# BAB 4

# ASPEK HUKUM ELECTRONIC SIGNATURE

## 4.1. Aspek Hukum Electronic Signature dalam Regulasi Internasional

Perkembangan teknologi dan media-media baru yang dipergunakan dalam praktek perdagangan baik skala nasional, regional, maupun internasional membuat organisasi internasional memandang perlu pengakuan dan pengaturan mengenai hukum hukum teknologi informasi, khususnya mengenai transaksi elektornik dan eksistensi tanda tangan digital sebagai organ penting dalam pelaksanaan transaksi elektronik. Beberapa landasan yuridis internasional dan nasional dari pelaksanaan tanda tangan digital.

### 4.1.1. UNCITRAL *Model law on Electronic Commerce* (*with Guide to Enactment* 1996) dan UNCITRAL *Model law on Electronic Signature* (*with Guide to Enactment* 2001)

UNCITRAL sebagai salah satu organisasi internasional yang memiliki fokus dalam perkembangan teknologi informasi merupakan organisasi yang pertama kali membahas mengenai dampak penting teknologi infomrasi terhadap perniagaan elektronik. Hasil dari UNCITRAL berupa *Model law*, yang sifatnya tidak mengikat, namun menjadi acuan atau model bagi negara-negara untuk mengadopsinya atau memberlakukannya dalam hukum nasional.[122] Pada tanggal

[122] Naskah Akademik RUU tentang ITE, Departemen Komunikasi dan Informasi, hal.16

16 Desember 1996 PBB kemudian mengeluarkan *UNCITRAL Model law on Electronic Commerce*.

*Model law* merupakan model hukum yang ditujukan untuk menawarkan model hukum kepada negara-negara yang sudah atau belum mempunyai peraturan mengenai materi ini. *Model law* ini bersifat bebas bagi negara untuk mengikuti atau tidak. Diharapkan melalui *model law* ini negara-negara di dunia melalui menkontruksi hukum nasionalnya untuk mengadaptasi dengan transaksi elektronik yang terus berkembang.[123]

UNCITRAL telah menjadi dasar dan kerangka untuk hukum *e-commerce* di banyak negara di dunia. *Model law* ini pertama kali dikeluarkan pada 1995 yang kemudian disetujui oleh Majelis Umum PBB dengan Resolusi 51/162 pada tanggal 16 Desember 1996. UNCITRAL *model law* merupakan landasan untuk mengatur otentikasi, perlengkapan, dan dampak pesan elektronik berbasis komputer dalam perdagangan. Pasal 5 kemudian diadopsikan oleh UNCITRAL sebagai amandemen di Juni 1998. *Model law* yang seluruhnya dapat diperoleh di *web site* UNCITRAL.[124] *Model law* ini terdiri atas:

a. mendefinisikan kontrak elektronik dan memberikan pengaturan penerimaan dan kekuatan pembuktian dari bukti elektronik;
b. peraturan yang didasarkan pada prinsip non diskriminasi.
c. mengatur *e-commerce* secara spesifik untuk perundang-undangan nasional atau undang-undang lain yang dibuat oleh negara/negara bagian; dan
d. memberikan aturan yang pasti untuk transaksi berbasis elektronik.

---

[123] Lihat http://www.foruminternet.org/documents/lois/lire.phtml?id=21
[124] Lihat http://www.un.org dan http://www.uncitral.org

Tanda tangan elektronik dalam *model law* ini secara diatur secara eksplisit dan diakui memiliki kekuatan hukum sama dengan tanda tangan tradisional. Teknologi tanda tangan elektronik ini dapat diperkenalkan sebagai teknologi yang cocok, tanpa harus mengubah undang-undang. Ketentuan-ketentuan Pasal 7 dalam model hukum berhubungan erat dengan praktik yang sedang berlangsung[125].

