BAB IV
ANALISIS MANAJEMEN RISIKO LAYANAN MOBILE BANKING

A. BSM Mobile

BSM Mobile adalah layanan transaksi perbankan melalui *mobile banking (handphone)* dengan menggunakan koneksi jaringan data yang dapat digunakan oleh nasabah dalam 24 jam/hari.[1] BSM Mobile termasuk fasilitas perbankan yang mempunyai fungsi yang sama seperti ATM kecuali mengambil uang tunai.[2] Setiap nasabah yang membuka rekening akan dianjurkan memakai layanan BSM Mobile. Manfaat yang dimiliki BSM Mobile adalah untuk transaksi cek saldo, cek mutasi transaksi, transfer antar rekening BSM, transfer *real time* ke 83 bank, transfer SKN, pembayaran tagihan, pembelian isi ulang pulsa seluler dan transaksi lainnya.

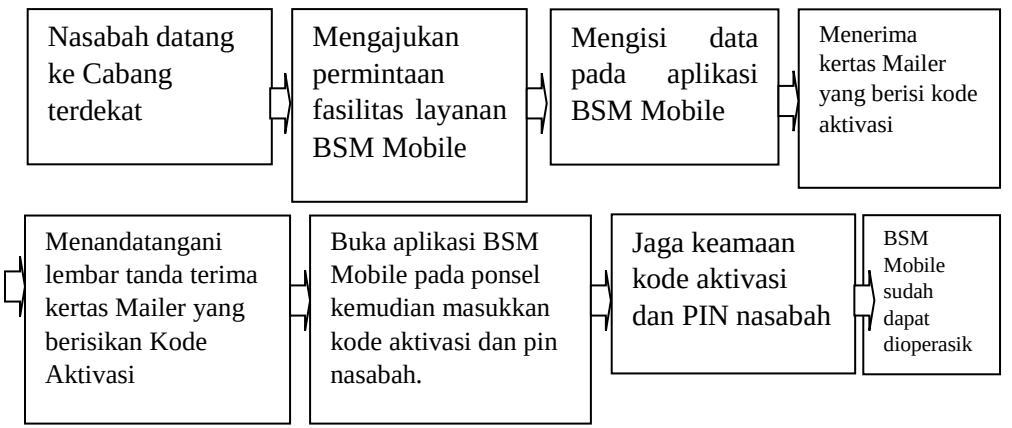
Melalui layanan ini, nasabah tidak perlu mengingat perintah transaksi seperti jika menggunakan SMS Banking. Menu transaksi BSM Mobile mencakup cek saldo, info mutasi rekening, pembelian pulsa, pembayaran tagihan, transfer

[1] https://www.syariahmandiri.co.id./category/layanan-24-jam/bsm-mobile-banking/, diakses 24 April 2017.

[2] Wiji Nurastuti, *Teknologi Perbankan*, Yogyakarta: Graha Ilmu, 2011, h. 110.

hingga pencarian lokasi ATM/cabang Bank Syariah Mandiri yang dilengkapi dengan peta. Keunggulan yang dimiliki BSM Mobile yaitu fitur menu yang dilengkapi dengan penawaran produk dan promo, jadwal shalat dan Hikmah (kata-kata mutiara). Dengan penggunaan BSM Mobile, nasabah tidak perlu lagi mendatangi cabang Bank hanya untuk transaksi perbankan. Sehingga dapat menghemat waktu dan biaya. Waktu yang biasanya digunakan untuk mengantri bisa digunakan untuk melakukan aktivitas lainnya.

Gambar 4. Prosedur Registrasi Layanan BSM Mobile



Gambar diatas menjelaskan tentang *Standard Operating Procedure* (SOP) nasabah yang akan mendaftar layanan BSM Mobile. SOP BSM Mobile sama seperti dengan SOP *mobile banking* milik bank lain pada umumnya. Sebelum

mengaktivasi *mobile banking* yaitu dengan menginput kode aktivasi dan saat melakukan transaksi yaitu menginput PIN terlebih dahulu. Namun jika dibandingkan dengan *mobile banking* milik BNI, tingkat keamanan transksi BSM Mobile lebih sederhana. Jika nasabah BSM hanya memiliki dua lapis keamanan, nasabah BNI yang akan mengaktivasi BNI Mobile Banking mempunyai lima lapis keamanan yaitu dengan cara menginput *user* ID, nomor kartu debit, M-PIN, *password* transaksi dan kode OTP.[3]

Dalam SOP BSM Mobile yang telah ditetapkan, nasabah dihimbau untuk selalu menjaga rahasia data-data pribadi yang menyangkut BSM Mobile agar tidak disalahgunakan oleh oknum yang tidak bertanggungjawab yang kemudian dapat terjadi penyimpangan, *fraud* atau kejahatan dan dapat mengakibatkan kerugian. Nasabah dihimbau untuk menjaga keamanan kode aktivasi dan PIN nasabah. Namun langkah ini lah yang sering membuat nasabah lalai sehingga *mobile banking* miliknya dibobol. Menjaga akun rahasia bank seperti kode aktivasi, PIN, nomer telefon, *user* ID dan *password* adalah suatu kewajiban bagi nasabah dan Bank. Tidak sedikit kasus pembobolan dana di

[3] bni.co.id/id-id/tarif/ebanking/bnimobilebanking, diakses 17 Mei 2017.

rekening terjadi akibat kelalaian dalam menjaga akun-akun rahasia tersebut.

