Bulletin of Monetary Economics and Banking

Volume 5 | Number 1 Article 3

6-30-2002

INTERNET BANKING DI INDONESIA

Tim Penelitian Pengaturan Perbankan Bank Indonesia

Follow this and additional works at: https://bulletin.bmeb-bi.org/bmeb

Recommended Citation
Bank Indonesia, Tim Penelitian Pengaturan Perbankan (2002) "INTERNET BANKING DI INDONESIA," *Bulletin of Monetary Economics and Banking*: Vol. 5: No. 1, Article 3.
DOI: https://doi.org/10.21098/bemp.v5i1.304
Available at: https://bulletin.bmeb-bi.org/bmeb/vol5/iss1/3

This Article is brought to you for free and open access by Bulletin of Monetary Economics and Banking. It has been accepted for inclusion in Bulletin of Monetary Economics and Banking by an authorized editor of Bulletin of Monetary Economics and Banking. For more information, please contact bmebjournal@gmail.com.

INTERNET BANKING DI INDONESIA

Oleh : Direktorat Penelitan dan Pengaturan Perbankan Bank Indonesia

Abstraksi

Perkembangan pelayanan jasa-jasa perbankan yang dilakukan melalui internet semakin marak seiring dengan pertumbuhan teknologi informasi yang semakin cepat. Faktor inovasi produk dan perkembangan teknologi sudah merupakan bagian yang tak terpisahkan dengan perkembangan industri perbankan untuk meningkatkan kualitas pelayanan sehingga menjadi lebih cepat, bagus dan efisien

Namun demikian, masalah keamanan bertransaksi serta perlindungan nasabah menjadi perhatian tersendiri untuk pengembangan intenet banking ke depan, terutama karena tidak adanya kepastian hukum bagi nasabah dimana belum terdapat suatu bentuk pengaturan atas kegiatan internet di Indonesia. Masalah keamanan tidak hanya untuk kepentingan nasabah tetapi juga untuk kepentingan bank penyelenggara internet banking itu sendiri maupun industri perbankan secara keseluruhan.

Bank Indonesia sebagai otoritas pengawas bank sangat berkepentingan untuk menjaga agar bank-bank pelaksana internet banking senantiasa menerapkan prinsip-prinsip kehati-hatian dalam perbankan (prudential banking operation), manajemen risiko dan perlindungan terhadap nasabah (customer protection) dalam penyelenggaran jasa perbankan melalui internet mengingat ketergantungan terhadap teknologi dan pihak ketiga sangat tinggi

Kajian mengenai internet banking ini nantinya akan menjadi bahan penyusunan pedoman serta dasar pemikiran dalam pembuatan ketentuan atau peraturan mengenai internet banking di Indonesia.

Key Words : *Website, Prudential Banking Operation, Risk Management , Customer Protection*

Pendahuluan

Perkembangan teknologi informasi telah mengubah strategi bisnis dunia usaha termasuk perbankan dengan menempatkan teknologi informasi sebagai unsur utama dalam proses produksi atau pemberian jasa. Selain itu perkembangan teknologi informasi juga telah mendorong inovasi di bidang jasa pelayanan termasuk jasa pelayanan perbankan. *Electronic transaction* dalam bentuk *internet banking* merupakan salah satu bentuk baru pengembangan *delivery channel* pelayanan bank yang telah mengubah strategi bisnis perbankan yang semula lebih banyak mengandalkan pada teknologi manusia menjadi teknologi informasi.

Pelayanan bank dalam bentuk *internet banking* sepertinya telah menjadi keharusan. Kebutuhan dunia usaha dan nasabah bank semakin meningkat seiring dengan kemajuan teknologi maupun informasi. Untuk itu *internet banking* dapat menjembatani kebutuhan dunia usaha maupun nasabah dalam hal mempercepat pelayanan jasa bank.

Sejalan dengan perkembangan *information technology* di atas, peranan *electronic banking* semakin berarti. *Authomatic Teller Machine* (ATM), *credit card* dan *phone banking* seperti menjadi keharusan bagi setiap bank di Indonesia dalam merebut pangsa pasar. Inovasi perbankan berbasis teknologi terus berkembang sesuai dengan keinginan nasabah. Saat ini *internet banking* sedang menjadi perhatian dimana nasabah dapat melakukan transaksi perbankan (*non cash*) setiap saat dari manapun dengan begitu mudah dan nyaman hanya dengan mengakses melalui komputer (jaringan *internet*). Teknologi internet mampu menghilangkan batas ruang dan waktu, bersifat global/internasional bahkan tanpa batas negara. Bagi bank sendiri, pelayanan melalui *internet banking* dapat menekan biaya operasional karena dapat menghemat kertas, tenaga manusia, dan tidak perlu investasi ATM atau kantor cabang.

Di Indonesia praktek *internet banking* dipelopori oleh salah satu bank swasta nasional pada medio 1999. Sekarang ini ada sekitar 7 bank yang telah menyelenggarakan *internet banking* yaitu Bank Lippo, BCA, Bank Bali, BII, Bank Universal, Bank Niaga dan Citibank. *Internet banking* ke 7 bank tersebut sudah pada tahapan transaksional, bukan lagi informasional (atau sekedar *website*) sebagaimana dimiliki oleh hampir seluruh bank. Di masa mendatang, sejalan dengan semakin banyaknya pengguna *internet* dan semakin ketatnya persaingan antar bank, diperkirakan akan semakin banyak bank yang akan menyelenggarakan jasa pelayanan *internet banking* di Indonesia.

Namun demikian, kecanggihan apapun teknologi informasi dan komputer, dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggungjawab untuk mencari keuntungan pribadi (*hacker/cracker*). Sama halnya dengan *internet banking*, terdapat risiko finansial baik bagi bank maupun nasabah karena *hacker/cracker* mampu menembus *firewall* dari *internet banking* suatu bank. Munculnya kasus *domain/website* palsu atau mirip dengan milik BCA

https://bulletin.bmeb-bi.org/bmeb/vol5/iss1/3
DOI: 10.21098/bemp.v5i1.304

yang terjadi pada medio Juni 2001 merupakan bukti bahwa sistem pengamanan *internet banking* perlu mendapat perhatian semua pihak, khususnya Bank Indonesia sebagai otoritas pengawas bank.

Berkaitan dengan hal tersebut di atas, Bank Indonesia mempunyai tanggung jawab moril untuk memberikan perlindungan kepada nasabah. Untuk itu, Bank Indonesia harus melihat apakah penyelenggaran *internet banking* oleh suatu bank telah memperhatikan prinsip-prinsip prudensial, dan telah mempersiapkan segala sesuatunya dengan *risk management system* dan *contingency plan* yang baik dan memadai.

Dari aspek ketentuan, Bank Indonesia telah mengeluarkan Surat Keputusan Direksi No. 27/164/KEP/DIR dan Surat Edaran No. 27/9/UPPB masing-masing tentang Penggunaan Teknologi Sistem Informasi oleh Bank tanggal 31 Maret 1995. Ketentuan tersebut mengatur mengenai prosedur aplikasi teknologi oleh industri perbankan, namun tidak secara spesifik mengatur aspek operasional dari penerapan *internet banking*. Oleh karena itu, perlu dikembangkan pengaturan yang lebih konkrit mengenai jasa pelayanan bank melalui internet.

Konsep Internet Banking

Definisi oleh Cronin dalam bukunya *Banking and Finance on the Internet* yang dipublikasi oleh John Wilery & Sons – Canada tahun 1998 adalah:

The financial services application that enables financial institutions to offer traditional banking products and services such as checking, savings and money market accounts and certificates of deposit over the internet

Bank Negara Malaysia yang telah menyusun ketentuan mengenai *internet banking* mendefinisikannya sebagai berikut:

Internet banking refers to banking products and services offered by banking institutions on the internet through access devices including personal computers, and other intelligent devices

Dalam bahasa Indonesia, terjemahan bebas dari *internet banking* adalah jasa yang memungkinkan nasabah bank melakukan transaksi perbankan melalui jaringan internet. *Internet banking* lebih fleksibel dibandingkan dengan pelayanan dengan sistem counter, karena tidak mengenal batas waktu dan tempat.

Terdapat 3 tingkatan *internet banking*:

1. *Entry/informational*

Merupakan tingkatan atau tahapan yang paling sederhana, yaitu hanya menyediakan

informasi statistik mengenai bank tersebut serta jasa/produk yang ditawarkan. Tingkatan ini tidak lebih dari sekedar brosur elektronik dari suatu bank. Tingkat risikonya sangat rendah karena tidak terhubung dengan *data base* bank.

2. *Intermediate/communicative*

   Pelayanannya lebih luas daripada sekedar informasi, karena nasabah bisa melakukan interaksi dengan bank penyedia jasa internet secara terbatas, misalnya *account inquiry*, *on line account application, electronic mail*, dan sebagainya. Dalam tahapan ini tidak ada *execution of transaction* sama sekali. Tingkatan ini memiliki risiko yang lebih besar *informational website.*

3. *Advance/transaction*

   Tingkatan ini adalah yang paling lengkap dan dapat menampilkan seluruh transaksi yang diperlukan oleh nasabah termasuk transfer dana, pembayaran tagihan dan lain-lain seperti layaknya pelayanan melalui *counter* atau ATM kecuali penarikan kas.