> *Article 7. Signature (1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:*
>
> *(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and*
>
> (b) *that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.*

*S*elain *The UNCITRAL Model law on Electronic Commerce*, ada juga *The UNCITRAL Model law on Electronic Signature Signatures* of 2001 (*the 2001 Model law*) diadopsi sebagai implementasi dari UNCITRAL *Model law on Electronic Commerce*. *Model law* 2001 ini disusun untuk membantu negara dalam mengharmonisasikan, memodernisasikan, dan menciptakan secara lebih efektif mengenai tanda tangan elektronik. *The UNCITRAL Model Law on Electronic Signatures of 2001 (the "2001 Model Law")* merupakan implementasi (adopsi) dari *UNCITRAL Model Law on Electronic Commerce*. Pasal 7 UNCITRAL *Model Law on Electronic Commerce* ditujukan agar terdapat pemenuhan dari fungsi tanda tangan di dunia elektronik yang dapat membantu

[125] Richard hill and Ian Walden, *The Draft UNCTRAL Model Law for Electronic Commerce isues and solutions*, terjem. oleh M. Fajar dipublikasikan maret 1996, hal 1. Lihat http/:www.Banet.com/_ricardhill

negara dalam mengharmonisasikan, memodernisasikan, dan menciptakan kerangka legislatif yang adil, untuk dapat menangani secara lebih efektif masalah tanda tangan elektronik.[126]

Eksistensi *Model Law* ini pada akhirnya dapat menjadi dasar hukum dalam pelaksanaan tanda tangan elektronik, sehingga adanya perlakukan antidiskriminasi terhadap dokumentasi tertulis dengan informasi elektronik. Diharpakan pedoman dari *Model Law* ini dapat mendorong adanya legislasi nasional di negara-negara dunia yang menyadari pentingnya regulasi mengenai tanda tangan elektronik.

*Model Law* 2001 memperhatikan prinsip bahwa tidak adanya diskriminasi terhadap berbagai teknik yang mungkin dapat dipakai untuk berkomunikasi atau di simpan informasinya secara elektronik *(technology neutrality)*.[127]

### 4.1.2. *European Union* (Uni Eropa)

Uni Eropa mengeluarkan banyak aturan terkait permasalahan perkembangan teknologi informasi, tidak hanya persolan kejahatan teknologi informasi, EU juga telah mengatur masalah perdagangan elektronik yang terdiri atas: *The General EU Electronic Commerce Directive*-4 Mei 2000, *Electronic Signature Directive on* November 30th 1999, dan *Brussels Convention on Online Transactions*, yang berlaku 1 Maret 2002.[128]

*Directive* 1999/93/EC merupakan kerangka hukum bagi tanda tangan elektronik dan pelayanan sertifikasi elektronik di Uni Eropa. Secara berlahan hampir 25 (dua puluh lima) negara EU telah mengadopsi prinsip-prinsip umum

---

[126] Naskah Akademik RUU tentang ITE, *op cit*, hal. 20.
[127] *Ibid*.
[128] *Ibid.*

*Directive* 1999/93/EC. Tujuan dari *Directive* 1999/93/EC adalah untuk memudahkan penggunaan tanda tangan elektronik di negara-negara Uni Eropa dan sebagai pengakuan hukum penggunaan tanda tangan elektronik. *Directive* mendefinisikan tanda tangan elektronik sebagai data dalam bentuk elektronik yang terpasang atau terkait dengan data logis dan data elektronik lainnya dengan menggunakan metode otentikasi.[129]

### 4.1.3. General Usage for International Digitally Ensured Commerce (GUIDEC) dari ICC

GUIDEC merupakan panduan yang dibuat oleh *International Chamber of Commerce* (ICC) bagi penggunaan suatu metode yang akan menjamin (ensured) keberadaan suatu dokumen/data elektronik dalam penggunaannya dalam dunia internasional. Panduan ini menggunakan *terminologi ensured* untuk membedakannya dengan terminologi *sign* dalam hal panandatanganan (signature) terhadap suatu dokumen[130].

