BAB III

PERATURAN DAN PENERAPAN MANAJEMEN RISIKO LAYANAN PERBANKAN ELEKTRONIK DAN PRINSIP PERTANGGUNGJAWABAN BANK XYZ ATAS KERUGIAN NASABAH AKIBAT PENIPUAN *SIM SWAP*

A. Peraturan Manajemen Risiko Layanan Perbankan Elektronik dan Prinsip Pertanggungjawaban Bank

Dunia digital berkembang sangat cepat. Positifnya, masyarakat dapat memanfaatkan teknologi informasi tersebut untuk bertransaksi perbankan selama terhubung internet, kapan saja dan di mana saja. Namun hal tersebut juga dapat dimanfaatkan untuk tindak kejahatan yang menyebabkan kerugian. Untuk itu, Otoritas Jasa Keuangan terus mendorong perbankan di Indonesia untuk meningkatkan keamanan teknologi informasi, salah satunya melalui POJK MRTI.[102]

1. Peraturan Manajemen Risiko Layanan Perbankan Elektronik dalam Peraturan Otoritas Jasa Keuangan Nomor 38/POJK.03/2016 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum

Menurut pasal 2 ayat (1) POJK MRTI diatur bahwa "Bank wajib menerapkan manajemen risiko secara efektif dalam penggunaan teknologi

[102] Wawancara dengan Mudo Laksito Staf Informasi dan Dokumentasi KR 2 Jabar OJK melalui email, 1 Mei 2020.

informasi". Cakupan penerapan manajemen risiko secara efektif menurut Pasal 2 ayat (2) POJK MRTI diantaranya:

a. Pengawasan Aktif Direksi dan Dewan Komisaris

Dalam rangka meminimalisir terjadinya risiko yang terkait dengan penggunaan teknologi informasi dan untuk melindungi kepentingan bank dan nasabah, bank perlu menerapkan tata kelola teknologi informasi *(information technology governance)* yang dilakukan melalui penyelarasan rencana strategis teknologi informasi[103] yang keberhasilannya tergantung komitmen direksi, dewan komisaris, dan seluruh unit kerja di bank.[104]

Dalam Pasal 4 POJK MRTI disebutkan bahwa "Bank wajib menetapkan wewenang dan tanggung jawab yang jelas dari direksi, dewan komisaris, dan pejabat pada setiap jenjang jabatan yang terkait dengan penggunaan teknologi informasi"

Menurut Pasal 5 POJK MRTI wewenang dan tanggung jawab direksi terkait penggunaan teknologi informasi adalah:[105]

a. menetapkan rencana strategis teknologi informasi dan kebijakan bank terkait penggunaan teknologi informasi;
b. menetapkan kebijakan, standar, dan prosedur terkait penyelenggaraan teknologi informasi yang memadai dan mengomunikasikannya secara

[103] Rencana strategis teknologi informasi adalah dokumen yang menggambarkan visi dan misi teknologi informasi bank, strategi yang mendukung visi dan misi teknologi bank, dan prinsip-prinsip utama yang menjadi acuan dalam penggunaan teknologi informasi untuk memenuhi kebutuhan bisnis serta mendukung strategis jangka panjang, POJK MRTI, Pasal 1 angka 4.

[104] SEOJK MRTI, Hlm. 5.

[105] POJK MRTI, Pasal 5.

efektif, baik pada satuan kerja penyelenggara maupun pengguna teknologi informasi;

c. Direksi memastikan teradapat kegiatan peningkatan kompetensi sumber daya manusia yang terkait dengan penyelenggaraan dan penggunaan teknologi informasi.

Menurut Pasal 6 POJK MRTI wewenang dan tanggung jawab dewan komisaris terkait penggunaan teknologi informasi adalah:[106]

a. Mengevaluasi, mengarahkan, dan memantau rencana strategis penggunaan teknologi informasi dan kebijakan bank terkait penggunaan teknologi informasi; dan
b. Mengevaluasi pertanggungjawaban direksi atas penerapan manajemen risiko dalam penggunaan teknologi informasi.

Menurut Pasal 7 ayat (1) POJK MRTI "bank wajib memiliki komite pengarah teknologi informasi *(information technology steering committee)".*[107] Pasal 7 ayat (2) POJK MRTI menyebutkan tanggung jawab komite pengarah teknologi informasi kepada direksi paling sedikit terkait dengan:[108]

a. rencana strategis teknologi informasi yang sejalan dengan rencana strategis kegiatan usaha Bank;
b. perumusan kebijakan, standar, dan prosedur teknologi informasi yang utama;

[106] POJK MRTI, Pasal 6.
[107] POJK MRTI, Pasal 7 ayat (1).
[108] POJK MRTI, Pasal 7 ayat (2).