Memang tidak bisa dikatakan bahwa seluruhnya adalah kesalahan dari nasabah. Meningkatkan lapisan keamanan BSM Mobile juga perlu. Semakin tebal dan rumit keamanannya maka akan semakin sulit untuk ditembus para *hacker.* Namun selalu waspada karena di zaman serba canggih ini segala teknologi dan informasi dapat dibobol dan diretas dengan mudah. Dalam hal ini dapat dikatakan bahwa antara Bank dan nasabah harus saling bersinergi agar keamanan Bank tetap terjaga dan nasabah harus lebih berhati-hati sehingga tidak terjadi hal yang tidak diinginkan.

Dari *Standard Operating Procedure* (SOP) BSM Mobile yang telah ditetapkan, sampai saat ini BSM Mobile belum pernah mengalami kesalahan atau *fraud* yang terjadi pada nasabahnya.[4] Namun harus diingat bahwa *mobile banking* adalah sebuah pengembangan teknologi yang dibuat oleh manusia maka tidak luput dari kesahalan-kesalahan yang dilakukan secara internal maupun eksternal. Kesalahan operasional *(human error),* penipuan *(fraud),* kejahatan melalui dunia maya *(cyber crime)* dan masih banyak lagi

[4] Hasil wawancara dengan Ibu Lissa (*Customer Service)* pada tanggal 5 April 2017 di Bank Syariah Mandiri KC Ungaran.

risiko yang mungkin terjadi dalam penggunaan *mobile banking*. Keamaan adalah salah satu faktor penyebab risiko-risiko tersebut terjadi. Maka dari itu, dalam penggunaannya, pihak Bank dan nasabah harus saling berhati-hati dalam memanfaatkan fasilitas BSM Mobile.

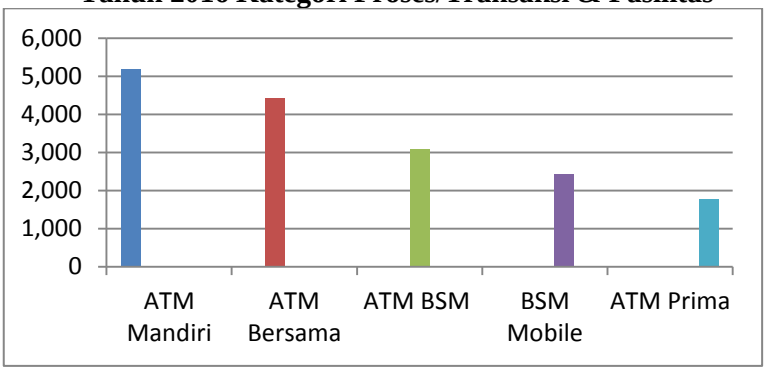
B. Risiko Mobile Banking

Kondisi layanan BSM Mobile tercatat belum pernah mengalami kesalahan atau *fraud* dari sejak diluncurkanyan pertama kali pada tahun 2007.[5] Nasabah hanya memberikan keluhan atau pengaduan atas ketidaknyamanan atau kesalahan pada layanan *mobile banking* yang dimilikinya. Berikut adalah grafik pengaduan nasabah Bank Syariah Mandiri :[6]

[5] Hasil wawancara dengan Ibu Lissa (*Customer Service)* pada tanggal 5 April 2017 di Bank Syariah Mandiri KC Ungaran.

[6] Laporan Tahunan Bank Syariah Mandiri Tahun 2016 dalam Dokumen Internal Bank Syariah Mandiri.

Gambar 5. Grafik Pengaduan Nasabah Tahun 2016 Kategori Proses/Transaksi & Fasilitas



Sumber : Dokumen Laporan Tahunan BSM Tahun 2016

Selama nasabah tidak menghilangkan atau memberikan kode aktivasi dan PIN ATM kepada orang lain, *mobile banking* miliknya akan tetap aman dan dana yang ada di ATM atau rekening tidak akan menghilang. *Mobile banking* milik BSM terhubung langsung dengan ATM. Sehingga ketika nasabah salah memasukkan nomor PIN dan membuat kartu ATM tertelan dan kemudian terblokir, seketika itu juga *mobile banking* miliknya akan terblokir. Sehingga ketika kartu ATM hilang atau terblokir, segera mendatangi cabang Bank untuk menonaktifkan BSM Mobile.[7]

[7] Hasil wawancara dengan Ibu Lissa (*Customer Service)* pada tanggal 5 April 2017 di Bank Syariah Mandiri KC Ungaran.