   Pada dasarnya bank yang menyediakan jasa pelayanan *internet banking* dapat bebas menentukan transaksi atau produk/jasa apa yang disediakan. Untuk itu bank dalam *business plan*-nya harus memperhitungkan dengan seksama untung ruginya, risiko yang akan dihadapi serta kebutuhan dari nasabah. Penentuan jenis produk/jasa tentunya akan disesuaikan dengan kemampuan dan strategi masing-masing bank namun demikian Bank tidak diperkenankan untuk menawarkan produk/jasa di *internet banking* yang dilarang oleh undang-undang atau peraturan yang berlaku.

Secara umum terdapat beberapa jenis produk/jasa yang ditawarkan melalui *internet banking* :

1. Informasi saldo
2. Pembukaan rekening
3. Transfer
   Transfer dengan menggunakan jasa *internet banking* adalah cara yang paling efisien dan murah karena nasabah dapat melakukannya dimana saja dan tidak dibatasi oleh waktu.
4. Paymet Gateway
   Merupakan fasilitas pembayaran jasa tertentu (antara lain pembayaran telepon, air PAM dan listrik) yang disediakan oleh bank sehingga nasabah dapat melakukan pembayaran langsung melalui *internet*. Konsep *payment gateway* ini mirip dengan transfer karena nasabah maupun penyedia jasa (perusahaan telepon atau listrik) harus sama-sama memiliki *account* di bank tersebut. Dengan demikian selain nasabah bank tersebut, orang lain tetap saja tidak bisa melakukan transaksi *payment gateway*. Bahkan saat ini telah berkembang layanan *account aggregation* yaitu jasa bank yang menyatukan informasi

https://bulletin.bmeb-bi.org/bmeb/vol5/iss1/3
DOI: 10.21098/bemp.v5i1.304

dari berbagai *website* dan menampilkan informasi tersebut dalam format terkonsolidasi kepada nasabah. Informasi dapat berkisar dari informasi untuk konsumsi publik hingga informasi rekening pribadi nasabah. *Account aggregation* banyak digunakan untuk layanan *bill presentment and payment*, dimana nasabah mendelegasikan kepada bank atau pihak ketiga untuk mendebet rekening milik nasabah untuk melakukan pembayaran sejumlah tagihan milik nasabah, misalnya tagihan listrik, telepon,dll. Untuk itu nasabah perlu menyerahkan *Personal Identification Number* serta *Password* milikinya kepada bank atau pihak ketiga.

5. Kliring
6. *Trade Services & Finance*
7. Penutupan rekening
8. Transaksi lainnya

Bank penyedia *internet banking* dapat juga menyediakan pelayanan jasa bagi korporasi seperti *cash management service, continuous link settlement*, pemesanan buku cek bahkan nasabah dapat memperoleh informasi, berita, analisis seputar *foreign exchange transaction* serta juga dapat melakukan *transaksi spot, swap, forward*,dll melalui *internet banking*. Selain itu bank dapat memberikan pelayanan lainnya di luar produk perbankan seperti misalnya nasabah dapat membeli *voucher* isi ulang telepon genggam dengan langsung mendebet rekening nasabah yang bersangkutan, pembelian saham secara *on line*, pembayaran polis asuransi dan sebagainya.

Lembaga keuangan yang menyelenggarakan *internet banking* adalah:

1. Bank

Pada prinsipnya semua bank umum yang beroperasi di Indonesia bisa menyelenggarakan jasa *internet banking*. Untuk BPR, saat ini belum memungkinkan memberikan jasa pelayanan *internet banking* mengingat ruang lingkup usahanya terbatas dan jangkauan wilayah usahanya yang tidak begitu luas.

2. Bank khusus penyelenggara *internet banking* (*internet only banks*/IOB)

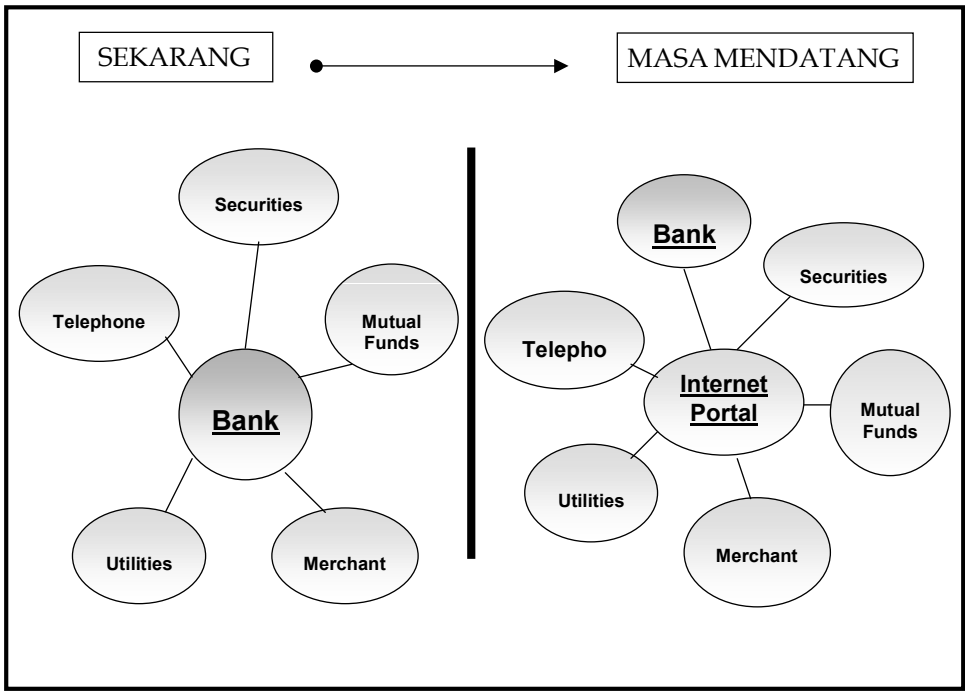
Jenis usaha seperti ini belum ada di Indonesia dan sebaiknya untuk saat ini dilarang sampai kita mengetahui seberapa besar perkembangan kegiatan usaha tersebut serta dampak risikonya terhadap nasabah dan perbankan secara keseluruhan.

Perkembangan *Internet Banking*

Perkembangan teknologi *internet* diperkiraan akan mengubah wajah sistem keuangan yang awalnya menempatkan bank sebagai mediator transaksi perdagangan antara para

pelaku bisnis *(business to business)* maupun dengan konsumen perorangan *(business to consumer)*. Seiring dengan globalisasi pemanfaatan teknologi *internet* di masa mendatang yang memberikan banyak manfaat dan kemudahan, *internet portal* akan berperan sebagai *gateway* bagi setiap interaksi bisnis. Fenomena ini menuntut masing-masing pihak, baik pelaku bisnis, konsumen individu, maupun bank membangun kapasitas jaringan *on-line*

Gambar 1. Peran Internet dalam Perkembangan Perbankan



Sumber : American Bankers Association

Teknologi *internet* juga dipandang sebagai sarana yang efisien dalam mendisain, memasarkan serta menjadi saluran distribusi produk dan jasa keuangan dengan biaya yang relatif murah. Efisiensi biaya tersebut menjadi salah satu daya tarik penerapan *internet banking*, sehingga konsekuensinya perbankan akan memiliki kesamaan dalam komoditas pelayanan yang ditawarkan yang berupa kemudahan-kemudahan *(conveniences)* karena memiliki kesamaan dalam jangkauan geografis, jam beroperasi, dan jenis pelayanan.

Perkembangan Internet Banking Di Beberapa Negara Asia

Internet banking pertama kali diperkenalkan oleh bank-bank di Amerika pada tahun 1995, yang selanjutnya melalui proses globalisasi telah berkembang sampai di Asia, termasuk

https://bulletin.bmeb-bi.org/bmeb/vol5/iss1/3
DOI: 10.21098/bemp.v5i1.304

Indonesia. Perkembangan penyediaan layanan *internet banking* di Asia dipelopori oleh Hong Kong dan Singapura, yang ditandai dengan semakin bertambahnya jumlah bank yang menawarkan *internet banking* dari waktu ke waktu. Mengantisipasi perkembangan yang pesat, otoritas perbankan di kedua negara tersebut telah mengeluarkan *policy statement* yang mengatur mengenai *internet banking*. Sementara itu, perkembangan *internet banking* di negara-negara asia lainnya seperti Malaysia, India, Vietnam, dan Filipina diyakini akan mengikuti jejak Hongkong dan Singapura, mengingat teknologi informasi merupakan terobosan penting yang bermanfaat sebagai perangkat strategis untuk meningkatkan produktivitas dan kualitas pelayanan nasabah yang pada gilirannya dapat meningkatkan pangsa pasar.

Pembahasan berikut akan melihat perkembangan internet banking di beberapa negara serta membandingkan dengan perkembangan di Indonesia. Dalam uraian tersebut akan diperoleh gambaran sejauhmana kemajuan dan permasalahan yang ada di Indonesia.