Pengaturan tentang *electronic commerce* menjadi salah-satu wujud kepastian hukum bagi penerapan tanda tangan elektronik. panduan ini berisi penjelasan mengenai terminologi yang ada dalam UNCIRTAL *Model Law on e-commerce*, salah satunya terminologi penandatangan data informasi elektronik. Penandatangan yang dimaksud dalam pedoman ini bukan penandatangan secara fisik (manual), namun penggunaan teknik enkripsi melalui kunci publik, yang selanjutnya cara ini disebut dengan penandatangan elektronik. melalui teknik

---

129 *Ibid.*

130 Andiyono,dkk, *Tujuan Aspek Legal, Tinjuan Kritis RUU ITE CA*, http://www.mti.ugm.ac.id/~slamet/kuliah/Aspek_Legal/uu/tugas%20pak%20ongkokel%205/Tugas%20Aspek%20Legal%20%20Tinjauan%20kritis%20RUU%20ITE%20CA.doc, hal.7.

kunci publik ini, maka faktor keamanan dan keutuhan informasi yang dikirimkan akan terjamin, apalagi risko penggunaan internet sangat rawan penyimpangan, sehingga melalui tanda tanga elektronik akan timbul jaminan keamanan dan kepastian.[131]

### 4.2. Hukum Nasional Indonesia

Sistem hukum nasional Indonesia, sebelum diundangkannya UU ITE belum memiliki payung hukum dalam perihal pengaturan transaksi elektronik serta tanda tangan elektronik sebagai otentifikasi informasi yang melekat pada sebuah sertifikat elektronik. Terdapat kekosongan hukum sebelum UU ITE diundangkan, sehingga kemungkinan terjadi sengketa yang tidak dapat diselesaikan sangat besar. Menghadapi persoalan ini, hakim diharuskan untuk dapat melakukan penemuan hukum sebagai upaya pemecahan atas persoalan hukum yang belum diatur dalam hukum nasional. Yurisprudensi hakim menjadi hal penting bagi penyelesaian sengketa yang disebabkan oleh belum adanya regulasi mengenai transaksi elektronik.

Transaksi elektronik yang merupakan bentuk perpindahan informasi secara elektronik sebenarnya telah memiliki basis tradisional yang berbentuk nonelektronik. Bentuk perpindahan atau peralihan informasi yang sejenis transaksi elektronik misalnya dalam hal penyelenggaraan pengarsipan elektronik. Hukum positif Indonesia telah mengatur cara peralihan dokumen-dokumen konvensional perusahaan ke dalam media lainnya serta penyimpanannya pada Undang-undang Nomor 8 tahun 1997 tentang dokumen perusahaan.[132]

---

[131] *Ibid.*

[132] Lihat http://www.foruminternet.org/documents/lois/lire.phtml? id=21www.legalitas.org

Mengenai aspek pembuktian transaksi elektronik sebelum UU ITE ada, maka dalam hukum permbuktian perdata hanya dikenal beberapa alat bukti yang di dalamnya tidak diatur alat bukti elektronik, sebagaimana dalam Pasal Pasal 164 *Herzien Inlands Reglements* (HIR) dan Pasal 1903 Kitab Undang-undang Hukum Perdata (KUHPerdata) terdapat 5 alat bukti, yaitu:

(a) bukti tulisan;

(b) bukti dengan saksi;

(c) persangkaan-persangkaan;

(d) pengakuan;

(e) sumpah

Secara kontekstual dengan jenis alat bukti di atas. Jelaslah menjadi hal yang penting bila dikaitkan dengan perkembangan teknologi informasi yang konvergensi sekarang ini. Bila tetap menggunakan ketentuan HIR dan KUH Perdata tersebut pasti dalam pembuktian di pengadilan hakim akan menolak alat bukti elektronik karena ketiadaan pengaturan mengenai hal tersebut. Dampaknya akan terjadi ketidakadilan dan ketidakpastian hukum serta *vacum of law* dalam perkara hukum transaksi elektronik yang secara faktual menjadi trend transaksi kontemporer.