Layanan *mobile banking* memang diciptakan agar nasabah dapat lebih mudah melakukan transaksi perbankan. Tetapi nasabah tetap harus berhati-hati karena layanan perbankan ini rentan akan risiko. Disamping adanya kemungkinan risiko yang disebabkan oleh operasional Bank maupun kelalaian nasabah, adapun risiko yang sering dialami pada layanan *E-banking*, seperti halnya pada *mobile banking*, yaitu *cyber crime. Cyber crime* merupakan segala tindakan yang dilakukan secara langsung maupun tidak langsung melalui komputer dan jaringan komputer (internet) yang melanggar etika, hukum dan wewenang, terkait dengan pemrosesan data dan pengiriman data.[8]

Beberapa waktu lalu telah terjadi kasus pembobolan uang senilai Rp 420 juta dengan cara pemalsuan *sim card.* Eric, nasabah Bank Danamon pengguna aplikasi Danamon Mobile Banking (DMB) terus mendapatkan pesan singkat dan telepon, kemudian Eric memutuskan untuk menutup akun Kartu Hallo yang digunakannya. Namun tanpa disadari, telah terjadi transfer berturut-turut sebanyak sembilan kali dengan total senilai Rp 420 juta. Eric mengadu ke Bank Danamon, pihak Danamon mengatakan bahwa terdapat permintaan pengiriman kode aktivasi DMB dari nomor Kartu Hallo yang

[8]I Putu Agus Eka Pratama, *Komputer dan Masyarakat*, Bandung: Informatika, 2012, h. 334.

digunakan Eric. Eric kemudian mendatangi Grapari dan menanyakan kenapa Kartu Hallo yang digunakannya masih berfungsi. Pihak Grapari menjawab bahwa nomor Kartu Hallo yang digunakan Eric ternyata digandakan sebelum proses penonaktifan berakhir.[9]

Kelalaian yang menyebabkan raibnya uang nasabah Bank Danamon melalui *mobile banking* adalah dari operasional pihak Bank. Ketika ada permintaan kode aktivasi, seharusnya pihak Bank menanyakan identitas nasabah lebih rinci serta menanyakan data-data pribadi yang menyangkut data *mobile banking* milik nasabah dan hanya nasabah terkait yang mengetahui. Serta tidak asal memberikan kode aktivasi ketika nasabah meminta melalui telefon sekalipun nomor telefon tersebut adalah milik nasabah. Karena saat ini *sim card* bisa diduplikasi dan dipalsukan dengan mudahnya. Kasus Danamon ini dapat dijadikan evaluasi ulang bagi pihak Bank untuk lebih menekankan pada operasional akses permintaan data nasabah. Bank jangan mudah percaya dan kemudian memberikan akun bank nasabah kecuali nasabah tersebut datang langsung ke Bank dengan membawa data identitas pribadi nasabah. Karena sekarang ini segala bentuk teknologi

[9]Imam Wahyudiyanta, "Rp 420 Juta di Rekening Bank ini Raib Tanpa Nasabah Mengambilnya", htttp://m.detik.com/news/beita-jawa-timur/3292602/rp, diakses 14 Januari 2017.

dan informasi seperti *handphone* dan komputer dapat di*hack* oleh *hacker* dengan mudah.

Kasus lainnya yaitu nasabah PT. Bank Mandiri di Kota Malang yang kehilangan uang Rp 15 juta akibat transaksi *m-banking* miliknya dibobol orang. Raibnya uang belasan juta rupiah itu bermula dari telepon dari seseorang ke ponselnya. Penelepon mengaku dari sebuah Bank Nasional. Penelepon hanya memaparkan tentang fasilitas *m-banking* dan manfaatnya bagi pemakai. Beberapa menit usai menerima telepon, dia mendapatkan pemberitahuan melalui pesan singkat di ponselnya. Pesan itu berbunyi bahwa Ita telah mengirim uang Rp 15 juta ke sebuah rekening dengan nama seseorang melalui *m-banking*.[10]

Kasus yang kedua ini tidak bisa dikatakan sepenuhnya kesalahan dari nasabah. Karena nasabah bertindak benar yaitu tidak memberitahukan data-data *m-banking* (kode aktivasi dan PIN) miliknya. Canggihnya kemampuan teknologi dari pihak oknum lah yang dengan cepat membobol uang nasabah sekalipun hanya memiliki nomor telefon nasabah. Dan saat nasabah mengangkat telefon oknum, selama mereka mengobrol itulah oknum tersebut melangsungkan aksinya.

[10] Deny Rahmawan, "Ngaku Orang Bank, Ternyata Menipu Belasa Juta Rupiah", malangvoice.com/, diakses 14 Januari 2017.

Sebaiknya ketika si penelepon mengaku dari pihak Bank lalu menawarkan fasilitas-fasilitas Bank, nasabah jangan pecaya dan segera menutup telefon. Karen kebanyakan bank menawarkan produknya dengan cara *face-to-face* mendatangi calon nasabah secara langsung.