Prospek Dan Tantangan Internet Banking

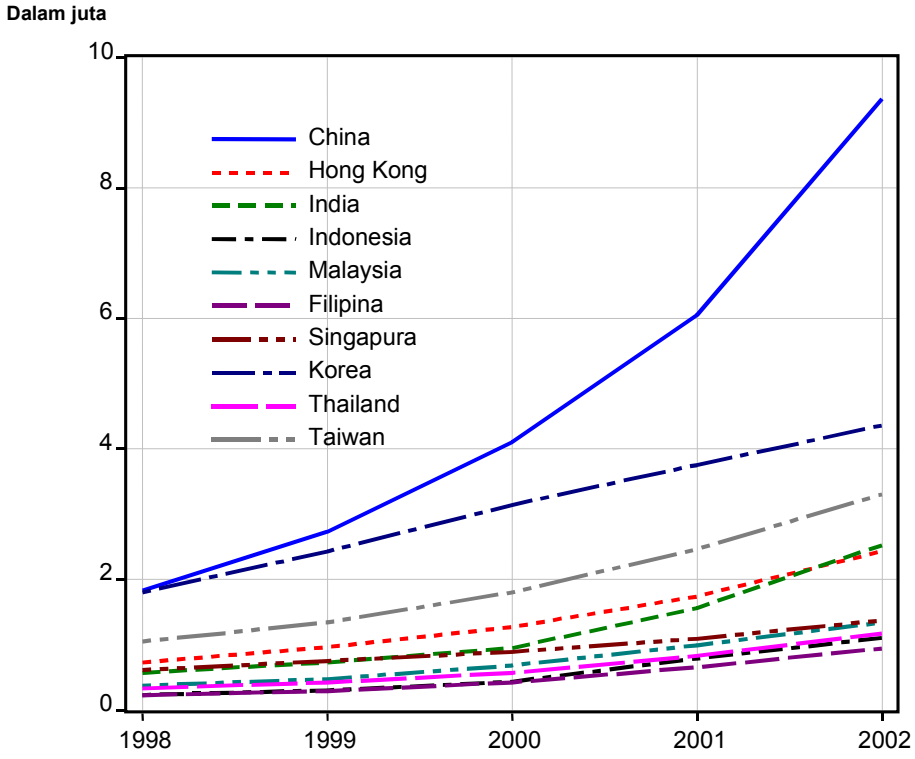
Untuk melihat sejauhmana prospek pelayanan perbankan lewat *internet* di Indonesia, maka dalam uraian dibawah ini akan memuat mengenai perkembangan *internet banking* di Asia. Survey tahunan yang dilakukan oleh World Economic Forum dan Pricewaterhouse Coopers terhadap CEO di negara-negara Asia menunjukkan bahwa lebih dari separuh responden yakin dalam dua tahun mendatang industri keuangan akan sangat dipengaruhi oleh *internet*[1]. Hal ini didukung oleh survey yang dilakukan oleh International Data Corporation yang menggambarkan pesatnya perkembangan penggunaan *Internet*, khususnya di negara-negara Asia. Berdasarkan survey tersebut, China, Hong Kong dan Malaysia merupakan negara-negara yang diperkirakan akan mengalami tingkat pertumbuhan tertinggi diantara negara asia lainnya dalam dua tahun mendatang.

Survey tersebut juga memberikan gambaran mengenai rasio pengguna *internet* terhadap total populasi pada akhir tahun 2000 untuk beberapa negara Asia. negara Singapura, Hongkong dan Taiwan menduduki rasio tertinggi. Hal ini berkaitan erat dengan majunya tingkat perekonomian dan luasnya penggunaan teknologi informasi oleh masyarakat di negara tersebit. Khusus untuk Indonesia, diperkirakan rasio akan mencapai angka 0,2%, yang berarti sekitar 430.000 orang dari seluruh total penduduk Indonesia akan menggunakan *internet*. Dengan demikian, perkembangan *internet banking* di Indonesia diproyeksikan akan tumbuh pesat sebagai konsekuensi perkembangan teknologi, besarnya populasi dan perkembangan *internet banking* di negara-negara sekitarnya.

Penerapan *internet banking* sebagai *delivery channel* secara perlahan akan membawa

1 Tan Khee Giap, PhD, The Impact of Information Technology on Banking Industry, hal. 6-7

Gambar 2. Proyeksi Penggunaan Internet di Asia



Sumber : International Data Corporation

perubahan dalam struktur industri perbankan nasional di masa mendatang. Hal ini dikaitkan dengan perubahan iklim persaingan antar bank dimana aplikasi *internet banking* menghilangkan batasan/hambatan demografis yang pada akhirnya berpotensi mengeliminasi *competitive advantage* yang dimiliki melalui jaringan kantor cabang *(branch network)*. Penggunaan *internet* memungkinkan bank menjangkau serta memelihara hubungan dengan para nasabahya, sehingga dapat menggantikan fungsi operasional sebuah kantor cabang. Hal ini mendorong dunia perbakan untuk cenderung melakukan *streamlining* melalui pendirian *virtual branch* yang tidak membutuhkan investasi dalam jumlah yang besar.

Dari sisi bank, *internet banking* dapat menghemat biaya pelayanan (*overhead cost*) cukup signifikan. Hasil survei *American Banking Association* tahun 1997 menunjukkan bahwa biaya transaksi melalui *internet banking* jauh lebih murah dibandingkan melalui *delivery channels* lainnya.

https://bulletin.bmeb-bi.org/bmeb/vol5/iss1/3
DOI: 10.21098/bemp.v5i1.304

On line/internet banking	*: USD 0.01*
ATM	*: USD 0.27*
Telephone	*: USD 0.54*
Branch	*: USD 1.07*

Perkembangan Internet Banking Di Indonesia

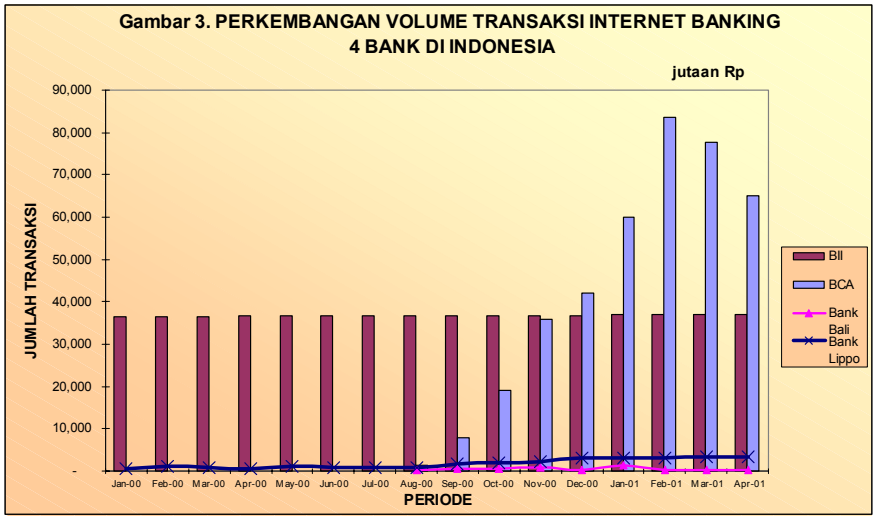
Belum pesatnya perkembangan *internet banking* di Indonesia terutama adanya kendala-kendala sebagai berikut: (i) persiapan dan investasi yang matang dan mahal dengan dukungan teknologi yang canggih, (ii) kepercayaan publik atas sistem pengamanan *internet banking*, (iii) promosi *internet banking* yang belum merata ke seluruh lapisan masyarakat, dan (iv) pasar yang terbatas hanya pada masyarakat pengguna *internet* yang umumnya adalah lapisan menengah ke atas dan berpendidikan.

Selain penghematan biaya, terdapat beberapa manfaat yang diharapkan oleh bank dalam penerapan *internet banking*, antara lain:

1. Menambah jumlah nasabah, mengingat dewasa ini semakin banyak masyarakat menggunakan internet. Disamping itu, nasabah pada level tersebut biasanya mempunyai kemampuan finansial yang cukup besar.
2. Tuntutan pasar yang menghendaki pelayanan bank yang berorientasi *paperless, timeless,* dan *borderless*.
3. *Contagion willingness*, karena pengaruh bank-bank lain pada *peer* yang sama telah menyelenggarakan *internet banking*.
4. Membangun *image* dan peningkatan level persaingan, khususnya bagi bank-bank yang belum banyak dikenal masyarakat.
5. Memperluas jaringan pelayanan, yang atas dasar analisis ekonomis dan geografis lebih menguntungkan dan mudah untuk menerapkan *internet banking* dibandingkan dengan membuka kantor cabang.
6. *Information collection*, terutama informasi mengenai keinginan pasar perbankan. Lebih cepat dan *up to date* diserap melalui *internet banking*.
7. Instalasi *internet banking* semakin hari akan semakin murah karena persaingan perusahaan di antara penyedia jasa *internet*.
8. Belum adanya ketentuan prudensial yang mengatur *internet banking* secara khusus, misalnya tentang perizinan dan persyaratan sehinga bank merasa bebas menyelenggarakan *internet banking*

Sebagaimana dikemukakan di atas, di Indonesia telah terdapat 7 bank yang telah menyelenggarakan *internet banking* pada tahapan *advance/transactional website* yaitu Bank Lippo, Bank Central Asia, Bank Bali, Bank Internasional Indonesia, Bank Universal, Bank Niaga dan Citibank. Sedangkan pada tahapan *informational* dan *communication*, terdapat sekitar 40 bank yang memiliki *website*. Selanjutnya Bank Mega, HSBC dan Standard Chartered Bank pun akan segera menyelenggarakan jasa *internet banking* tersebut. Layanan *internet banking* BII, BCA, Bank Bali dan Bank Lippo telah dinikmati oleh 154.375 nasabahnya. Adapun perkembangan jumlah volume transaksi empat bank yang telah menyelenggarakan layanan *internet banking* hingga bulan April 2001 dapat dilihat pada gambar 3.