Transaksi elektronik memiliki alat bukti tanda tangan elektronik yang melekat secara terintegrasi dalam sebuah akta elektronik. Akta ini merupakan alat bukti yang sebelum UU ITE ada tidak dapat dijadikan alat bukti. Sehingga peran UU ITE sangat signifikan dalam mengisi kekosongan hukum. Sebelum UU ITE

ada, maka peranan suatu yurisprudensi tetap sangat dibutuhkan dalam mengisi *recht vacuum*[133], seperti yang dikemukakan oleh Van Apeldoorn:

> "Bilamana sesuatu peraturan yang tercantum dalam keputusan hakim tetapi diturut, jadi, pada kenyataannya peraturan itu telah menjadi bagian dari keyakinan-hukum umum, yakni apabila tentang soal yang bersangkutan telah ditimbulkan suatu yurisprudensi tetap, maka peraturan itu telah menjadi hukum".[134]

UU ITE belum mengatur secara komprehensif mengenai transaksi elektronik khususnya mengenai otentifikasi melalui tanda tangan elektronik. Tanda tangan elektronik akan diatur lebih teknih dalam suatu peraturan pemerintah yang sekarang masih dalam sebuah rancangan, yakni Rancangan Peraturan Pemerintah tentang Tanda Tangan Elektronik (RPP TTDE), sehingga eksistensi PP ini kelak dapat menjadi dasar hukum bagi pelaksanaan tanda tangan elektronik.

Pasal 2 RPP TTDE membagi tanda tangan elektronik terdiri atas:[135]

a. tanda tangan digital melalui penggunaan infrastruktur kunci publik;
b. biometrik;
c. kriptografi simetrik;
d. tanda tangan dalam bentuk asli yang diubah menjadi data elektronik melalui media elektronik.

---

133 Aloysius Winusbroto, *Kebijakan hukum pidana dalam penanggulangan penyalahgunaan komputer*, cetakan pertama, Penerbitan Universitas Atma Jaya Yogyakarta, 1999, hal. 195.

134 E. Utrecht dan Moh. Saleh Djindang, *Pengantar dalam hukum Indonesia*, cetakan kesebelas, penerbit P.T. Ichtiar Baru dan Penerbit Sinar Harapan, Jakarta, 1989, h.162, angka 174.

135 Pasal 2 RPP tentang Tanda Tangan Elektronik (RPP TTDE).

RPP TTDE juga mengatur mengenai kekuatan hukum dan akibat hukum yang sah bagi suatu tanda tangan elektronik. Tanda tangan elektronik memiliki kekuatan hukum dan akibat hukum yang sah selama memenuhi persyaratan sebagai berikut:

a. data pembuatan tanda tangan elektronik terkait hanya kepada penandatangan saja;
b. data pembuatan tanda tangan elektronik pada saat proses penandatanganan elektronik hanya berada dalam kuasa penandatangan;
c. segala perubahan terhadap tanda tangan elektronik yang terjadi setelah waktu penandatanganan dapat diketahui;
d. segala perubahan terhadap informasi elektronik yang terkait dengan tanda tangan elektronik tersebut setelah waktu penandatanganan dapat diketahui;
e. terdapat cara tertentu untuk menunjukkan bahwa penandatangan telah memberikan persetujuan terhadap informasi elektronik yang terkait.

Setiap orang yang terlibat dalam tanda tangan elektronik berkewajiban memberikan pengamanan atas tanda tangan elektronik yang digunakannya. Pengamanan tanda tangan elektronik sekurang-kurangnya meliputi:[136]

a. sistem tidak dapat diakses oleh orang lain yang tidak berhak;
b. penandatangan harus waspada terhadap penggunaan tidak sah dari data pembuatan tanda tangan oleh orang lain; dan
c. penandatangan harus segera menggunakan cara yang dianjurkan oleh penyelenggara tanda tangan elektronik ataupun cara-cara lain yang layak dan

[136] Pasal 4 RPP TTDE

sepatutnya memberitahukan kepada seseorang yang oleh penandatangan dianggap mempercayai tanda tangan elektronik atau kepada pihak pendukung layanan tanda tangan elektronik jika:

a) penandatangan mengetahui bahwa data pembuatan tanda tangan telah dibobol;
b) keadaan yang diketahui oleh penandatangan dapat menimbulkan resiko yang berarti, kemungkinan akibat bobolnya data pembuatan tanda tangan; atau
c) dalam hal sebuah sertifikat digunakan untuk mendukung tanda tangan elektronik, memastikan kebenaran dan keutuhan dari semua informasi yang disediakan penandatangan yang terkait dengan sertifikat selama berlakunya sertifikat tersebut atau yang akan dimasukkan dalam sertifikat.