c. kesesuaian antara proyek teknologi informasi yang disetujui dengan rencana strategis teknologi informasi;
d. kesesuaian antara pelaksanaan proyek teknologi informasi dengan rencana proyek yang disepakati (project charter);
e. kesesuaian antara teknologi informasi dengan kebutuhan sistem informasi manajemen serta kebutuhan kegiatan usaha Bank;
f. efektivitas langkah-langkah dalam meminimalkan risiko atas investasi bank pada sektor teknologi informasi agar investasi Bank pada sektor Teknologi Informasi memberikan kontribusi terhadap pencapaian tujuan bisnis bank;
g. pemantauan atas kinerja teknologi informasi dan upaya peningkatan kinerja teknologi informasi;
h. upaya penyelesaian berbagai masalah terkait teknologi informasi yang tidak dapat diselesaikan oleh satuan kerja pengguna dan penyelenggara teknologi informasi secara efektif, efisien, dan tepat waktu; dan
i. kecukupan dan alokasi sumber daya yang dimiliki bank.

b. Kecukupan Kebijakan, Standar, dan Prosedur Penggunaan Teknologi Informasi

Menurut Pasal 8 ayat (1) bank wajib: “memiliki kebijakan, standar, dan prosedur penggunaan teknologi informasi dan wajib menerapkan kebijakan, standar, dan prosedur penggunaan teknologi informasi secara konsisten dan

berkesinambungan". [109] Bank juga wajib menurut Pasal 8 ayat (4): "melakukan kaji ulang dan pengkinian kebijakan, standar, dan prosedur tersebut".[110] kebijakan, standar, dan prosedur tersebut salah satunya meliputi aspek layanan perbankan elektronik.[111]

Selain itu, bank menurut Pasal 8 ayat (3) juga wajib "menetapkan limit risiko yang dapat ditoleransi untuk memastikan aspek terkait teknologi informasi dapat berjalan optimal".[112]

c. Kecukupan Proses Identifikasi, Pengukuran, Pemantauan, dan Pengendalian Risiko Penggunaan Teknologi Informasi

Dalam Pasal 10 ayat (2) POJK MRTI diatur bahwa bank wajib: "melakukan proses manajemen risiko teknologi informasi", dalam penjelasan pasal tersebut disebutkan bahwa yang dimaksud dengan proses manajemen risiko adalah mengidentifikasi, mengukur, memantau, dan mengendalikan.

Penulis akan memfokuskan pembahasan terhadap proses manajemen risiko dalam layanan perbankan elektronik, yang lebih detail diatur dalam SEOJK MRTI, proses manajemen risiko diantaranya adalah:

1) **Pengukuran risiko** terkait layanan perbankan elektronik dilakukan terhadap potensi kerugian yang terjadi *(loss event)* pada setiap jenis layanan perbankan elektronik.

[109] POJK MRTI, Pasal 8 ayat (1).
[110] POJK MRTI, Pasal 8 ayat (4).
[111] POJK MRTI, Pasal 8 ayat (2).
[112] POJK MRTI, Pasal 8 ayat (3).

2) **Pemantauan risiko**, untuk data memantau besar dan kecenderungan risiko dari setiap jenis layanan perbankan elektronik maka bank harus membuat pangkalan data *(database)* yang berisi data historis kerugian *(loss event database)* setiap jenis layanan perbankan elektronik[113]
3) **Pengendalian risiko**, dalam rangka pengendalian risiko bank harus melakukan mitigasi atas risiko umum dan risiko spesifik yang mungkin terjadi dalam layanan perbankan elektronik dengan memperhatikan prinsip pengendalian pengamanan data nasabah dan transaksi layanan perbankan elektronik, antara lain dengan:[114]
    a. melakukan langkah-langkah yang memadai untuk menguji keaslian (*authentication*) identitas dan kewenangan (*authorization*) nasabah yang melakukan transaksi melalui layanan perbankan elektronik;
    b. memiliki kebijakan dan prosedur tertulis untuk memastikan bahwa bank mampu menguji keaslian identitas dan kewenangan nasabah;
    c. menggunakan berbagai metode untuk menguji keaslian yang didasarkan atas penilaian manajemen risiko layanan perbankan elektronik, sensitivitas, dan nilai data yang disimpan. Dalam menggunakan metode pengujian keaslian, bank memperhatikan hal-hal sebagai berikut:
        1) menerapkan kombinasi paling sedikit 2 (dua) faktor otentikasi *(two-factor authentication*) yaitu "*what you know*" (seperti PIN

[113] SEOJK MRTI, Hlm. 89.
[114] SEOJK MRTI, Hlm. 91.

atau password), "*what you have*" (seperti identitas elektronik, kartu magnetis dengan chip, token, atau digital signature), dan/atau "*something you are*" (antara lain biometric seperti retina atau sidik jari);