Gambar 3. PERKEMBANGAN VOLUME TRANSAKSI INTERNET BANKING 4 BANK DI INDONESIA

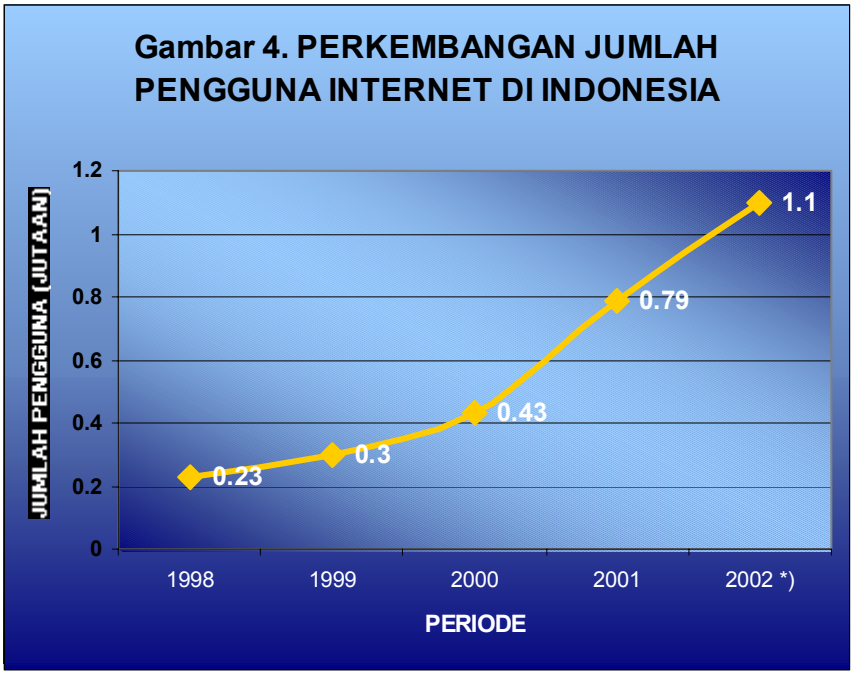


Tabel 1.
Jumlah Nasabah *Internet Banking* Empat Bank di Indonesia Hingga Bulan April 2001

No.	Nama Bank	Jumlah Nasabah Per April 2001
1	**BII**	40,838
2	**BCA**	99,504
3	**Bank Bali**	4,188
4	**Bank Lippo**	9,845
	TOTAL	**154,375**

https://bulletin.bmeb-bi.org/bmeb/vol5/iss1/3
DOI: 10.21098/bemp.v5i1.304

Adapun perkembangan jumlah masyarakat di Indonesia yang telah mempergunakan internet dapat dilihat pada gambar 4.



*) Proyeksi
Hasil penelitian oleh World Economic Forum dan Price Waterhouse Coopers th 1999
Responden Asian CEO

Resiko Spesifik Untuk Internet Banking

Selain risiko-risiko tersebut di atas, *internet banking* memiliki kekhususan tersendiri sehingga ada beberapa risiko yang sifatnya sangat spesifik untuk *internet banking,* diantaranya adalah :

1. *Technology risk*

   Risiko teknologi yang berhubungan dengan kehandalan dan sistem keamanan. Kecanggihan *software* dan *hardware* sangat menentukan besar kecilnya risiko teknologi yang dihadapi oleh bank penyelenggara jasa *internet banking*.

2. *Reputational risk*

Reputational risk berkaitan erat dengan *corporate image* dari bank itu sendiri. Nama baik bank

penyelenggara *internet banking* menjadi jaminan utama (*creditworthiness*) dalam pelayanan jasa *internet banking*. Kegagalan atau tidak befungsinya sistem, teknologi maupun aplikasi yang dipakai dalam *internet banking* dapat membuat nasabah menjadi *reluctant* atau enggan untuk melakukan transaksi perbankan melalui *internet*.

3. *Outsourcing risk*

   Dalam prakteknya hampir semua bank yang menyelenggarakan pelayanan transaksi melalui *internet* menggunakan jasa pihak ketiga sebagai *internet service provider* (ISP) ataupun sebagai data operator dalam pengoperasian dan pemeliharaan data. Di satu sisi bank dapat menghemat biaya yang cukup signifikan dengan melakukan *outsourcing* tetapi di sisi lain ada risiko yang mungkin timbul dengan adanya *outsourcing* tersebut antara lain ditutupnya ISP tersebut secara tiba-tiba karena kesulitan keuangan, kurang terjaminnya kerahasiaan data karena ISP tersebut karena mudah dibobol oleh *hacker,* kurangnya kapabilitas ISP, dll.

4. *Legal risk*

   Masalah hukum dalam *internet banking* dalam beberapa hal masih banyak yang belum jelas dan belum diatur secara eksplisit. Hal ini dapat menimbulkan potensi masalah yang besar di bidang hukum perdata atau pidana apabila di kemudian hari terjadi sengketa atau perselisihan yang menyangkut transaksi-transaksi perbankan yang dilakukan melalui *internet*. Selain itu *cross border issues* dalam transaksi *internet banking* sedikit banyak juga berkaitan dengan aspek hukum yang belum jelas.

5. *Transaction Risk*

   Risiko transaksi merupakan risiko saat ini dan di masa mendatang sebagai akibat dari kecurangan, kesalahan, dan ketidakmampuan menyalurkan produk dan jasa, memelihara posisi yang kompetitif, dan mengelola informasi. Risiko transaksi terdapat pada setiap produk dan jasa yang ditawarkan dan mencakup pengembangan dan penyaluran produk, pemrosesan transaksi, pengembangan sistem, sistem penghitungan, kompleksitas produk dan jasa, serta *internal control*. Risiko transaksi yang tinggi dapat terkandung pada produk *internet banking*, khususnya jika tidak direncanakan, diimplementasikan, dan dipantau dengan tepat.

Aspek Hukum

Keabsahan transaksi dan kekuatan pembuktian

Transaksi elektronik melalui *internet* tidak memerlukan *hard copy* atau warkat kertas.

https://bulletin.bmeb-bi.org/bmeb/vol5/iss1/3
DOI: 10.21098/bemp.v5i1.304

Namun demikian setiap transaksi yang melibatkan eksekusi diberikan tanda bukti yang berupa nomer atau kode yang dapat di-*save* di komputer atau dicetak. Apabila terjadi sengketa atau perselisihan yang berhubungan dengan transaksi yang dilakukan melalui *internet* tersebut, masih menjadi pertanyaan apakah bukti kode/nomer transaksi yang dicetak tersebut dapat dipakai sebagai alat bukti yang kuat menurut hukum di Indonesia mengingat belum terdapatnya ketentuan khusus yang mengatur kegiatan dan transaksi elektronik melalui internet. Walaupun demikian, perjanjian antar para pihak yang terkait dalam internet banking, misalnya antara bank, nasabah, vendor,dll. memiliki kekuatan mengikat para pihak dalam perjanjian serta berlaku seperti undang-undang bagi hanya kedua belah pihak (*pacta sun servanda)*. Selain itu bukti transaksi elektronik dapat digolongkan sebagai petunjuk, sesuai pasal 184 Kitab Undang-Undang Hukum Acara Pidana, sehingga dapat dijadikan bukti pendahuluan di pengadilan. Sedangkan untuk menguatkan pembuktian transaksi tersebut dapat menggunakan saksi ahli.

Berdasarkan model *law* untuk *e-commerce* UNCITRAL (*United Nations Commission on International Trade Law*) pasal 5 dan 6, transaksi elektronik diakui sederajat dengan 'tulisan' sehingga tidak bisa ditolak sebagai bukti di pengadilan. Penggunaan tanda tangan elektronik sebagai suatu sistem pengamanan yang menggunakan *Public Key Cryptography System* dalam transaksi elektronik sangat penting, karena berfungsi untuk memastikan kevalidan nasabah serta keutuhan dokumen selama proses transmisi. Untuk itu tanda tangan elektronik dapat dianggap sebagai bentuk khusus dari transaksi sehingga tanda tangan elektronik dapat dianggap pula sebagai akta.[2] Definisi *electronic signature* menurut *Uniform Rules on Electronic Signatures Draft* adalah "*Electronic signature means data in electronic form in, affected to or logically associated with, a data message, and (that may be) used to (identify the signature holder in relation to the data message and indicate the signature holder's approval of the information contained in the data message*". Kemungkinan pengakuan tanda tangan elektronik dalam hukum Indonesia sangat tergantung pada dimungkinkannya penerapan mekanisme untuk mengidentifikasi pihak yang melakukan penandatanganan dan mengindikasikan kesediaan dari pihak yang melakukan tanda tangan untuk sepakat dengan apa yang ditandatanganinya sehingga tanda tangan elektronik dapat diterima sebagai tanda tangan yang valid.