Ketentuan peraturan perundang-undangan yang mensyaratkan suatu tanda tangan atau memberikan sanksi terhadap ketiadaan tanda tangan, dinyatakan telah terpenuhi oleh tanda tangan elektronik, jika:[137]

a. tanda tangan elektonik itu diberikan berdasarkan setrtifikat elektronik oleh penyelenggara sertifikasi elektronik;
b. tanda tangan elektonik itu telah dilekatkan oleh penanda tangan dengan maksud untuk menandatangani informasi tersebut, dan
c. penerima tidak mengetahui bahwa penendatangan itu:
    1. telah melanggar kewajiban sebagai penandatangan elektronik.
    2. tidak memiliki kunci privat secara sah.

[137] Pasal 6 RPP TTDE

Dokumen yang ditandatangani dengan tanda tangan elektronik sesuai RPP tetap sah dan mengikat sebagaimana dokumen tertulis lainya, jika dokumen tersebut dilekatkan tanda tangan digital. Tanda tangan elektronik harus dapat diverifikasi oleh kunci publik yang terdapat dalam sertifikat elektronik yang[138]:

a. telah dikeluarkan oleh penyelanggara sertifikasi elektronik;

b. sah pada saat tanda tangan digital itu di buat.

Salinan dokumen yang dilekatkan oleh tanda tangan elektronik adalah sah dan memiliki akibat hukum yang sama dengan dokumen tertulis lainnya. Tanda tangan elektronik yang dibuat berdasarkan ketentuan RPP TTDE adalah sah dan mengikat sebagai suatu tanda tangan.

Dalam perkembangannya pembahasan RPP tentang TTDE mengalami perkembangan, terutama dalam hal materi muatan RPP yang akan dirumuskan secara sinergis dengan materi muatan UU ITE yang mengamanatkan materi muatan lainnya dalam peraturan pemerintah, seperti pengaturan mengenai sertifikasi keandalan dan lembaga sertifikasi keandalan, penyelanggaraan sertifikasi elektronik, penyelanggaraan sistem elektronik, dan nama domain.

RPP yang mengakomodasi Pasal 10 ayat (2), Pasal 11 ayat (2), Pasal 13 ayat (6), Pasal 16 ayat (2), Pasal 17 ayat (3), Pasal 22 ayat (2), dan Pasal 24 ayat (4) UU ITE ini dirumuskan menjadi satu ke dalam RPP tentang Penyelanggaraan Informasi dan Transaksi Elektronik (selanjutnya disebut RPP PITE).

Dalam ketentuan RPP PITE, perumusan hal tanda tangan elektonik diatur tersendiri dalam Bab III yang teridiri dari 7 Pasal. Di dalamnya mengatur

[138] Pasal 7 RPP TTDE

mengenai kekuatan hukum dan akibat hukum yang timbul dari tanda tangan elektronik; jenis tanda tangan elektonik; data pembuatan tanda tangan elektonik; proses penandatanganan; identifikasi, autentifikasi, dan verifikasi tanda tangan elektronik, serta kewajiban penyelenggara atau pendukung layanan tanda tangan elektonik.

Hal baru dalam RPP sebagaimana diatur dalam Pasal 10, antara lain mengenai jenis tanda tangan elektronik yang dibagi menjadi tanda tangan elektronik yang tersertifikasi dan tanda tangan elektonik yang tidak tersertifikasi. Beda antara keduanya terdapat pada penggunaan jasa penyelanggara sertifikaasi elektronik dan pembuktian dengan sertifikat elektronik, yakni tanda tangan terserifikasi dibuat dengan menggunakan jasa penyelenggara sertifikasi elektronik dengan bukti sertifikat elektronik, sebaliknya tanda tangan yang tidak tersertifikasi, maka tanda tangan tersebut tidak dibuat oleh penyelanggara sertifikasi elektronik sehingga tidak memiliki sertifikat elektonik.