Cyber crime pada bank-bank di Indonesia beberapa tahun terakhir ini sering menjadi *headline* di berbagai berita perbankan. Memang, BSM belum mengalami kejahatan pada *mobile banking* yang dimilikinya. Tapi tidak akan yang diketahui sampai kapan produk tersebut akan selalu aman. Ada modus-modus kejahatan yang melekat pada *e-banking* seperti *mobile banking*, yaitu sebagai berikut :[11]

1. *Phising* merupakan jenis kejahatan komputer atau kejahatan di dunia internet, di mana pelaku memanfaatkan kemampuannya di bidang komputer dan jaringan komputer, untuk dikombinasikan dengan kelemahan di sisi manusia (mudah ditipu dan tidak teliti). *Phising* dilakukan untuk mendapatkan informasi rahasia nasabah seperti *user* ID, PIN dan data pribadi dengan beberapa cara antara lain:

[11] https://www.syariahmandiri.co.id./category/layanan-24-jam/keamananku/, diakses 21 April 2017.

a. *Typo Site* yaitu modus kejahatan yang dilakukan dengan membuat situs/aplikasi yang memiliki alamat dan tampilan yang hampir serupa dengan situs/aplikasi resmi milik bank. Selain itu, bisa dilakukan dengan mengunggah aplikasi *mobile banking* yang sama namun tidak resmi dengan di *Playstore* dan *App Store*. Agar tampak meyakinkan, pelaku juga seringkali memanfaatkan logo atau merk bank atau penerbit kartu kredit. Pemalsuan ini dilakukan untuk memancing korban menyerahkan data pribadi, seperti; *Password,* PIN dan nomor kartu kredit.

b. Mengirimkan *e-mail* atau SMS yang disusun dengan kata-kata yang meyakinkan, yang mengarahkan korban kepada URL link atau *login screen* atau meminta nasabah *login* dengan cara memasukkan *user* ID dan PIN.

c. *Keylogger* yaitu suatu aplikasi atau *software* yang dapat mengunci tombol *keyboard* dengan menggunakan program *logger* tertentu sehingga apapun yang diketikkan oleh user di layar telepon, dapat terekam. Artinya, meskipun saat mengetikkan *password* di kotak *password* yang tampil di layar telepon hanyalah '*****' misalnya, namun isi

> *password* tersebut dapat terekam dan otomatis dapat terbaca. Hasil rekaman ini akan langsung tersimpan pada komputer dan dikirim melalui internet kepada si pencuri data tersebut. Bisa lewat *e-mail,* irc atau bahkan bisa diamati langsung secara *realtime* melalui web.

Kasus *phising* yang pernah terjadi di Indonesia adalah pada tahun 2016 yaitu kasus pemalsuan aplikasi *mobile banking* milik BNI. Berdasarkan informasi yang beredar dari pesan singkat, Tekno Liputan6.com menemukan aplikasi palsu bernama BNI Internet Banking yang dibuat oleh pengembang *Internet Banking* LLC, bukan PT. Bank Negara Indonesia. Selain itu, aplikasi ini juga memiliki alamat *e-mail* pengembang yang berbeda dari dua aplikasi resmi BNI yaitu BNI Mobile Banking dan BNI SMS Banking. Pada dua aplikasi resmi tersebut, alamat *e-mail* yang dapat dihubungi adalah bnicall@bni.co.id, sementara aplikasi palsu memiliki alamat *e-mail* berbeda yaitu paketjahildotcom@gmail.com.[12]

Menanggapi kasus tersebut, *Corporate Secretary* BNI menjamin tidak ada keluhan dari pengguna aplikasi tersebut.

[12] Agustinus Mario Damar, "*Soal Aplikasi Mobile Banking Palsu, BNI Bakal Temui Kemkominfo",* htttp://m.liputan6.com/amp/2446676/soal-aplikasi-mobile-banking-palsu-bni-bakal-temui-kemkominfo, diakses 17 Mei 2017.

Namun yang menjadi kendala yaitu tidak mudah untuk menghapus aplikasi *mobile banking* palsu tersebut karena aplikasi tersebut ada di server Google dimana Google sebagai penanggungjawab *Play Store* bernaung di Amerika Serikat.[13]

2. *Malware Image*

   Malware (*Malicious Software)* merupakan *software* berbahaya yang dibuat untuk merusak, menghapus sistem, menyembunyikan bahkan mencuri data, yaitu dengan cara menyebarkan *Virus* (*Worm* dan *Trojan*) dan memasang program pengintai *(Spyware*) pada *smartphone* dan komputer. Virus tersebut akan merekam segala bentuk data yang ada di komputer maupun *handphone*

3. Penipuan lewat telepon yaitu dilakukan oleh pelaku kejahatan dengan menelpon dan mengabarkan nasabah mendapatkan hadiah atau keluarga mengalami musibah atau menawarkan suatu produk iklan. Selama mengobrol, si penelpon akan menggali informasi pribadi nasabah. Dan tanpa disadari dana nasabah akan terkirim secara otomatis setelah telefon itu berakhir.