2) persyaratan jumlah karakter minimum PIN. Khusus untuk PIN yang digunakan dalam alat pembayaran dengan menggunakan kartu, mobile banking, dan internet banking, panjang PIN harus paling sedikit terdiri dari 6 (enam) digit karakter;
3) adanya batasan maksimum kesalahan memasukkan PIN untuk menghambat upaya akses secara tidak sah;
4) Bank harus memastikan penerapan prinsip kehati-hatian dalam penggunaan metode pengujian keaslian.
5) Bank harus menyusun dan menetapkan prosedur untuk menjamin bahwa transaksi tidak dapat diingkari oleh nasabah (*non repudiation*) sehingga transaksi dapat dipertanggungjawabkan.

d. Memastikan terdapat pemisahan tugad dan tanggung jawab terkait penggunaan sistem, pangkalan data *(database)*, dan aplikasi layanan perbankan elektronik.
e. Memastikan adanya pengendalian terhadap otorisasi dan hak akses *(privileges)* yang tepat terhadap sistem, pangkalan data *(database)*, dan aplikasi layanan perbankan elektronik.

f. Memastikan metode dan prosedur yang diterapkan untuk melindungi integritas data, catatan, dan informasi terkait layanan perbankan elektronik.
g. Memastikan tersedianya mekanisme penelusuran *(audit trail)* yang jelas untuk seluruh transaksi layanan perbankan elektronik.
h. Melakukan pendeteksian dan pemantauan atas transaksi yang tidak sah atau tidak wajar misalnya melalui *intrusion detection system* (IDS) dan *fraud detection.* Selanjutnya bank harus memiliki prosedur penanganan masalah atau kejahatan yang terdeteksi.
i. Menerapkan langkah-langkah untuk melindungi kerahasiaan informasi layanan perbankan elektornik yang disesuaikan dengan tingkat sensitivitas informasi.
j. Memiliki rencana pemulihan bencana termasuk *contingency plan* yang efektif untuk memastikan tersedianya sistem dan jasa layanan perbnkan elektronik secara berkesinambungan.
k. mengembangkan rencana penanganan kejadian (*incident response plan*) yang cepat dan tepat untuk mengelola, mengatasi, dan meminimalisasi dampak suatu insiden, *fraud*, kegagalan sistem (intern dan ekstern), yang dapat menghambat penyediaan sistem dan jasa layanan perbankan elektronik.

Dalam Pasal 29 POJK MRTI diatur bahwa “Bank wajib menerapkan prinsip pengendalian pengamanan data nasabah dan transaksi layanan

perbankan elektronik pada setiap sistem elektronik pada setiap sistem elektronik yang digunakan oleh bank".

d. Sistem Pengendalian Intern atas Penggunaan Teknologi Informasi

Sistem pengendalian intern (SPI) yang efektif merupakan komponen penting dalam manajemen bank dan menjadi dasar bagi kegiatan operasional bank yang sehat dan aman. Audit intern teknologi informasi sebagai salah satu bagian dari SPI diperlukan untuk melakukan evaluasi terhadap penyelenggaraan teknologi informasi secara independen dan objektif untuk meningkatkan efisiensi dan efektivitas manajemen risiko, pengendalian intern, dan tata kelola yang baik.

Pasal 17 ayat (1) mengatur bahwa bank wajib "melaksanakan sistem pengendalian intern secara efektif terhadap seluruh aspek penggunaan teknologi informasi". Sistem pengendalian intern paling sedikit mencakup:[115]

a. Pengawasan oleh manajemen dan adanya budaya pengendalian;
b. Identifikasi dan penilaian risiko;
c. Kegiatan pengendalian dan pemisahan fungsi;
d. Sistem informasi, sistem akuntansi, dan sistem komunikasi; dan
e. Kegiatan pemantauan dan koreksi penyimpangan, yang dilakukan oleh satuan kerja operasional, satuan kerja audit intern maupun pihak lain.

Apabila bank tidak melaksanakan penerapan manajemen risiko, maka sebagaimana diatur Pasal 36 POJK MRTI bahwa bank yang tidak melaksanakan

[115] POJK MRTI, Pasal 17 ayat (2).

ketentuan penerapan manajemen risiko sesuai dengan POJK MRTI dapat dikenai sanksi administratif berupa:

a. Teguran tertulis
b. Penurunan tingkat kesehatan berupa penurunan peringkat faktor tata kelola dalam penilaian tingkat kesehatan bank
c. Larangan untuk menerbitkan produk atau melaksanakan aktivitas baru
d. Pembekuan kegiatan usaha tertentu dan/atau
e. Pencantuman anggota direksi, dewan komisaris, dan pejabat eksekutif dalam daftar tidak lulus melalui mekanisme penilaian kemampuan dan kepatutan.

