dan pemeliharaan bukti forensik untuk memfasilitasi kajian terhadap kejadian yang terkait dengan kegiatan *internet banking* maupun dalam membantu proses penuntutan hukum terhadap pihak eksternal yang mengganggu *internet banking*.

e. Dalam hal sistem penyelenggaraan *internet banking* dilakukan oleh pihak ketiga (*outsourcing*), Bank harus menetapkan dan menerapkan prosedur pengawasan dan *due dilligence* yang menyeluruh dan berkelanjutan untuk mengelola hubungan Bank dengan pihak ketiga tersebut.

Dalam pengelolaan hubungan tersebut, Bank harus memastikan bahwa:

1) Bank sepenuhnya memahami risiko yang terkait dengan perjanjian *outsourcing* atau kerjasama untuk penyediaan sistem dan aplikasi *internet banking*:

a) Bank harus mengidentifikasi tujuan strategik serta keuntungan dan kerugian yang berkaitan dengan penggunaan *outsourcing* dalam *internet banking*;

b) keputusan untuk melakukan *outsourcing* dalam *internet banking* harus konsisten dengan strategi usaha Bank dengan mempertimbangkan karakteristik risiko yang melekat pada

penggunaan *outsourcing*;

c) sesuai dengan struktur operasional, unit kerja Bank harus memahami tata kerja penyedia jasa (*provider*) yang melaksanakan strategi *internet banking*.

2) pelaksanaan *due dilligence* yang memadai terhadap kompetensi dan kondisi keuangan pihak ketiga yang menyediakan jasa (*service provider*) sebelum melakukan kontrak jasa *internet banking*:

a) Bank harus mempertimbangkan pengembangan proses dan menetapkan kriteria/persyaratan untuk pemilihan beberapa penyedia jasa;

b) Bank harus melakukan *due dilligence*, termasuk analisis risiko, kondisi keuangan, reputasi, kebijakan dan pengendalian manajemen risiko serta kemampuan penyedia jasa/layanan untuk memenuhi kewajibannya;

c) Bank harus secara berkala memantau dan melakukan review terhadap kemampuan penyedia jasa/layanan untuk memenuhi jasanya dan kewajiban penerapan manajemen risiko selama masa kontrak;

d) Bank harus memastikan tersedianya sumber daya manusia yang memadai dan mempunyai komitmen untuk melakukan pengawasan terhadap *outsourcing* yang menyelenggarakan *internet banking*;

e) Bank harus menetapkan tanggung jawab yang jelas kepada unit kerja atau petugas mengenai pengawasan terhadap pengelolaan *outsourcing*;

f) Bank harus menetapkan *exit strategy* yang tepat untuk mengelola risiko outsourcing apabila akan dilakukan langkah pemutusan kontrak dengan pihak *outsourcing*.

3) kejelasan cakupan tanggung jawab masing-masing pihak dalam perjanjian kontraktual dengan pihak ketiga, yang berkaitan dengan:

a) kewajiban kontraktual dari pihak-pihak yang ditunjuk serta tanggung jawab untuk membuat keputusan, termasuk jasa sub-kontrak;

b) tanggung jawab untuk menyediakan informasi kepada dan menerima informasi dari penyedia jasa/layanan, yaitu informasi dari penyedia jasa/layanan harus tepat waktu dan komprehensif sehingga memungkinkan Bank untuk menilai

tingkat dan risiko layanan *internet banking*;

c) peraturan yang secara khusus menetapkan cakupan (*coverage*) asuransi, kepemilikan dari penyimpanan data dari *server* atau *database* penyedia jasa/layanan, dan hak Bank untuk pemulihan data yang telah melampaui waktu tertentu serta pemutusan kontrak;

d) ekspektasi kinerja penyedia jasa, baik dalam kondisi normal maupun situasi darurat;

e) tersedianya pengaturan jaminan yang cukup, misalnya melalui klausul audit yang memastikan bahwa penyedia jasa/layanan mematuhi kebijakan Bank;

f) terdapat klausul pengaturan mengenai hak Bank untuk melakukan koreksi dan intervensi secara tepat waktu apabila kinerja penyedia jasa/layanan tidak sesuai dengan kontrak (di bawah standar yang disepakati);

g) penetapan hukum dan peraturan negara tertentu tentang kerahasiaan dan perlindungan nasabah, khususnya untuk pengaturan *cross-border outsourcing*;

h) tersedianya klausul hak Bank untuk melakukan *independent review* dan/atau audit terhadap sistem pengamanan, pengendalian intern dan kelangsungan usaha serta perencanaan darurat.

4) pengoperasian dan penyediaan sistem *internet banking* oleh pihak ketiga telah sesuai dengan kebijakan manajemen risiko, pengamanan dan kerahasiaan yang berlaku di Bank.

5) audit oleh auditor eksternal atau internal yang independen dilakukan secara berkala terhadap pengoperasian *internet banking* oleh pihak ketiga dengan frekuensi dan cakupan audit yang sama dengan apabila *internet banking* diselenggarakan secara *in-house*.

6) ketersediaan rencana darurat yang memadai untuk aktivitas *internet banking* yang dioperasikan oleh pihak ketiga, dengan cara antara lain:

a) Bank harus mengembangkan dan menguji secara periodik terhadap perencanaan darurat layanan dan sistem *internet banking* yang dioperasikan oleh pihak ketiga;

b) perencanaan darurat harus dapat memuat langkah penanganan oleh Bank dalam kondisi skenario terburuk (*worst case scenario*) agar kontinuitas usaha *internet*

*banking* tetap berlangsung meskipun terjadi gangguan yang dapat mempengaruhi operasional yang dilakukan pihak ketiga;

c) Bank harus memiliki tim atau petugas khusus yang bertanggungjawab untuk mengelola pemulihan dan menilai dampak keuangan yang ditimbulkan oleh suatu gangguan pada sistem *internet banking* yang dioperasikan oleh pihak ketiga.

---------- *00* ----------