[13] Agustinus Mario Damar, "*Soal Aplikasi Mobile Banking Palsu, BNI Bakal Temui Kemkominfo",* htttp://m.liputan6.com/amp/2446676/soal-aplikasi-mobile-banking-palsu-bni-bakal-temui-kemkominfo, diakses 17 Mei 2017.

4. Penipuan dengan menggunakan kartu kredit di internet, sekarang ini semakin banyak toko atau merchant yang menawarkan produk dan jasa melalui telepon ataupun internet, dengan kemudahan pembayaran menggunakan kartu kredit. Nasabah hanya diminta untuk menyebutkan nomor kartu kredit, masa berlaku (*expiry date)* dan 3 digit kode rahasia yang tertera pada bagian belakang kartu kredit nasabah, kemudian transaksi pun terlaksana.

Risiko dalam konteks perbankan menurut Adiwarman A. Karim (2004) merupakan suatu kejadian potensial, baik yang dapat diperkirakan *(anticipated)* maupun yang tidak dapat diperkirakan *(unanticipated)* yang berdampak negatif terhadap pendapatan dan permodalan bank.[14] Dalam usahanya mencari nafkah, seorang muslim dihadapkan pada kondisi ketidakpastian terhadap apa yang terjadi di kehidupan selanjutnya. Sama seperti usaha perbankan yang tidak akan luput dari suatu risiko. Hal ini telah Allah sampaikan kepada Nabi Muhammad saw, dalam surat Luqman ayat 34:

[14]Ari Kristin Prasetyoningrum, *Risiko Bank Syariah,* Yogyakarta: Pustaka Belajar, 2015, h. 38.

إِنَّ ٱللَّهَ عِندَهُۥ عِلۡمُ ٱلسَّاعَةِ وَيُنَزِّلُ ٱلۡغَيۡثَ وَيَعۡلَمُ مَا فِي ٱلۡأَرۡحَامِۖ وَمَا تَدۡرِي نَفۡسٞ مَّاذَا تَكۡسِبُ غَدٗاۖ وَمَا تَدۡرِي نَفۡسُۢ بِأَيِّ أَرۡضٖ تَمُوتُۚ إِنَّ ٱللَّهَ عَلِيمٌ خَبِيرٞ ٣٤

"Sesungguhnya Allah, hanya pada sisi-Nya sajalah pengetahuan tentang hari Kiamat; dan Dia-lah yang menurunkan hujan, dan mengetahui apa yang ada dalam rahim. Dan tidak seorang pun yang dapat mengetahui (dengan pasti) apa yang akan diusahakannya besok. Dan tidak seorang pun yang dapat mengetahui di bumi mana dia akan mati. Sesungguhnya Allah Mahamengetahui lagi Mahamengenal." (QS. 31:34)[15]

Ayat di atas menjelaskan tentang kita sebagai manusia tidak mengetahui apa yang akan terjadi besok. Entah itu suatu perkerjaan yang menghasilkan keuntungan atau kerugian. Sesuatu yang tidak pasti yang dapat menghasilkan kerugian disebut dengan risiko. Oleh karena itu, sebagai nasabah, sebelum memanfaatkan fasilitas layanan *mobile banking*, sebaiknya nasabah paham terlebih dahulu tentang mekanisme dan risiko yang kemungkinan terjadi.

Modus-modus kejahatan yang telah dijelaskan di atas adalah bagian dari risiko yang terjadi pada bank dan nasabah baik itu terjadi karena oknum internal maupun eksternal bank. Adapun risiko yang berkaitan secara langsung dengan bank

[15]M. Quraish Shihab, *Tafsir Al-Misbah*, Jakarta: Lentera Hati, 2012, h. 274.

akibat penyimpangan yang terjadi pada *mobile banking* adalah risiko likuiditas, risiko operasional, risiko hukum dan risiko reputasi, sebagai berikut :

1. Risiko likuiditas terjadi jika nasabah melakukan transaksi keuangan mencapai batas limit maksimal dengan menggunakan *mobile banking* yang mana pihak bank tidak mampu dalam memenuhi kewajibannya. Hal ini akan menyebabkan Bank mengalami illikuiditas.
2. Risiko operasional dapat disebabkan oleh faktor internal dan eksternal. Faktor internal yaitu berupa kesalahan operasional bank *(human errror)* dan Sistem Informasi Manaemen (SIM) Bank. Faktor eksternal dapat berupa persaingan antar bank dengan melalui pencurian data rahasia bank dan sabotase teknologi bank.
3. Risiko hukum dapat berupa akibat dari pengaduan nasabah terhadap pihak hukum yang berwajib atas ketidaknyamanannya dengan pihak Bank yang menjadikan Bank harus berurusan dengan hukum.
4. Risiko reputasi timbul antara lain karena adanya pemberitaan media dan/atau rumor negatif mengenai

Bank yang berdampak pada citra nama Bank di mata masyarakat.[16]

Dari 4 risiko yang telah dijelaskan diatas, risiko yang terjadi pada *mobile banking* lebih meangarah pada risiko operasional. Risiko operasional yang terjadi akibat kesalahan internal bank atau eksternal bank. Risiko operasional bisa meliputi kesalahan manusia *(human error)*, kesalahan teknologi, penipuan *(fraud)*, modus kejahatan dunia maya *(cyber crime)* dan kelalaian nasabah itu sendiri.