2. Peraturan terkait Pertanggungjawaban Bank atas Kerugian Nasabah dalam Peraturan Otoritas Jasa Keuangan Nomor 1/POJK.07/2013 tentang Perlindungan Konsumen Sektor Jasa Keuangan

Pertanggungjawaban bank sebagai pelaku usaha terdapat dalam Pasal 29 POJK PKJK yang mengatur bahwa "pelaku usaha jasa keuangan wajib bertanggung jawab atas kerugian konsumen yang timbul akibat kesalahan dan/atau kelalaian, pengurus, pegawai pelaku usaha jasa keuangan dan/atau pihak ketiga yang bekerja untuk kepentingan pelaku usaha jasa keuangan".[116]

Mudo Laksito[117] dalam wawancara yang dilakukan pada tanggal 1 Mei 2020 melalui media email menuturkan bahwa pertanggungjawaban bank tidak

[116] POJK PKJK, Pasal 29.
[117] Wawancara dengan Mudo Laksito Staf Informasi dan Dokumentasi KR 2 Jabar OJK melalui email, 1 Mei 2020.

terbatas pada isi Pasal 29 POJK PKJK saja, karena bank juga wajib bertanggungjawab atas kerugian nasabah yang disebabkan oleh pihak ketiga yang tidak berkaitan dengan bank, misalnya pihak ketiga melakukan pembobolan pada rekening nasabah melalui *sim swap.*

Bentuk penggantian kerugian yang diterima nasabah terdapat dalam Pasal 19 ayat (2) yaitu penggantian kerugian yang dilakukan bank: "dapat berupa pengembalian uang atau penggantian barang dan/atau jasa yang sejenis atau setara nilainya, atau perawatan kesehatan dan/atau pemberian santunan yang sesuai dengan ketentuan peraturan perundang-undangan yang berlaku".

Bilamana bank menolak mengganti kerugian, sesuai dengan Pasal 53 POJK PKJK bahwa pelaku usaha jasa keuangan dan/atau pihak yang melanggar ketentuan dalam peraturan Otoritas Jasa Keuangan ini dikenakan sanksi administratif antara lain berupa:

a. peringatan tertulis;
b. denda yaitu kewajiban untuk membayar sejumlah uang tertentu;
c. pembatasan kegiatan usaha;
d. pembekuan kegiatan usaha; dan
e. pencabutan izin kegiatan usaha.

B. Kasus Posisi dalam Penerapan Manajemen Risiko Layanan Perbankan Elektornik dan Prinsip Pertanggungjawaban Bank XYZ atas Kerugian Nasabah Akibat Penipuan *Sim Swap*

1. Kronologi Penipuan *Sim Swap* yang Mengakibatkan Kerugian pada Nasabah Bank XYZ

a. Kasus Posisi

Jumat 3 Januari 2020 pukul 21.02 WIB berlokasi di gerai Indosat di Bintaro Jaya Xchange seseorang mengaku sebagai Ilham Bintang dan meminta mengganti *sim card* Indosat miliknya dan permintaan tersebut di penuhi pihak Indosat. Saat itu Ilham sedang berada di Sydney Australia.[118]

Sabtu 4 Januari 2020 sebelum berangkat menuju Melbourne Australia sinyal kartu Indosat milik Ilham Bintang tidak dapat digunakan dan berstatus "SOS", pada saat Ilham Bintang mencoba untuk mengakses aplikasi *mobile banking* dan *internet banking* beberapa kali, muncul notifikasi bahwa *password* salah. Senin 6 Januari 2020 Ilham bintang bermaksud melakukan penarikan tunai di mesin ATM Bank XYZ di Meulborne Australia namun tidak berhasil karena saldo tidak mencukupi. Saat Ilham meminta pihak Bank XYZ menutup rekeningnya, Ilham mendapatkan informasi data transksi bahwa melalui

[118] Iskandar Zulkarnaen, *Rekening Ilham Bintang Dibobol, ini Modusnya*, https://kaltara.antaranews.com/amp/berita/459344/rekening-ilham-bintang-dibobol-ini-modusnya (diakses tanggal 31 Mei 2020 pukul 19.21 WIB).

rekeningnya telah terjadi 98 transaksi tercatat.[119] Ternyata setelah peristiwa pencurian *sim card* miliknya, rekening Ilham Bintang di Bank XYZ dibobol.[120]

b. Modus Pembobolan

Kabid Humas Polda Metro Jaya Kombes Pol Yusri Yunus mengatakan dalam kasus ini modus pelaku diantaranya:

1) Pelaku mencari data nasabah dengan kartu kredit aktif melalui BI Checking atau melalui Sistem Laporan Informasi Keuangan (SLIK) OJK. SLIK berisi informasi data pribadi seseorang meliputi alamat, pekerjaan, jabatan, nomor telepon, dan nomor kartu kredit serta limit kartu kredit. Dalam kasus ini data SLIK OJK dijual melalui jejaring sosial facebbok oleh Hendri, Rifan dan Heni yang merupakan pegawai Bank Perkreditan Rakyat Bintara Pratama Sejahtera. [121]
2) Desar sebagai otak pembobolan menyuruh Jati Waluyo membuat KTP palsu dengan data Ilham Bintang yang kemudian digunakan untuk menggandakan *sim card* Indosat milik Ilham Bintang oleh Teti Rosmiwati, Wasno, Arman