Selain ketentuan jenis tanda tangan, diatur pula mengenai funsgi dari tanda tangan elektronik. Sebagaimana dijelaskan pada pembahasan terdahulu, tanda tangan elektonik memiliki fungsi sebagai alat autentifikasi dan verifikasi atas identitas penanda tangan dan/atau jaminan keutuhan dan keaslian sebuah informasi elektronik. Dalam transaksi elektronik, tanda tangan elektronik berfungsi sebagai persetujuan penanda tangan atas informasi elektronik dan/atau dokumen elektronik yang ditandatangani dengan tanda tangan elektonik dengan segala akibat hukum yang ditimbulkannya.

Berdasarkan Penjelasan RPP PITE, tanda tangan elektronik berfungsi sebagaimana tanda tangan manual dalam hal mempresentasikan identitas penanda

tangan. Dalam hal pembuktian keaslian (autentikasi) tanda tangan manual dapat dilakukan melalui verifikasi atau pemeriksaan terhadap spesimen tanda tangan dari penanda tangan. Pada tanda tangan elektronik, data pembuatan tanda tangan elektronik yang terkait hanya kepada penanda tangan serta merupakan unsur penghasil tanda tangan elektronik berperan sebagai spesimen tanda tangan dari penanda tangan.

Tanda tangan elektronik harus dapat digunakan oleh para ahli yang berkompeten untuk melakukan pemeriksaan dan pembuktian bahwa Informasi Elektronik yang ditandatangani dengan Tanda Tangan Elektronik tersebut tidak mengalami perubahan setelah ditandatangani

Dalam menjalankan fungsi tanda tangan elektronik dimaksud, maka tanda tangan elektronik harus dilengkapi dengan data pembuatan yang secara unik merujuk kepada penanda tangan dan dapat digunakan untuk mengidentifikasi penanda tangan. Data yang dibuat oleh penyelenggara atau pendukung layanan harus memenuhi ketentuan sebagai berikut:

a. seluruh proses pembuatan data pembuatan tanda tangan elektronik dijamin kemanan dan kerahasiaannya oleh penyelenggara atau pendukung layanan tanda tangan elektonik;
b. jika menggunakan kode kriptografi, data pembuatan tanda tangan elektronik harus tidak dapat dengan mudah diketahui dari data verifikasi tanda tangan elektronik melalui penghitungan tertentu, dalam kurun waktu tertentu, dan dengan alat yang wajar;
c. data pembuatan tanda tangan elektronik tersimpan dalam suatu media elektronik yang berada dalam penguasaan penanda tangan;

d. data yang terkait dengan penanda tangan wajib tersimpan di tempat penyimpanan data atau sarana penyimpanan data yang menggunakan sistem terpercaya milik penyelenggara atau pendukung layanan tanda tangan elektronik yang dapat mendeteksi adanya perubahan serta memenuhi persyaratan:
   a) hanya orang yang diberi wewenang yang dapat memasukkan data baru, mengubah, menukar, atau mengganti data yang ada;
   b) informasi identitas penanda tangan dapat diperiksa keautentikannya;
   c) perubahan teknis apa pun yang melanggar persyaratan keamanan dapat dideteksi atau diketahui oleh penyelenggara.

Data sebagaimana dijelaskan di atas, pada proses penandatanganannya harus melalui mekanisme yang digunakan untuk memastikan data pembuatan tanda tangan elektronik masih berlaku, tidak dibatalkan, atau tidak ditarik; tidak dilaporkan hilang; tidak dilaporkan berpindah tangan kepada orang yang tidak berhak; dan berada dalam kuasa penanda tangan. Mekanisme yang harus digunakan sebelum dilakukan penandatangan yang didahului dengan pesertujuan, yaitu mekanisme afirmasi dan/atau mekanisme lain yang memperlihatkan maksud dan tujuan penanda tangan yang terikat dalam suatu transaksi elektronik.[139]

[139] Pasal 13 ayat (1) dan ayat (2) RPP PITE

### 4.3. Aspek Hukum Electronic Signature di Sektor Perbankan

Sektor perbankan merupakan salah-satu bidang usaha jasa juga dalam pelaksanaan bisnisnya menerapkan dan memanfaatkan teknologi informasi. Bank Indonesia (BI) sebagai bank sentral telah mengimplementasikan sistem kliring elektronik Jakarta (SKEJ) yang memungkinkan bank-bank peserta kliring dapat melakukan kliring secara elektronik, selain itu ada juga sistem *real time gross settlement* (RTGS) untuk mendukung pembayaran bernilai tinggi (*high value payment*) yang harus dilakukan secara cepat.