Salah satu cara yang banyak digunakan di berbagai negara adalah dengan melakukan audit dan memberikan lisensi pemerintah terhadap infrastruktur yang dipergunakan untuk 'membuat' tanda tangan elektronik. Lisensi tersebut memberikan jaminan bahwa infrastruktur tersebut telah diaudit dan memenuhi syarat minimum yang ditetapkan pemerintah. Oleh karena itu, tanda tangan yang dihasilkan infrastruktur kunci publik yang

---

2,2 *Naskah Akademik RUU tentang Tanda Tangan Elektronik dan Transaksi Elektronik*, Dirjen Perdagangan Dalam Negeri dan Deperindag serta LKHT-FHUI, 2001

disediakan oleh *Certification Authority* berlisensi (*designated CA* atau *recognized CA*) seharusnya dapat langsung diterima di pengadilan tanpa perlu dibuktikan dahulu keasliannya (penerapan standar ketat). Dalam pembuktian di pengadilan dilakukan berdasarkan prinsip pembuktian terbalik atas keaslian tanda tangan elektronik di pengadilan. Tanda tangan elektronik yang dihasilkan dari *Public Key Infrastructure* CA berlisensi tersebut langsung diakui di pengadilan sederajat dengan tanda tangan biasa, dan jika ingin dibantah maka harus dibuktikan sebaliknya (bahwa CA tersebut melanggar standar operasi yang ditetapkan untuk mendapatkan lisensi). Dapat pula diberikan jaminan pihak ketiga dari negara,dsb. Sedangkan untuk tanda tangan elektronik yang berasal dari CA tidak berlisensi, saat persidangan harus dibuktikan dulu bahwa sistem *Public Key Infrastructure* (PKI) termasuk standar operasinya sudah aman. Penentuan badan yang dapat memberikan lisensi pada CA tersebut, apakah satu atau lebih badan pemerintah ataukah suatu lembaga yang independen, harus menjadi bahan pertimbangan lebih lanjut. Dapat pula ditentukan bahwa lisensi CA dilakukan oleh Lembaga Swadaya Masyarakat yang diakui pemerintah yang terdiri dari pengguna, pelaku usaha, pemerintah, akademisi, pengacara,dll. Sedangkan audit dapat dilakukan oleh badan pemberi lisensi atau badan pemberi lisensi itu menunjuk auditor khusus untuk melakukan audit.[3] Beberapa *International Certification Authority* beserta cakupan sertifikasinya dapat dilihat pada tabel 2. Hingga saat ini di Indonesia baru terdapat satu penyelenggara *Certification Authority* yaitu PT. Telekomunikasi Indonesia.

Tabel 2. Perbandingan Antar Berbagai *Certification Authority*

Product	Cost	Privacy of Data	Security of Data	Business Policies	Transaction Processing Integrity
BBBOnline	Low	No	No	Lightly Covered	No
TRUSTe	Low	Yes	No	No	No
Verisign	Low to Medium	No	Yes: Data transmittal No : Data Storage	No	No
ICSAHigh	Yes	Yes	Somewhat Covered	Lightly Covered	
WebTrust	High	Yes	Yes	Yes	Yes

Sumber : Greenstein, Mailyn, and Todd M. Feinman, *Electronic Commerce : Security, Risk Management and Control*, Irwin McGraw-Hill, 2000.

https://bulletin.bmeb-bi.org/bmeb/vol5/iss1/3
DOI: 10.21098/bemp.v5i1.304

Sanksi pelanggaran

Sanksi hukum terhadap pelanggaran yang dilakukan dalam elektronik banking khususnya *internet banking* perlu diatur secara tegas. Pelanggaran yang dilakukan oleh nasabah, *hacker*, pegawai bank itu sendiri ataupun pihak ketiga yang menyangkut *internet banking* harus diperjelas sanksinya. Apabila sarana perangkat hukum yang ada sekarang belum ada, kemungkinan penerapan analogi atau penafsiran daripada ketentuan yang sudah ada harus dilakukan apabila dipandang perlu.

Security/Privacy Breaches

Pengamanan data transaksi maupun data nasabah merupakan suatu hal yang sangat penting dalam *internet banking*. Keselamatan dan keamanan data-data transaksi dari segala gangguan sadapan maupun pencurian dari pihak manapun harus dilindungi. Begitu halnya dengan data dan informasi nasabah bank pemakai jasa *internet banking* juga harus mendapatkan perlindungan. Perlindungan data transaksi dan nasabah tersebut akan lebih kuat dan mempunyai kekuatan hukum yang pasti apabila diatur dalam bentuk undang-undang atau peraturan.

Cross Border Issues

Masalah lintas batas antar negara memiliki dampak yang cukup luas dalam *internet banking*. Beberapa pihak yang terkait dengan transaksi *internet banking* ada kemungkinan berada di negara lain dari negara asal bank tersebut. Apabila ISP berada di luar negara asal bank tersebut dan mengalami kebangkrutan akan timbul masalah berkaitan dengan dampak hukumnya terhadap bank tersebut. Begitu pula aturan hukum yang belum jelas seandainya transaksi *internet banking* dilakukan nasabah pada saat berada di luar negeri kemudian transaksi tersebut disadap atau diubah oleh pihak lain di negara tersebut. Hal ini mungkin terjadi karena ISP di negara tersebut berbeda dengan yang ada di negara asal bank yang bersangkutan.

Berkaitan dengan pelaksanaan *cross border electronic transaction*, perlu terdapat *cross border recognition* atas tanda tangan elektronik dan sertifikat digital. Perlu terdapat perjanjian bilateral atau multilateral agar lisensi terhadap CA tiap negara memperoleh pengakuan secara internasional. Selain itu perlu pula suatu sistem akreditasi untuk menjadi CA suatu negara berdasarkan suatu standar regional maupun internasional. Perjanjian atau kesepakatan antar negara tersebut perlu memperhatikan asas *reciprocitas* (timbal balik), *mutual consent* (saling menguntungkan) dan *pacta sun servanda* (berlaku seperti undang-undang bagi hanya kedua belah pihak). Dalam perjanjian/kesepakatan tersebut perlu diatur pula

mengenai aspek-aspek hukum dalam hal terjadi sengketa perdata, seperti pemakaian hukum negara yang digunakan, tempat dan metode penyelesaian hukum,dll. Perjanjian tersebut juga perlu diterapkan bila bank menggunakan jasa ISP luar negeri. Bila terjadi wanprestasi dari suatu perjanjian, maka selain atas alasan *force majeur*, sengketa dapat diselesaikan melalui mekanisme Peradilan Internasional atau International *Court of Justice*, maupun badan arbitrase, mediasi, konsiliasi atau pengadilan internasional seperti *International Criminal Court* atau Mahkamah Internasional.

Konsep Pengaturan Internet Banking

Policy Approach

Prinsip-Prinsip dalam Pengaturan Internet Banking

Pengaturan *internet banking* di Indonesia bersifat longgar dan *technology neutral* agar tidak menghambat proses inovasi layanan perbankan melalui internet banking, bahkan diharapkan dapat mendorong pengembangannya di masa datang. Prasyarat yang perlu dipenuhi bank dalam menyelenggarakan pelayanan *internet banking* merupakan persyaratan minimum yang harus dipenuhi bank untuk memastikan bank telah menerapkan prinsip-prinsip *prudential banking operation, risk management* dan perlindungan terhadap nasabah dan bank itu sendiri.

Keberadaan praktek *internet banking* yang tidak terlepas dari berbagai risiko telah menjadi dasar bagi Bank Indonesia untuk membuat pengaturan yang bersifat *prudential* dan menganut prinsip *self regulatory banking*. Pada dasarnya pengaturan yang dibuat harus memperhatikan dan mengakomodasi beberapa aspek penting, antara lain :

1. *Bank regulatory focus* bukan *technology focus*.

   Ketergantungan *internet banking* dengan teknologi sangat besar sekali bahkan unsur teknologi tersebut sangat dominan dalam *internet banking*. Oleh karena itu pengaturan *internet banking* ke depan akan lebih lebih terfokus pada tujuan operasional perbankan dalam penyelenggaraan *internet banking* (*bank regulatory focus*) dan tidak terfokus pada aspek-aspek pengembangan teknologi itu sendiri (*technology focus*). Perkembangan teknologi dan inovasinya dapat berubah tanpa mengenal batas waktu sehingga pengaturan yang bersifat *technology focus* tidak akan mampu menampung perubahan-perubahan yang terjadi.

2. *The same protection level*

   Praktek *internet banking* masih merupakan sesuatu yang baru di Indonesia mengingat

https://bulletin.bmeb-bi.org/bmeb/vol5/iss1/3
DOI: 10.21098/bemp.v5i1.304

masih terbatasnya jumlah bank penyedia jasa *internet banking* maupun karena masih belum banyaknya *internet user* di Indonesia. Perkembangan *internet banking* ke depan selain dipengaruhi oleh faktor teknologi dan inovasi juga sangat dipengaruhi oleh unsur kepercayaan dari nasabah. Kepercayaan dari nasabah menyangkut transaksi di internet harus dijamin bahwa transaksi *internet banking* memberikan tingkat perlindungan yang seoptimal mungkin. Untuk itu pengaturan *internet banking* ke depan harus mampu menjamin kepentingan nasabah baik itu keamanan dalam bertransaksi ataupun kerahasian data nasabah.

3. Peraturan tidak menghambat pertumbuhan dan inovasi jasa pelayanan keuangan melalui *internet* dan justru sebaliknya harus mampu meningkatkan manfaatnya.

4. Harus memberi jaminan proteksi yang optimal terhadap nasabah maupun bank itu sendiri. Jaminan tersebut dimulai sejak transaksi dilakukan sampai selesainya transaksi tersebut.

5. Perhatian juga harus diarahkan pada aspek-aspek yang bersifat internasional, misalnya *home country supervision*, *cross border issues*, dan sebagainya.