[119] Wahyunanda Kusuma Pertiwi, *Ilham Bintang Ceritakan Bagaimana Kartu SIM-nya Ditukar hingga Rekening Dibobol*, https://tekno.kompas.com/read/2020/01/21/15065917/ilham-bintang-ceritakan-bagaimana-kartu-sim-nya-ditukar-hingga-rekening-dibobol?page=all#page2 (diakses tanggal 31 Mei 2020 Pukul 01.50 WIB)

[120]Brigitta Winasis, *Ilham Bintang Laporkan SIM Card Dicuri dan Rekeningnya Dibobol, Berikut Kronologinya*, https://wow.tribunnews.com/2020/01/20/ilham-bintang-laporkan-sim-card-dicuri-dan-rekeningnya-dibobol-berikut-kronologinya?page=1 (diakses tanggal 31 Mei 2002 Pukul 02.00 WIB).

[121] Antara, Martha Warta Silaban, *Satu Lagi Tersangka Pembobol Rekening Ilham Bintang Dibekuk*, https://metro.tempo.co/read/1316538/satu-lagi-tersangka-pembobol-rekening-ilham-bintang-dibekuk (diakses tanggal 2 Juni 2020 pukul 02.20 WIB).

Yunianto. Kebetulan pada saat penggandaan kartu *sim card* tersebut Ilham sedang di Australia sehingga penggandaan mudah dilakukan oleh pelaku.[122]

3) Desar dengan berbekal *sim card* Ilham mereset *password* aplikasi perbankan (*mobile banking* dan *internet banking*) milik Ilham dengan menggunakan kode OTP *(one-time password).* [123] Yusri menjelaskan sebelumnya tersangka Desar me-*reset password* akun email Ilham dengan menggunakan kode OTP juga. "setelah email terbuka, terbukalah data bank, jadi rekening Ilham Bintang di Bank XYZ habis terkuras" jelasnya.[124]

c. Kerugian yang Timbul

Kabid Humas Polda Metro Jaya Kombes Pol Yusri Yunus mengatakan total kerugian yang dialami Ilham Bintang dari kasus pembobolan rekening tersebut adalah: "Dari bank XYZ sebesar Rp. 200 juta dan dari Bank ABC sebesar Rp. 83 Juta. Akan tetapi dari pihak Bank ABC telah mengganti kerugian Ilham Bintang tersebut" tutur Yusri.[125]

---

[122] Ahmad Romadoni, *Alur Pembobolan Rekening Bank Ilham Bintang*, https://kumparan.com/kumparannews/alur-pembobolan-rekening-bank-ilham-bintang-1smSiR6NIeV (diakses tanggal 4 Juni 2020 pukul 22.42 WIB).

[123] *Ibid.*

[124] Flori Sidebang, *Ini Cara Pelaku Menguras Habis Rekening Ilham Bintang*, https://republika.co.id/berita/q57wr6377/ini-cara-pelaku-meguras-habis-rekening-ilham-bintang (diakses tanggal 6 Juni 2020 Pukul 08.20 WIB).

[125] Adhi Muhammad Daryono, *Akhir Pelarian Pembobol Rekening Ilham Bintang*, https://kumparan.com/kumparannews/akhir-pelarian-pembobol-rekening-ilham-bintang-1smbq52xbsG (diakses tanggal 2 Juni 2020 pukul 14.50).

d. Bank XYZ Menolak Mengganti Kerugian

Tanggal 6 Januari Ilham Bintang menyampaikan laporan atas pembobolan *mobile bangking* dan *internet banking* nya kepada Bank XYZ. Kemudian tanggal 7 Januari, Ilham mendapat respon atas laporannya tersebut dari Bank XYZ yang diwakili Anwar Zainuddin selaku *Head Region* Bank XYZ Jakarta melalui sambungan telepon. Bank XYZ menyampaikan permintaan maaf atas ketidaknyamanan yang dirasakan. Lalu Anwar berjanji akan menyelesaikan persoalan yang dihadapi Ilham dan menjanjikan pengembalian uang sebelum Anwar kembali ke Jakarta.[126]

Tanggal 13 januari 2020 Anwar kembali menelepon dan memberi kabar bahwa jajaran Direksi Bank XYZ tidak setuju usulan pengembalian uang dan menolak mengganti kerugian.[127]

2. Implementasi Manajemen Risiko Layanan Perbankan Elektronik dan Pelaksanaan Prinsip Pertanggungjawaban Bank XYZ atas Penipuan *Sim Swap* yang Merugikan Nasabah

a. Implementasi Manajemen Risiko Layanan Perbankan Elektronik Bank XYZ

Penelitian ini dilakukan pada masa pandemi covid-19 yang menyebabkan penulis tidak dapat leluasa melakukan penelitian dengan maksimal terutama untuk melakukan wawancara langsung kepada

[126] Widian Vebriyanto, *Ilham Bintang dan Bank XYZ Sepakat Tempuh Jalur Hukum,* https://hukum.rmol.id/read/2020/01/27/419158/ilham-bintang-dan-bank-XYZ-sepakat-tempuh-jalur-hukum (diakses pada tanggal 31 Mei 2020 pukul 18.55 WIB).