C. Manajemen Risiko Mobile Banking

Risiko bukanlah hal yang dapat dihilangkan namun dapat dihindari, dihadapi dan dikelola dengan baik sehingga dapat diminimalisir besaran kerugiannya. Bank Syariah Mandiri menerapkan manajemen risiko bank mengacu pada PBI No. 13/23/PBI/2011 dan POJK No. 65/POJK.03/2016 tentang Penerapan Manajemen Risiko bagi Bank Umum Syariah dan Unit Usaha Syariah.[17] Dari kedua peraturan mengenai penerapan manajemen risiko memiliki isi yang sama, hanya berbeda pada lembaga yang mengeluarkan yaitu dari Bank Indonesia dan Otoritas Jasa Keuangan. Selain itu,

---

[16] Bambang Rianto Rustam, *Manajemen Risiko Perbankan Syariah di Indonesia*, Jakarta: Salemba Empat, 2013, h. 243.

[17] Laporan Tahunan Bank Syariah Mandiri Tahun 2015 dan 2016 dalam Dokumen Internal Bank Syariah Mandiri.

Bank Syariah Mandiri meminimalisir risiko dengan memberikan tips-tips aman pada nasabah dalam penggunaan BSM Mobile yaitu diantaranya :[18]

1. Menjaga Informasi Rahasia Akun Bank

   Ada 2 faktor yang menyebabkan terbongkarnya rahasia akun bank yaitu faktor intern dan ekstern. Faktor intern yaitu faktor yang berasal dari dalam pihak Bank itu sendiri antara lain adanya sikap buruk dari para karyawan bank atau pejaba bank seperti rasa iri hati, cemburu dan dendam yang membuat para karyawan atau pejabat membongkar rahasia akun bank atau nasabah yang kemudian akan disalahgunakan. Sedangkan faktor ekstern adalah faktor yang berasal dari luar bank antara lain adanya persaingan usaha antar bank sehingga dapat terjadi suatu kerjasama antara pihak Bank dengan pihak luar untuk membongkar rahasia bank.[19]

   Adapun upaya yang dilakukan Bank untuk menjaga rahasia akun bank adalah bank tidak akan memberikan informasi apapun apabila ada orang yang menanyakan identitas nasabah atau aktivitasnya di bank kecuali pihak-

[18] https://www.syariahmandiri.co.id./category/layanan-24-jam/keamananku/, diakses 21 April 2017.

[19] Diana E. Rondonuwu, *Upaya Bank dalam Menjaga Rahasia Bank Sebagai Wujud Perlindungan Hukum terhadap Nasabah,* dalam Jurnal Sosial, Vo. II/No. 8/Sep-ov/2004, h. 9.

pihak yang telah diberi kuasa atau wewenang untuk meminta informasi tersebut sebagaimana yang telah ditentutkan dalam UU. No. 10 Tahun 1999 tentang Perbankan, yaitu kepada Kepolisian, Kejaksaan dan Pengadilan. Dan nasabah dihimbau agar lebih meningkatkan kewaspadaan dan ketelitian dalam menjaga keamaan informasi akun bank seperti kode aktivasi, nomor PIN, nomor rekening dan nomor telepon, bahkan kepada staff Bank yang bersangkutan, serta agar tidak memberikan informasi kepada siapapun termasuk pihak Bank.

2. Hindari Mengunduh *Software* Palsu

   Telah banyak tersebar *software* dengan nama dan logo yang sama dengan perbankan asli di *Playstore* dan *App Store*. Sehingga orang tidak dapat membedakan aplikasi tersebut asli atau palsu. Nasabah akan dituntun untuk mengisi data pribadi seperti kode aktivasi dan PIN. Kemudian data tersebut akan diolah dan disalahgunakan oleh oknum.

3. Waspadai *E-mail,* SMS dan Telepon Mencurigakan

   Waspadai upaya penipuan dari oknum yang mengatasnamakan petugas bank melalui telepon, sms atau *e-mail* yang meminta informasi pribadi atau mengharuskan untuk mentransfer sejumlah uang tanpa

alasan yang realistis. Cek dulu identitas pengirim. Terkadang ada sejumlah pihak yang menyamar sebagai instansi bank dan meminta nasabah mengunjungi suatu *link* atau *website* tertentu untuk memperbaharui informasi rekening nasabah. Bila terjadi hal seperi ini, sebaiknya lakukan konfirmasi terlebih dahulu pada bank yang bersangkutan. Segera tutup telepon dan lakukan pengecekan informasi yang diterima jika penelepon mengabarkan nasabah sebagai pemenang iklan tertentu. Modus lain jika penelepon mengabarkan keluarga mendapatkan musibah, jangan panik dan mengikuti perintah penelepon. Tanyakan identitas dan lakukan pengecekan.