Agar penyelenggaraan *internet banking* dapat memenuhi standar keamanan yang memadai dan memberikan perlindungan yang maksimum terhadap nasabah serta bank itu sendiri, maka sekurang-kurangnya pengaturan *internet banking* antara lain mencakup :

a. Perijinan
b. Prudential Management :
   - √ Sistem
   - √ Prosedur
   - √ Nama Domain
   - √ *Security*
   - √ *Internal Control*

Konsistensi Pengaturan Internet Banking dengan Kebijakan Publik Lainnya

Internet banking hanya merupakan salah satu bentuk *distribution channel* atau media pelayanan perbankan selain media lain yang telah dikenal masyarakat luas seperti *counter* bank, ATM, dll. Untuk itu produk dan jasa perbankan yang ditawarkan melalui *internet banking* serta *risk exposure* yang dihadapi bank dan nasabah tidak berbeda dengan produk dan jasa yang ditawarkan melalui *distribution channel lain*, bahkan muncul potensi risiko baru yaitu keamanan penggunaan internet. Dengan demikian dalam penyelenggaraan *internet banking*, bank tetap tunduk terhadap peraturan lain yang dikeluarkan Bank Indonesia serta kebijakan publik lain seperti ketentuan perbankan mengenai kehati-hatian, ketentuan SK

Dir BI No. 27/164/KEP/DIR tanggal 31 Maret 1995 tentang Penggunaan Teknologi Sistem Informasi oleh Bank, pencegahan terhadap *money laundering*, proteksi data personal *(bank secrecy*), kebijakan persaingan sehat, ketentuan PBI No. 3/10/PBI/2001 tentang penerapan prinsip mengenal nasabah (*know your customer*) serta PBI No. 3/3/PBI/2001 tentang Pembatasan Transaksi rupiah dan Pemberian Kredit Valas oleh Bank berkaitan dengan *cross border transaction*.

Perijinan

Proses pemberian izin penyelenggaran *internet banking* di Indonesia harus didasarkan pada risikonya. Sepanjang bank hanya memiliki *informational* atau *communication website* tidak perlu meminta persetujuan Bank Indonesia sebagai otoritas pengawas bank, tetapi cukup melaporkan saja. Dalam hal yang direncanakan bank adalah *internet banking* pada tahapan *advance* atau *transactional*, Bank Indonesia perlu memberikan izin atau persetujuan. Bank yang hanya menyediakan *website* untuk informasi atau komunikasi (yang tidak melibatkan eksekusi transaksi) tidak perlu membutuhkan ijin operasi dari BI melainkan hanya pemberitahuan atau pelaporan ke Direktorat Pengawasan.

Bank Indonesia akan menentukan "*minimum requirement*" yang harus dipenuhi oleh bank-bank sebelum ijin diberikan yang diantaranya mencakup kesiapan sistem, prosedur , pengendalian internal dan sumber daya yang telah mencakup aspek *prudential banking*, *risk management* dan *customer protection*, persyaratan baiknya kondisi keuangan bank, telah memiliki sertifikasi *website*, serta sistem bank telah diaudit oleh pihak ketiga yang independen, dll.

Tujuan proses perijinan adalah agar bank-bank senantiasa mematuhi prinsip-prinsip *prudential* dan *risk management* serta perlindungan nasabah dalam pelayanan *internet banking*. Pengawas bank yang bersangkutan meneliti kebenaran laporan rencana bank, dan apabila dirasakan perlu dapat meminta pihak ketiga *(expert)* untuk melakukan "*audit trail*" atas keamanan dan kehandalan sistemnya.

Di beberapa negara, diberlakukan ketentuan persyaratan bagi bank yang akan menyelenggarakan *internet banking* baik persyaratan yang bersifat teknis (*hardware* dan *software*) maupun non teknis seperti kinerja usaha bank dan lain sebagainya. Hal ini diperlukan dengan pertimbangan *internet banking* merupakan investasi yang mahal dan akan membebani biaya operasional bank, serta relatif rawan terhadap gangguan sekuriti.

Dalam perkembangannya, pelayanan *internet banking* dapat dilakukan dalam 2 model, yaitu (i) *internet banking* yang dilakukan oleh bank-bank yang sudah berdiri, baik sebagai tambahan *channel* dari *traditional banking* atau dalam bentuk divisi khusus, dan (ii) *stand*

https://bulletin.bmeb-bi.org/bmeb/vol5/iss1/3
DOI: 10.21098/bemp.v5i1.304

alone entities, misalnya *Internet-only-Bank* (IOB) yang dapat dimiliki oleh bank-bank yang sudah berdiri maupun oleh lembaga baru dalam industri perbankan. Dalam perbankan nasional, perlu dilakukan kajian lebih lanjut mengenai kemungkinan penerapan model kedua (IOB) di Indonesia, dengan penekanan khusus pada aspek yuridis. Dengan demikian hingga saat ini IOB belum diperkenankan pendiriannya karena belum adanya landasan hukum yang kuat.

Prudential Management

Nama Domain

Domain name atau alamat situs suatu bank haruslah jelas serta mencerminkan nama suatu bank misalnya www.bii.co.id atau www.citibank.com. Bank wajib mengumumkan nama domainnya secara luas dan disosialisasikan dengan baik kepada nasabah untuk mengurangi kemungkinan terjadinya kesalahan dalam melakukan akses ke situs bank. Bank juga perlu menerapkan segala mekanisme maupun prosedur yang diperlukan untuk memperkecil kesalahan nasabah dalam mengakses alamat situs *website* bank. Nama domain perlu memperoleh sertifikasi oleh *Certification Authority* selanjutnya akan dimuat pula pada *website* Bank Indonesia sebagai portal yang terhubung dengan *website* bank-bank tersebut. Hal ini penting untuk mengantisipasi risiko terjadinya *cybersquatters* (pengambilan nama domain atau penggunaan merk dagang untuk nama domain tanpa izin pemilik) seperti kasus pemalsuan nama domain yang terjadi pada situs BCA baru-baru ini. Tidak ada pengaturan khusus mengenai *top level domain* bank baik penggunaan *Global Top Level Domain* (seperti .com, .net,dll.) ataupun *Country Code Top Level Domain* (seperti .co.id,dll.), namun bank tetap perlu mempertimbangkan faktor keamanan di samping pertimbangan komersial.

Sistem

Penyedia jasa teknologi

Bank penyedia jasa *internet banking* dapat menyelenggarakan sendiri pelayanan jasa *internet banking* (*in house*) atau menyerahkan kepada pihak luar (*outsourcing*). Masing-masing pelayanan memiliki keuntungan dan kerugian sendiri-sendiri, namun demikian dalam hal *outsourcing* perlu diperhatikan beberapa hal :

- Manajemen bank perlu mengidentifikasi tujuan, keuntungan dan biaya yang timbul serta sesuai dengan strategi bisnis bank serta telah melalui proses identifikasi risiko

terkait dengan *outsourcing* kepada pihak ketiga.

- Pemilihan dilakukan dengan seleksi dan persyaratan yang ketat, terdokumentasi serta sesuai prosedur intern bank yang berlaku untuk pemilihan *vendor*. Dasar pemilihan vendor meliputi antara lain *financial soundness,* reputasi dan kemampuan vendor.
- Dalam hal terjadi kehilangan data, masalah dalam sistem,dll. akibat kesalahan pihak ketiga maka sepenuhnya akan menjadi tanggung jawab bank untuk menyelesaikannya.
- Bank tetap harus mempunyai kontrol terhadap sistem yang dibuat maupun dioperasikan oleh *vendor* serta dapat mengantisipasi risiko-risiko yang mungkin akan dihadapi oleh *vendor* tersebut.
- Bank harus memantau secara rutin *operational performance dan financial performance* dari *vendor*.

Jangkauan Sistem

Jangkauan sistem dalam *internet banking* dapat terbatas (*stand alone*) ataupun *interconnected* dengan sistem lain. Dengan *stand alone system*, *website* dari bank penyedia jasa *internet banking* tidak dihubungkan dengan *website* lainnya. Dengan sistem *interconnected*, *website* bank dihubungkan dengan *website* lainnya seperti bank-bank lain, bursa efek, penyedia produk/jasa lain, *website* iklan dan sebagainya. Sebagai konsekuensinya dengan *interconnected* sistem bank haruslah menganalisa risiko yang mungkin akan timbul dengan adanya hubungan antara *website* bank dengan *website* lainnya. Beberapa hal yang harus diperhatikan dengan sistem yang *interconnected* adalah :

- Apabila *website* bank mempunyai *link* dengan *website* lainnya, maka sistem pengamanan *website* bank serta *website* yang terhubung haruslah sangat bagus. Hal ini berkaitan dengan adanya layanan *internet banking Business to Business* (B2B) atau *Business to Customer* (B2C) atau *Account Aggregation*. Perlu dipertegas dalam suatu pernyataan di *website* bank bahwa bank tidak bertanggung jawab terhadap segala tuntutan dan kerugian atas produk/jasa yang ditawarkan pada *website* yang terhubung dengan *website* bank tersebut.
- Apabila bank menyediakan ruang tersendiri untuk *website* iklan maka perlu dibatasi agar iklan yang dipasang pada *website* bank adalah yang memiliki hubungan langsung dengan produk atau jasa pelayanan keuangan atau perbankan. Selain itu perlu dipertegas dalam suatu pernyataan di *website* bank bahwa bank tidak bertanggung jawab atas produk/jasa yang ditawarkan pada *website* iklan tersebut.

https://bulletin.bmeb-bi.org/bmeb/vol5/iss1/3
DOI: 10.21098/bemp.v5i1.304

Prosedur

Tahapan prosedur transaksi melalui *internet banking* sesedikitnya perlu melalui namun tidak terbatas pada tahapan sebagai berikut :

1. *Authentication* (Pengujian keotentikan)

   Uji keotentikan biasanya digunakan untuk memeriksa validitas identitas nasabah berupa *user identification* yang unik yang dapat berupa "*what the customer knows*" (*password* atau *Personal Identification Number* (PIN)), "*what the customer has*" (*security token, smart card* atau *digital certificate*) atau *who you are* (*biometric*,dll). Keefektifan uji keotentikan tersebut perlu ditinjau secara berkala dengan uji penetrasi atau metode monitoring lainnya.