[127] *Ibid.*

perwakilan Bank XYZ. Sehingga penulis menggunakan data tersier berupa laporan tahunan Bank XYZ pada tahun 2019 yang dapat diakses di *website* bank untuk mendapat gambaran awal bagaimana pelaksanaan penerapan manajemen risiko berdasarkan POJK MRTI.

1) Pengawasan Aktif Direksi dan Dewan Komisaris

Pengawasan aktif direksi tampak pada bagian laporan tahunan Bank XYZ di dalam tugas dan tanggungjawab direksi juga tugas dan tanggung jawab komite pengarah teknologi informasi.

Dalam hal ini Direksi dibantu oleh komite pengarah teknologi informasi yang menetapkan rencana strategis teknologi informasi Bank XYZ dan memantau kegiatan teknologi informasi terkait penyelarasan rencana strategis teknologi informasi dengan strategi bisnis bank, optimalisasi pengelolaan sumber daya, nilai yang diberikan teknologi informasi (*IT value delivery),* pengukuran kinerja dan efektivitas penerapan manajemen risiko. [128] Selain itu direksi menetapkan kebijakan, standar, dan prosedur terkait penyelenggaraan teknologi informasi dibantu oleh komite pengarah teknologi informasi. Direksi juga mengembangkan dan memastikan pelaksanaan manajemen risiko di semua tingkatan organisasi Bank XYZ.[129]

Pengembangan sumber daya manusia dilakukan Bank XYZ melalui penyelenggaraan pelatihan dan pengembangan terhadap keterampilan teknis manajemen risiko dan teknologi informasi dalam bentuk pelatihan dan

[128] Laporan Tahunan Bank XYZ Tahun 2019, Hlm. 150.
[129] *Ibid*, Hlm. 138.

workshop. Keterangan tersebut terdapat pada bagian Sumber Daya Manusia dalam Laporan Tahunan Bank XYZ.[130]

Pengawasan aktif komisaris tampak pada bagian laporan tahunan Bank XYZ di dalam tugas dan tanggungjawab Komisaris. Dalam hal ini dewan komisaris melaksanakan pengawasan atas kinerja direksi secara aktif mengenai segala tugas dan tanggung jawabnya, serta memberikan rekomendasi, saran, juga memantau dan mengevaluasi pelaksanaan kebijakan strategis Bank XYZ. Pengaturanya terdapat dalam pedoman dewan komisaris melalui rapat dewan komisaris yang selalu dilaksanakan minimal empat kali setahun serta rapat gabungan dengan direksi maupun rapat komite. [131]

Data mengenai komite pengarah teknologi informasi (ITSC) tampak pada bagian laporan tahunan Bank XYZ di dalam tugas dan tanggungjawab komite ITSC.

Bank XYZ telah memiliki komite pengarah teknologi informasi (ITSC) yang berada dibawah direksi dan membantu dalam memantau kegiatan teknologi informasi terkait penyelenggaraan rencana strategis teknologi informasi dengan strategi bisnis bank. tugas dan tanggung jawab ITSC Bank XYZ secara umum adalah memastikan:[132]

a) Keselarasan rencana serta implementasi strategis teknologi infromasi dengan strategi bisnis bank.
b) Efektivitas implementasi kebijakan pengamanan informasi bank.

[130] *Ibid*, Hlm. 105.
[131] *Ibid*, Hlm 135.
[132] *Ibid*, Hlm. 151.

c) Efektivitas langkah-langkah mitigasi risiko yang dilakukan untuk meningkatkan pengamanan informasi bank.

Selain tugas dan tanggung jawab secara umum, ITSC memiliki tugas dan tanggung jawab secara khusus namun tidak terbatas pada:[133]

a) Rencana strategis teknologi informasi sejalan dengan rencana strategis kegiatan usaha bank.
b) Perumusan kebijakan, standar, dan prosedur teknologi informasi yang utama, misalnya kebijakan pengamanan teknologi informasi dan manajemen risiko terkait penggunaan teknologi informasi.
c) Kesesuaian antara teknologi informasi dengan kebutuhan sistem informasi manajemen serta kebutuhan kegiatan usaha bank.
d) Efektivitas langkah-langkah dalam meminimalisasi risiko atas investasi bank pada sector teknologi informasi memberikan kontribusi terhadap pencapaian tujuan bisnis bank.
e) Pemantauan atas kinerja teknologi informasi dan upaya peningkatan kinerja teknologi informasi.
f) Upaya penyelesaian berbagai masalah terkait teknologi informasi yang tidak dapat diselesaikan oleh satuan kerja pengguna dan penyelenggara teknologi informasi secara efektif, efisien, dan tepat waktu.