4. Hubungi *Customer Service* Bank

   Ketika semua cara telah dilakukan namun ada kejanggalan pada akun rekening bank, maka telepon atau datangi *customer service* bank yang bersangkutan.

5. Konfirmasi Penerima Uang dan Rutin Mengecek Rekening

   Setelah melakukan transfer sebaiknya nasabah segera menghubungi si penerima uang dan mengkonfirmasi apakah uang telah diterima di rekening penerima. Selanjutnya secara berkala rutin mengecek rekening,

sehingga bila ada transaksi yang aneh dapat dilaporkan ke pihak bank secepatnya.

Manajemen Risiko adalah serangkaian metodologi dan prosedur yang digunakan untuk mengidentifikasi, mengukur, memantau, dan mengendalikan risiko yang timbul dari seluruh kegiatan usaha Bank.[20] Pengelolaan risiko adalah penting hukumnya sebagaimana firman Allah Swt. dalam surat Al-Hasyr ayat 18:

يَٰٓأَيُّهَا ٱلَّذِينَ ءَامَنُواْ ٱتَّقُواْ ٱللَّهَ وَلۡتَنظُرۡ نَفۡسٞ مَّا قَدَّمَتۡ لِغَدٖۖ وَٱتَّقُواْ ٱللَّهَۚ إِنَّ ٱللَّهَ خَبِيرُۢ بِمَا تَعۡمَلُونَ ١٨

"Hai orang-orang yang beriman, bertakwalah kepada Allah dan hendaklah setiap diri memerhatikan apa yang telah dikedepankannya untuk hari esok dan bertakwalah kepada Allah, sesungguhnya Allah menyangkut apa yang kamu kerjakan Maha Mengetahui."[21]

Dikisahkan pada masa Nabi Yusuf as. Suatu hari, Raja Fir'aun, Raja Negeri Mesir, dalam tidunya ia bermimpi melihat dirinya berdiri di tepi sungai Nil. Air sungai Nil turun tenggelam di depan matanya dan habis sehingga sungai itu menjadi tumpukan tanah yang kosong dari air. Kemudian ikan-ikan yang melompat-lompat bersembunyi di balik tanah sungai. Lalu keluarlah dari sungai itu tujuh sapi yang gemuk

[20] PBI No. 13/23/PBI/2011 tentang Penerapan Manajemen Risiko Bagi Bank Umum Syariah dan Unit Usaha Syarah

[21] Shihab, *Tafsir* ..., h. 552.

dan keluar juga tujuh sapi yang kurus. Sapi-sapi yang kurus menjadi binatang buas kemudian menyerang dan melahap sapi-sapi yang gemuk. Kemudian di atas tepi sungai Nil muncul tujuh bulir gandum dan tujuh bulir gandum itu tenggelam dalam tanah. Dan muncullah di tanah yang sama itu tujuh bulir gandum yang kecil.

Sampailah cerita mimpi itu kepada telinga Nabi Yusuf yang sedang di penjara. Kemudian Nabi Yusuf pun mampu menafsirkan mimpi sang raja. Ia menjelaskan bahwa Negeri Mesir akan mengalami masa-masa kesuburan selama tujuh tahun di mana saat itu tanaman-tanaman akan tumbuh segar, dan kemudian akan disusul tujuh tahun kelaparan. Nabi Yusuf memberikan nasihat yaitu hendaklah orang-orang Mesir tidak melampaui batas dalam memanfaatkan masa kesuburan karena akan disusul dengan tujuh tahun masa kelaparan. Pada masa kesuburan, apa saja yang disimpan oleh penduduk Mesir akan habis. Oleh karena itu, cara terbaik untuk mempersiapkan dalam menghadapi masa paceklik yang akan datang yaitu dengan menyimpan hasil tanaman dan merawat bulir-bulir gandum agar tidak rusak atau terkena hama. Atas kehendak Raja Fir'aun mengutus untuk mengumpulkan bahan makanan dalam tahun-tahun baik yang akan datang, menimbun gandum di kota-kota sebagai bahan makanan, serta

menyimpannya. Sehingga segala bahan makanan itu menjadi persediaan Negeri Mesir untuk menghadapi tujuh tahun masa paceklik dan kelaparan supaya Negeri Mesir tidak binasa karena kelaparan tersebut.