2. Transaksi

   Selama terjadinya transaksi secara *on-line*, bank harus memastikan bahwa proses uji keotentikan dan pengamanan atas transaksi berlangsung terus. Nasabah perlu mengetahui mekanisme pengamanan yang digunakan bank melalui *Secure Socket Layer server–authentication*.

3. Validasi

   Validasi untuk setiap transaksi on-line perlu dilakukan diantaranya melalui penggunaan *Public Key Cryptography, digital signature,* dll. Selain itu bank juga harus mampu untuk mendeteksi dan menindaklanjuti dalam hal terdapat indikasi terjadinya transaksi yang mencurigakan (*unusual transaction*).

4. Pencatatan

   Pencatatan transaksi yang dilakukan melalui *internet banking* harus dilakukan pada saat yang sama dengan terjadinya transaksi, sedangkan pembukuan transaksi dapat dilakukan tersendiri/khusus atau digabung dengan semua transaksi yang dilakukan secara konvensional. Setiap nasabah yang melakukan transaksi dalam *internet banking* yang melibatkan eksekusi harus mendapatkan bukti transaksi yang dapat disimpan atau dicetak oleh nasabah. Selain itu bank juga harus mengirimkan konfirmasi terjadinya transaksi dengan mengirimkan bukti transaksi melalui *e-mail* atau instrumen lain melalui jalur komunikasi yang aman kepada nasabah. Bukti transaksi itu juga harus disimpan oleh bank dalam jangka waktu tertentu.

5. Pembatasan Transaksi

   Tujuan pembatasan transaksi adalah untuk melindungi dan mencegah bank maupun nasabah menderita kerugian yang lebih besar akibat rendahnya tingkat likuiditas bank, adanya *fraud* atau *hacking* dalam transaksi yang dilakukan melalui internet.

Pembatasan transaksi dapat dilakukan oleh bank dalam bentuk pembatasan jumlah transaksi dan/atau nominal uang sampai jumlah tertentu yang dapat dipindahbukukan atau ditransfer antara satu rekening dengan rekening lainnya dalam satu bank sepanjang dianggap perlu dengan menimbang kondisi likuiditas, tingkat keamanan sistem bank,dll.

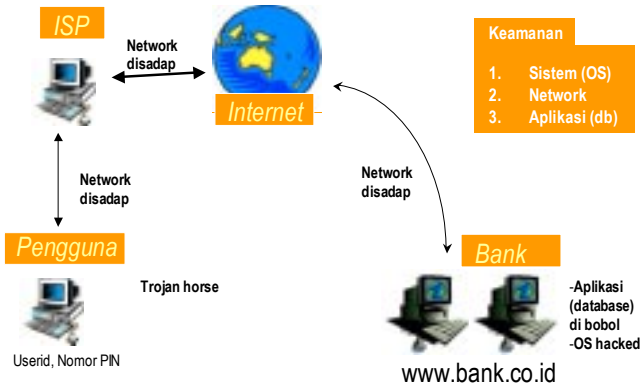
Security

Sistem dan Infrastruktur

Tantangan dan ancaman atas keamanan sistem *internet banking* terutama atas keamanan internet itu sendiri meliputi *network*, sistem operasi dan aplikasi yang diantaranya mencakup namun tidak terbatas pada :

- Penggunaan *account* orang lain
- *Denial of service attack*
- *Typosquatting*
- Penyadapan komputer pengguna, ISP maupun jaringan
- Pembobolan aplikasi database
- *Hacking* atas sistem operasi

Gambar 5. Sumber Celah Risiko Keamanan Sistem *Internet Banking*



Sumber :
Aspek Teknologi Dan Keamanan Dalam Internet Banking, Budi Rahardjo,INDOCISC,2001.

Aspek-aspek penting dari keamanan sistem *internet banking* adalah :

√ Kerahasiaan data pribadi dan transaksi nasabah;
√ Integritas data : tidak terjadi perubahan data tanpa seijin pemilik informasi;
√ Ke-otentikan : meyakinkan keaslian data, sumber data dan pihak yang mengakses data;
√ *Availability* : informasi dan sistem dapat tersedia dan berfungsi ketika dibutuhkan;
√ *Non repudiation* : pihak-pihak yang telah melakukan transaksi tidak dapat menyangkal telah melakukan transaksi;
√ Pengendalian akses ke sistem.

Prinsip-prinsip pengamanan dan perlindungan atas integritas dan kerahasiaan sistem *internet banking* terhadap ancaman internal maupun eksternal meliputi :

1. Manajemen Sumber Daya Manusia, meliputi pemisahan tugas, rotasi serta pengendalian akses ke dalam sistem

2. Infrastruktur *firewall* :

   Firewall merupakan komponen kunci terdiri dari jaringan yang aman yang dibutuhkan untuk membatasi segmen jaringan internal dan internet, sehingga jaringan internal dan eksternal terpisah secara fisik maupun logik. Firewall sebaiknya dilengkapi pula oleh suatu *Intrusion Detection System* untuk mendeteksi upaya penyusupan ke dalam sistem oleh pihak yang tidak berwenang.

3. *Security practices*, seperti :

   i. penggunaan sistem operasi (*operating system*) yang aman

   ii. implementasi sistem kriptografi yang aman untuk enkripsi maupun dekripsi seperti penggunaan *Secure Socket Layer*

   iii. melakukan penggantian atas *password* untuk sistem baru segera setelah instalasi suatu sistem

   iv. menggunakan software anti-virus

   v. analisis *security log* setiap terdapat upaya akses yang mencurigakan, terutama di luar jam-jam operasional bank.

   vi. melakukan monitoring atas *network* untuk mendeteksi anomali pada level jaringan, misalnya penggunaan *bandwith* berlebihan, *ping* terus menerus,dll.

   vii. *user ID* dan *password* yang unik untuk setiap nasabah yang harus diinput nasabah setiap kali *login*. Proses otentifikasi dapat berupa verifikasi "*what customer knows*" (seperti *Personal Identification Number*), "*what customer has*" (seperti *smart card, token*,

digital certificate, dll.) atau "*who you are*" (*biometric*,dll.) *User ID* dan *password* ini juga sebaiknya ditinjau dan diganti secara berkala.

viii. otomatis *log out,* bila nasabah tidak melakukan transaksi selama jangka waktu tertentu.

ix. pemberitahuan laporan transaksi kepada nasabah melalui *e-mail*, *short message service* nasabah atau media komunikasi lain milik nasabah yang aman, untuk melakukan konfirmasi atas transaksi yang telah dilakukan. Bank perlu melakukan konfirmasi kepada nasabah sebelum order nasabah dieksekusi jika terdapat indikasi terjadinya *unusual transaction*.

x. fasilitas pengaman dari Verisign yang menggunakan *certificate digital signature*. Bila situs tidak dilengkapi dengan fasilitas ini maka *browser* akan otomatis menampilkan peringatan bahwa *website* tersebut tidak aman.

xi. wajib melakukan *penetration testing* misalnya berupa percobaan *hacking* atas *website bank* untuk mensimulasi dan mengidentifikasi kemungkinan terjadi kelemahan desain *security system.*

xii. perlunya peninjauan berkala atas *security system* yang digunakan untuk mengantisipasi perkembangan teknologi informasi

xiii. perlunya audit secara berkala yang dilakukan oleh auditor internal atau auditor eksternal yang merupakan profesional dalam *security, bonafid* dan bukan merupakan pihak terkait dengan bank.

Kerahasiaan Data (*Privacy/Confidentiality*)

Perlu dilakukan perlindungan terhadap hak atas informasi personal nasabah yang merupakan elemen penting untuk membangun kepercayaan publik dalam pelayanan *internet banking*. Sistem yang ada dalam *internet banking* harus mampu menjamin kerahasiaan data nasabah baik dari akses internal maupun eksternal dengan implementasi kriptografi yang aman.

Contingency Planning

Bank harus memiliki alternatif skenario cara-cara pengamanan dan penyelamatan sistem maupun data/transaksi yang dilakukan melalui internet dalam hal terjadi *worst condition untuk menjamin kontinuitas pemberian layanan internet banking oleh bank,* baik atas sistem yang dikembangkan secara *in-house* maupun *outsourcing*.

https://bulletin.bmeb-bi.org/bmeb/vol5/iss1/3
DOI: 10.21098/bemp.v5i1.304

Data Recovery Center

Back up data recovery center harus dimiliki oleh setiap bank yang menyelenggarakan jasa *internet banking*.serta harus berada di lokasi terpisah dari lokasi sistem data nasabah.

Internal Control

Manajemen bertanggung jawab menyusun dan melaksanakan sistem pengendalian intern yang baik atas produk/jasa yang ditawarkan dan teknologi yang dipakai dalam *internet banking* serta memastikan tercapainya konsistensi antara perencanaan teknologi dan strategi, ketersediaan data, termasuk *Business Recovery Planning*, integritas dan kerahasiaan data serta keandalan sistem informasi manajemen. Berdasarkan standar yang disusun oleh *Information System Audit and Control Association (ISACA)*, komponen dasar pengendalian intern mencakup :

√ pengendalian akuntansi intern : menjaga nilai aset dan keandalan laporan keuangan.

√ pengendalian operasional : memastikan tujuan perusahaan dapat dipenuhi.

√ pengendalian administrasi : mengukur efisiensi operasional dan kepatuhan terhadap kebijakan dan peraturan.

Untuk itu perlu dilakukan audit berkala baik oleh pihak internal bank maupun eksternal.