[133] *Ibid*.

2) Kecukupan Kebijakan, Standar, dan Prosedur Penggunaan Teknologi Informasi

Data mengenai kebijakan, standar dan prosedur penggunaan teknologi informasi Bank XYZ tampak pada bagian laporan tahunan Bank XYZ dalam tugas dan tanggungjawab ITSC serta pada bagian Manajemen risiko.

Kebijakan, standar, dan prosedur penggunaan teknologi informasi Bank XYZ disusun oleh direksi bersama dengan komite pengarah teknologi informasi (ITSC). Kebijakan dan prosedur tersebut diperbarui secara berkala.[134]

Bank telah menetapkan limit risiko untuk setiap jenis potensi risiko yang melekat dalam aktivitas bank, selain itu bank juga mengevaluasi dan memantau kepatuhan terhadap *risk appetite,* toleransi dan limit risiko yang dipantau oleh komite pemantau risiko.[135]

3) Kecukupan proses identifikasi, pengukuran, pemantauan dan pengendalian risiko penggunaan teknologi informasi

Proses manajemen risiko tampak pada bagian laporan tahunan Bank XYZ dalam bagian manajemen risiko serta pada syarat dan ketentuan yang berada di *website* Bank XYZ.

[134] *Ibid*, Hlm 161.
[135] *Ibid*.

Bank secara umum telah melakukan proses manajemen risiko meliputi identifikasi, pengukuran, pemantauan dan pengendalian risiko. Identifikasi risiko dilakukan melalui analisis risiko yang melekat *(inherent risk)* antara lain risiko-risiko yang timbul dari produk, layanan dan kegiatan usaha Bank.[136]

Pengukuran risiko dilakukan secara berkala dengan menggunakan metode pengukuran yang ditetapkan oleh regulator atau *"best practice"* antara lain melalui *risk scoring*, *stress testing*, serta kesesuaian limit yang ditetapkan dengan *risk appetite*. Hal tersebut dilakukan evaluasi secara berkala terhadap asumsi, sumber data dan prosedur yang digunakan untuk mengukur risiko, pemantauan risiko dilakukan melalui pelaporan secara periodik atas eksposur risiko untuk memastikan tingkat risiko yang diambil sesuai dengan *risk appetite* Bank.[137]

Pemantauan risiko dilakukan oleh masing-masing unit kerja dan Direktorat Manajemen Risiko. Hasil pemantauan tersebut disampaikan kepada manajemen senior Bank secara berkala untuk dilakukan mitigasi risiko dan tindak lanjut yang diperlukan.[138]

Bank memiliki sistem pengendalian risiko yang memadai sesuai dengan eksposur risiko yang dihadapi, tingkat risiko yang diambil dan toleransi risiko. Pengendalian risiko antara lain dilakukan melalui penetapan limit risiko dan *early warning indicators* yang merupakan

[136] *Ibid*, Hlm. 59.
[137] *Ibid*.
[138] *Ibid*.

mekanisme pengendalian risiko dalam aktivitas bisnis Bank. Limit dipantau dan dievaluasi secara berkala sesuai dengan perubahan bisnis, perekonomian dan peraturan regulator. [139] Dalam pengendalian manajemen risiko *mobile banking* dan *internet banking*, bank memberikan *username/user id, password* kepada nasabah serta nasabah diwajibkan memiliki nomor telepon genggam dengan provider lokal agar dapat menerima kode OTP *(one-time password)* sebagai SMS token yang digunakan untuk otorisasi transaksi melalui *internet banking* dan *mobile banking.*[140]

Bank menerima dan menjalankan setiap instruksi dari nasabah sebagai instruksi yang sah berdasarkan penggunaan *username, password,* dan SMS OTP. Nasabah bertanggung jawab atas keaslian maupun keabsahan atau kewenangan penggunaan *username, password,* dan SMS OTP tersebut.[141]

Bank telah menetapkan jumlah karakter minimum *password mobile banking* dan *internet banking* berjumlah enam sampai dua belas karakter yang terdiri dari kombinasi huruf dan angka.[142]

Untuk keperluan pemantauan profil dan transaksi nasabah, Bank XYZ telah memiliki sistem aplikasi untuk mengidentifikasi, menganalisa, memantau, dan menyediakan laporan mengenai karakteristik transaksi

---

[139] *Ibid*.

[140] Bank XYZ, *syarat dan ketentuan*, https://www.commbank.co.id/id/bisnis/syarat-dan-ketentuan_1/syarat-ketentuan_1 (diakses tanggal 1 Juli 2020 pukul 20.00 WIB).

[141] *Ibid.*

[142] *Ibid.*

yang dilakukan nasabah, termasuk identifikasi transaksi keuangan mencurigakan.[143]

4) Sistem Pengendalian Intern atas Penggunaan Teknologi Informasi

Sistem pengendalian intern atas penggunaan teknologi informasi tampak pada bagian laporan tahunan Bank XYZ dalam sistem pengendalian intern serta dalam struktur organisasi satuan kerja manajemen risko.