Jadi, pengelolaan manajemen risiko telah ada sejak zaman Nabi Yusuf as. Pengelolaan yang dilakukan oleh Nabi Yusuf adalah suatu usaha yang dilakukan untuk mengantisipasi dan menjadi solusi atas terjadinya suatu bencana yang akan berdampak pada negerinya. Terlihat dari cara Nabi Yusuf mempersiapkan segala cara untuk menghadapi masa kelaparan yang akan datang, yaitu dengan menimbun bahan makanan, menghimbau untuk tidak berlebihan dalam pemanfaatan dan lain-lain.

Seperti yang dijelaskan sebelumnya bahwa *mobile banking* memiliki 4 risiko yang melekat yaitu risiko likuiditas, risiko operasional, risiko hukum dan risiko reputasi. Berikut adalah metode yang dilakukan Bank untuk mengelola 4 risiko tersebut:

1. Risiko Likuiditas
    a. Mengukur nilai tingkat keseimbangan dana pihak ketiga bank (giro, tabungan dan deposito) dan mengukur ketersediaan kemampuan dalam memenuhi kewajiban (likuiditas) dengan cara pemeliharaan arus kas dan rasio

kecukupan likuiditas, serta penggunaan alat analisis likuiditas untuk menilai dan mengukur keadaan likuiditas (*liquidity gap*);

b. Memelihara akses ke pasar uang antar bank syariah dengan cara memperoleh dan memberikan batas kredit (limit) dari dan untuk bank lain;

c. Memantau objek yang rentan terhadap risiko likuiditas (eksposur) dan standar yang mengatur likuiditas secara rutin.[22]

2. Risiko Operasional

a. Dalam mengelola risiko operasional, Bank menggunakan suatu aplikasi yang disebut dengan *Operational Management Information Sytem* (ORMIS). Dengan menggunakan aplikasi ini, bank dapat mengidentifikasi, memantau dan memitigasi kejadian kerugian akibat terjadinya risiko operasional yang dialami oleh Bank. ORMIS berfungsi sebagai penanda peringatan lebih dini tentang potensi kejadian suatu risiko.

b. Bank menerapkan manajemen risiko pada teknologi informasi melalui menetapkan standard pada perangkat jaringan komunikasi data dan *software*, mengelola

[22] Laporan Tahunan Bank Syariah Mandiri Tahun 2016 dalam Dokumen Internal Bank Syariah Mandiri.

kewenangan akses pada sistem, mengembangkan layanan perbankan elektronik dari segi keamanan dan rencana memulihkan bencana akibat risiko.

c. Bank mengkaji setiap risiko yang akan ditimbulkan oleh setiap produk dan atau aktivitas baru yang akan diluncurkan oleh Bank.

3. Risiko Hukum
   a. Menggunakan jasa pengacara handal dalam membantu penanganan kasus-kasus hukum yang mengandung tuntutan ganti rugi.
   b. Pencadangan aset terkait dengan potensi kerugian bank akibat tuntutan hukum.[23]
4. Risiko Reputasi
   a. Meningkatkan pelayanan penyelesaian nasabah sesuai *service level agreement* (SLA) yang berlaku.
   b. Implementasi *command center* untuk pengelolaan publikasi yang terkait dengan pelaporan kasus yang terjadi di BSM.
   c. Melaksanakan media *visit* dan media *briefing.*[24]

Dari pengelolaan-pengelolaan risiko yang dilakukan oleh Bank Syariah Mandiri, pengelolaan risiko operasional

[23] Laporan Tahunan Bank Syariah Mandiri Tahun 2016 dalam Dokumen Internal Bank Syariah Mandiri.

[24] Laporan Tahunan Bank Syariah Mandiri Tahun 2016 dalam Dokumen Internal Bank Syariah Mandiri.

adalah pengelolaan yang lebih mengarah pada pengendalian risiko *mobile banking* sehingga dapat meminimalisir adanya potensi kerugian baik dikarenakan faktor internal maupun eksternal Bank.

Dalam rangka pengelolaan risiko, Bank memiliki organisasi manajemen risiko meliputi :

1. Komite Pemantau Risiko

   Membantu Dewan Komisaris melakukan pengawasan secara aktif penerapan manajemen risiko.
2. Komite Manajemen Risiko

   Memberikan rekomendasi yang berisikan langkah-langkah antisipatif maupun pengendalian terhadap risiko yang berpotensi merugikan.
3. Direktur Manajemen Risiko

   Menyampaikan laporan evaluasi risiko kepada Dewan Komisaris, serta meningkatkan kesadaran risiko dan keterampilan dalam pengelolaan risiko.
4. Satuan Kerja Manajemen Risiko

   Unit kerja yang independen terhadap unit bisnis dan unit audit internal.[25]

[25] Laporan Tahunan Bank Syariah Mandiri Tahun 2016 dalam Dokumen Internal Bank Syariah Mandiri.

Demikian keempat unit tersebut saling bersinergi dalam penerapan manajemen risiko sebagai *first line*, *second line* dan *third line of defense*. Bank mengelola risiko melalui permodalan maupun aktivitas operasional.

1.