Perlindungan Nasabah

Perlindungan nasabah sangat penting untuk menimbulkan kepercayaan dan kenyamanan nasabah untuk melakukan transaksi melalui *internet banking*. Karena *technology risk* dalam *internet banking* sangat tinggi, ada kemungkinan nasabah menderita kerugian karena datanya disadap oleh *hacker /cracker* atau memasuki *website* yang memiliki nama *domain* yang hampir sama. Untuk itu terdapat beberapa hal penting yang perlu diterapkan bank dalam rangka melakukan perlindungan terhadap nasabahnya, diantaranya :

√ ***Client Charter*** : yang memuat pernyataan dan komitmen bank untuk melaksanakan operasional *internet banking* yang aman, menjaga *privacy* atas informasi nasabah, memberikan pelayanan yang andal dan berkualitas, transparansi produk dan jasa serta respon segera atas pertanyaan dan keluhan nasabah.

√ ***Kerahasiaan Data Nasabah (Privacy Policy)*** *: Privacy* atas informasi personal nasabah merupakan elemen penting dari kepercayaan dan keyakinan masyarakat atas sistem perbankan Indonesia, untuk itu perbankan Indonesia diharapkan menyusun dan

menerapkan kebijakan serta langkah-langkah nyata untuk menjaga dan menghargai *privacy* atas informasi personal nasabah dan mengungkapkan kebijakan tersebut secara terbuka kepada publik.

√ ***Test and Trial Drive*** *:* Dalam rangka meningkatkan pemahaman nasabah dalam menggunakan layanan *internet banking*, bank dapat memberikan panduan penggunaan serta pelatihan (*test and trial drive*) bagi nasabah dalam menggunakan fitur dan fungsi yang dapat diperoleh nasabah di kantor bank atau pada *website* bank dalam bentuk *frequently asked question*, demo program,dll.

√ ***Customer Support Service*** *:* Bank wajib menyediakan jasa layanan nasabah (*Customer Support Service)* 24 jam yang dapat dihubungi melalui telepon, *electronic mail* atau media lainnya untuk menjawab pertanyaan nasabah serta membantu para nasabah yang mengalami kesulitan dalam pengoperasian *internet banking*. Selain itu bank harus memiliki dan menginformasikan tentang prosedur pengajuan komplain nasabah, misalnya berupa kesanggupan bank untuk melakukan *audit trail* dalam rangka pembuktian terbalik jika terjadi *dispute* antara bank dan nasabah mengenai suatu transaksi .

√ Sosialisasi : Bank perlu mengambil langkah proaktif untuk memberikan pendidikan secara berkesinambungan dan menjelaskan kepada nasabah mengenai hak dan kewajiban mereka dan bagaimana mereka wajib menjaga kerahasiaan data-data mereka dalam melakukan kegiatan/transaksi di internet. Setiap terjadi perubahan sistem terutama yang terkait dengan keamanan (*security*), integritas data (*integrity*) dan keotentikan (*authentication*), kepada nasabah perlu diberikan informasi yang memadai agar mereka dapat menggunakan sistem tersebut. Sebelum menawarkan produk/jasa *internet banking* kepada nasabah, bank harus membuat suatu Pedoman Penggunaan *Internet Banking bagi nasabahnya.*

Client Charter dan Privacy Policy harus ditampilkan pada *website* bank. Perlu disampaikan juga pada *website* bank tentang *internet clause* yang memuat risiko-risiko yang timbul akibat transaksi *internet banking*.

Selain itu pada *website* perlu ditampilkan pula Terminologi dan Persyaratan *(term and conditions)* dalam bahasa yang sederhana, jelas dan mudah dipahami yang harus dipahami serta perlu disetujui nasabah sebelum dapat melakukan transaksi melalui *internet banking*. *Jika term and conditions* disampaikan dalam Bahasa Inggris harus disertai pula dengan Bahasa Indonesia. Perubahan atas pasal-pasal dalam *term and condition* perlu disampaikan kepada nasabah dengan diberi penandaan khusus agar menarik perhatian (seperti warna yang berbeda, *higlight,*dll.)

https://bulletin.bmeb-bi.org/bmeb/vol5/iss1/3
DOI: 10.21098/bemp.v5i1.304

Kesimpulan

Perkembangan *internet banking* di Indonesia akan meningkat pesat sejalan dengan perkembangan teknologi, permintaan pasar, letak geografis dan jumlah penduduk. Penataan operasi *internet banking* diperlukan untuk menghindari permasalahan dimasa mendatang serta memudahkan pengawasan yang dilakukan oleh Bank Indonesia. Pada saat ini secara khusus pengaturan untuk *internet banking* belum ada di Indonesia, maka perlu disusun standard minimal bagi bank-bank dalam melakukan jasa pelayanan menggunakan *internet*.

Pengaturan yang diperlukan berkaitan dengan perijinan maupun standar operasi pelayanan nasabah dengan menggunakan jasa *internet*. Perijinan akan menyangkut kriteria bank untuk dapat diberi ijin serta produk-produk apa yang dapat dilayani melalui *internet*. Mengingat besarnya risiko yang terkait dengan kegiatan *internet banking*, maka perlu diatur mengenai bentuk produk dan layanan *internet banking* yang dapat ditawarkan bank. Standar operasi akan meliputi masalah teknologi sistim informasi, standar-prosedur, kontrol internal, legal dan *risk management* operasi *internet banking*. Pengaturan dilakukan sedemikian rupa sehingga diharapkan agar bank-bank tetap menerapkan prinsip *prudential banking operation*, manajemen risiko dan perlindungan nasabah. Untuk *Internet Only Banking,* pendiriannya di Indonesia belum dimungkinkan.

Pengawasan terhadap jasa pelayanan *internet* oleh bank akan meliputi kepatuhan bank terhadap peraturan dan risiko terhadap produk *internet banking*. Pengecekan tingkat kepatuhan terhadap standar operasi yang telah disepakati bersama antara bank-bank dengan otoritas lembaga pengawas akan dilakukan secara rutin meliputi keamanan dalam mengunakan sistim informasi serta manajamen risikonya, baik dilakukan dengan mengirimkan *questionaires* maupun melakukan pemeriksaan. Fokus pengawasan juga akan mencakup aspek-aspek yang berkaitan dengan risiko operasional dan legal bagi bank, khususnya berkaitan dengan *fraud*, verifikasi informasi, dan kontinuitas sistem informasi. Untuk itu perlu diberikan sosialisasi kepada para pengawas dan pemeriksa mengenai *internet banking* dan aspek-aspek pentingnya termasuk sistem keamanan, aspek hukum, risiko *internet banking*,dll.

Beberapa hal yang perlu dikaji lebih lanjut diantaranya adalah mengenai aspek hukum, khususnya keabsahan transaksi dan kekuatan pembuktian dari bukti transaksi elektronik dimana masih menunggu berlakunya suatu Undang-Undang yang mengatur transaksi elektronik di Indonesia. Di samping itu perlu dikaji selanjutnya mengenai lembaga yang dapat menjadi *Certification Authority (CA)* bagi transaksi elektronik melalui *internet banking*, apakah akan tersentralisasi atau diserahkan kepada bank atau pihak ketiga yang memiliki infrastruktur yang andal dan aman serta memenuhi persyaratan minimum, dimana untuk itu dibutuhkan pula suatu standar audit sistem informasi untuk mengaudit lembaga-lembaga

CA tersebut. Selain itu mengantisipasi berkembangnya transaksi elektronik lintas batas negara, menuntut pengawas bank untuk dapat menerapkan pengawasan terkonsolidasi berbasis pada risiko dan melakukan kerjasama pengawasan dengan instansi terkait lain dan terutama pengawas bank di negara lain, khususnya di lokasi kantor pusat bank asing yang beroperasi di Indonesia.

DAFTAR PUSTAKA

Bank Negara Malaysia, Minimum *Guidelines on The Provision of Internet Banking Services by Licensed Banking Institution*, 2000.

Basle Committee on Banking Supervision, *Risk Management for Electronic Banking and Electronic Money Activities*, 1998.

Comptroller of the Currency Administrator of National Banks, *Internet Banking : Comptroller's Handbook*, October 1999.

Greenstein, Mailyn, and Todd M. Feinman, *Electronic Commerce : Security, Risk Management and Control*, Irwin McGraw-Hill, 2000.

Monetary Authority of Singapore, *Internet Banking : Technology Risk Management Guidelines*, March 2001.

Tan Khee Giap, *The Impact of Information Technology on Banking Industry*, Nanyang Technological University, 2000.

Cronin, *Banking and Finance on the Internet*, John Wilery & Sons – Canada, 1998

Direktorat Jenderal Perdagangan Dalam Negeri dan Deperindag serta LKHT-FHUI, *Naskah Akademik RUU tentang Tanda Tangan Elektronik dan Transaksi Elektronik*, 2001

Direktorat Jenderal Pos dan Telekomunikasi Departemen Perhubungan RI, *Naskah Akademik Rancangan Undang-Undang tentang Teknologi Informasi*, 2000.

PBI No.3/3/PBI/2001 tentang *Pembatasan Transaksi Rupiah dan Pemberian Kredit Valuta Asing oleh Bank..*

PBI No. 3/10/PBI/2001 tentang *"Know Your Customer"*.

Rahardjo, Budi, *Aspek Teknologi Dan Keamanan Dalam Internet Banking*, INDOCISC,2001.

https://bulletin.bmeb-bi.org/bmeb/vol5/iss1/3
DOI: 10.21098/bemp.v5i1.304