Penerapan tersebut sudah dilaksanakan dalam mendukung pelaksanaan manajemen risiko sesuai dengan tujuan bisnis bank. Hal ini dibuktikan dengan bank yang telah menerapkan sistem pengendalian internal bank melalui kerangka tiga lini akuntablitas [144] Direksi melaksanakan lini pertama, kedua, dan ketiga sedangkan dewan komisaris melaksanakan lini ketiga.

Lini Pertama bertanggung jawab untuk identifikasi, penilaian, eskalasi, pemantauan dan pelaporan risiko serta kelemahan pengendalian atau proses selama kegiatan usaha. Lini Kedua menetapkan kerangka kerja dan kebijakan Manajemen Risiko dan memastikan kebijakan tersebut dilaksanakan dengan baik. Lini ketiga merupakan lini pengawasan, SKAI mengulas audit secara berkala dengan akuntabilitas kepada manajemen, direksi dan dewan komisaris.[145] SKAI melakukan

[143] Laporan Tahunan Bank XYZ Tahun 2019, Hlm. 159.
[144] *Ibid*, Hlm. 161.
[145] *Ibid*.

pemantauan atas pencapaian rencana audit serta risiko-risiko yang muncul.[146] SKAI selaku lini tiga bertindak sebagai penilai independen atas efektivitas sistem pengendalian internal yang dilakukan oleh lini satu dan dua dengan menjalankan rencana tahunan audit yang telah disetujui oleh direktur utama dan dewan komisaris melalui ketua komite audit.[147]

Mengenai pengawasan manajemen sistem pengendalian intern tampak pada laporan tahunan Bank XYZ dalam tugas dan tanggungjawab komisaris.

Dewan komisaris mengkaji efektivitas dan efisiensi sistem pengendalian intern berdasarkan informasi yang diperoleh dari SKAI paling sedikit sekali dalam satu tahun. Selain itu memastikan bahwa direksi telah menyusun dan memelihara sistem pengendalian intern yang memadai, efektif dan efisien, serta bersama direksi menindaklanjuti temuan audit dan rekomendasi dari satuan kerja audit internal (SKAI).[148]

b. Prinsip Pertanggungjawaban Bank XYZ atas kerugian Nasabah akibat Penipuan *Sim Swap*

Tanggal 6 Januari 2020 Ilham Bintang melaporkan telah terjadi pembobolan *mobile banking* dan *internet banking* miliknya kepada Bank XYZ. Tanggal 7 Januari 2020 Bank XYZ yang diwakili *Head Region* Bank XYZ Jakarta Anwar Zainuddin memberikan respon akan mengembalikan

[146] *Ibid*, Hlm. 156.
[147] *Ibid*.
[148] *Ibid*, Hlm. 135.

uang Ilham Bintang. Akan tetapi, tanggal 13 Januari Anwar menyampaikan keputusan jajaran Direksi Bank XYZ yang tidak setuju usulan pengembalian uang dan menolak mengganti kerugian pada kasus *sim swap* yang terjadi kepada Ilham Bintang dengan pertimbangan transaksi yang dilakukan sudah sesuai dengan prosedur bank.[149]

Menurut SVP Corporate Communications & Financial Inclusion Bank XYZ Bayu Irawan mengatakan bahwa transaksi *mobile banking* dan *internet banking* Ilham Bintang, yang menurutnya dilakukan oleh pelaku penipuan *sim swap,* telah dilakukan sesuai dengan prosedur bank. "Transaksi dilakukan dengan *user id* dan *password* yang benar. Sebelum transaksi dijalankan, bank selalu mengirimkan OTP (*one-time password)* untuk konfirmasi transaksi baik yang melalui *mobile banking* maupun *internet banking* sesuai dengan prosedur bank. Sesudah transaksi dijalankan, sesuai dengan prosedur bank, akan dikirimkan notifikasi melalui sms dan email".[150]

Dalam syarat dan ketentuan Bank XYZ semua transaksi *mobile banking* dan *internet banking* yang dilakukan dengan mempergunakan OTP *(one-time password)* baik dipergunakan dengan atau tanpa sepengetahuan nasabah bagaimanapun pelaksanaannya menjadi tanggung jawab penuh nasabah. Sehingga Bank XYZ tidak perlu mengganti kerugian Ilham Bintang, apabila mengacu pad syarat dan ketentuan tersebut.[151]

---

[149] Widian Vebriyanto, *loc.cit.*

[150] Sylke Febrina Lauereno, *Rekening Ilham Bintang Dibobol, Commonwealth Buka Suara,* https://finance.detik.com/moneter/d-4866122/rekening-ilham-bintang-dibobol-commonwealth-buka-suara (diakses tanggal 31 Mei 2020 Pukul 16.24 WIB).

[151] Bank XYZ, *loc.cit.*