Pengakuan data elektronik sebelum UU ITE juga diatur di dalam UU Nomor 23 Tahun 1999 tentang Bank Indonesia, yakni dalam Penjelasan Pasal 16 yang menyatakan bahwa kliring adalah pertukaran warkat atau data kauangan elektronik antar bank baik atas nama bank maupun nasabah yang hasil perhitungannya diselesaikan pada waktu tertentu.

Selanjutnya dalam Peraturan Bank Indonesia (PBI) Nomor 1/3/PBI/1999 tanggal 13 Agustus 1999 tentang Penyelenggaraan Kliring Lokal dan Penyelesaian Akhir Transaksi Pembayaran Antar Bank Atas Hasil Kliring Lokal, sebagaimana diatur dalam Pasal 1 angka 8 yang menjadi dasar pengakuan atas data elektronik sebagai dasar pembukuan,yaitu data keuangan elektronik (DKE) merupakan data keuangan dalam bentuk elektronik yang digunakan sebagai dasar perhitungan dalam kliring lokal. Berdasarkan ketentuan di atas diketahui bahwa perhitungan kliring lokal dalam semi otomasi dan elektronik didasarkan pada DKE.

Peraturan lain adalah PBI Nomor 2/24/PBI/2000 tentang Hubungan Rekening Giro Antar Bank Indonesia Dengan Pihak Ekstern, selain Peraturan Bank Indonesia (PBI) Nomor 1/3/PBI/1999 di atas. Pasal 15 dan 19 PBI Nomor 2/24/PBI/2000 mengatur mengenai penarikan rekening giro rupiah dengan menggunakan sarana elektronik. Sarana elektronik dimaksud adalah suatu fasilitas yang ditetapkan oleh BI dnegan memanfaatkan teknologi komputer guna melakukan penarikan dana secara tunai dari satu rekening giro atau memindahkan dana dari satu rekening giro ke rekening giro lainnya.

Selanjutnya peraturan terbaru Bank Indonesia yang berkaitan dengan teknologi informasi selain kedua peraturan di atas, yaitu PBI Nomor 9/15/PBI/2007 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi oleh Bank Umum. Bank Indonesia menganggap teknologi informasi sebagai aset yang berharga bagi bank sehingga pengelolaannya bukan hanya merupakan tanggung jawab unit kerja penyelenggara teknologi informasi namun juga seluruh pihak yang menggunakannya.[140]

Peraturan BI ini mengatur beberapa domain turunan dari teknlogi informasi yang relevan dengan perbankan, beberapa pengaturan tersebut di antaranya menejemen risiko teknologi informasi, kebijakan dan prosedur penggunaan teknologi informasi di bank, sistem pengendalian dan audit intern atas penyelenggaraan teknologi informasi, *electronic banking*, sanksi terhadap pelanggaran pengaturan teknologi informasi di bank.

---

[140] Huruf d, dasar Menimbang PBI No.9/15/PBI/2007 tentang Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi

Berlakunya PBI Nomor 9/15/PBI/2007 mencabut beberapa aturan lainnya di bidang teknologi informasi perbankan, yaitu:

a. SK Dir BI No.27/164/KEP/DIR Tgl.31-3-1995 tentang Penggunaan Teknologi Informasi oleh Bank;
b. SEBI No.27/9/UPPB Tgl.31-3-1995 tentang Penggunaan Teknologi Informasi oleh Bank;
c. SK Dir BI No.31/175/KEP/DIR Tgl.22-12-1998 tentang Teknologi Sistem Bank dalam Menghadapi tahun 2000;
d. SEBI No.31/14/UPPB Tgl.22-12-1998 tentang Penyempurnaan Teknologi Sistem Informasi Bank dalam Menghadapi Tahun 2000;
e. PBI No.1/11/PBI/1999 Tgl.22-12-1999 tentang Fasilitas Khusu dalam Rangka Mengatasi Kesulitan Pendanaan Jangka Pendek bagi Bank Umum yang disebabkan Masalah Komputer Tahun 2000; dan
f. SEBI No.6/18/DPNP Tgl.20-4-2004 tentang Penerapan Manajemen Risiko pada Aktivitas Pelayanan Jasa Bank melalui Internet (*Internet Banking*)

### 4.3.2. **Penyelanggaraan Electronic Signature dalam Mewujudkan *Secure Electronic Transaction* (SET) di Sektor Perbankan**

*Secure electronic transacation* (SET) di sektor perbankan memiliki berbagai macam jenis sebagaimana yang telah dijelaskan sebelumnya. *Electronic signature* pun merupakan salah satu bentuk SET yang digunakan sebagai autentifikasi dan verifikasi suatu informasi elektronik. Tanda tangan elektronik tersebut harus diintegrasikan ke dalam sertifikat elektronik yang memuat tanda tangan dan identitas yang menunjukan status subjek hukum para pihak dalam

transaksi elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik. Penyelenggara sertifikasi elektronik merupakan suatu badan hukum yang berfungsi sebagai pihak yang layak dipercaya, yang memberikan dan mengaudit sertifikat elektronik.

SET yang umum digunakankan yakni dengan keberadaan *public key* atau *privat key* pada mesin *web* yang menggunakan skema keamanan tersebut. Komputer yang akan berkomunikasi menggunakan data terenkripsi harus memiliki dua buah kunci untuk mengenskripsi data. Pertama, *public key* tersedia bagi siapa saja yang ingin melakukan komunikasi terhadapnya. Sehingga siapapun yang ingin melakukan komunikasi terhadap sebuah mesin secara *secure* akan memiliki salinan dari *public key* mesin tersebut. Namun, *public key* tidak cukup untuk dapat mendekripsi data, masih dibutuhkan *privat key* yang bersifat rahasia. Misalnya pada pemrosesan kartu kredit dengan sebuah bank, nasabah hanya memiliki *public key* bank tersebut dimana ia dapat melakukan dekripsi informasi, namun masih diperlukan *privat key* yang disimpan oleh bank tersebut, untuk melakukan dekripsi data.[141]

Meski masalah keamanan sudah ditangani dengan keberadaan *public key* atau *privat key*, masih ada masalah yang perlu diperhatikan lagi, yakni informasi atau data yang diperoleh merupakan data yang sesungguhnya yang dikeluarkan oleh pihak yang memiliki wewenang, bukan dari pihak yang berkepentingan dan menyalagunakan isi dari informasi tersebut. Sehingga dibutuhkan pihak ketiga untuk mengautentifikasi dan memverifikasi informasi yang datang. Informasi terenskripsi yang dikirim dan diterima akan memiliki tanda tangan elektronik, dan

[141] Dian Andriana, *Analisa dan Perancangan Prototipe Aplikasi E-Commerce*, diakses dari http://www.informatika.lipi.go.id , 1997, hal.4.

selanjutnya penyelenggara sertifikasi elektronik tersebut melakukan verifikasi. Lembaga ini akan mengeluarkan sertifikat yang memverifikasi informasi, lalu lembaga ini akan memberikan *public key* dan *privat key*. Lembaga sertifikasi elektronik ini misalnya lembaga Verisign,[142] Thawte, dan CaCert.org.

Sertifikat elektronik diatur dalam Pasal 1 angka 9 UU ITE yang secara tegas dan jelas mendefinisikan tentang tanda tangan elektronik dan sertifikat elektronik yakni masing-masing didefinisikan sebagai berikut:

> "Sertifikat elektronik adalah sertifikat yang bersifat elektronik yang memuat tanda tangan elektronik dan identitas yang menunjukkan status subjek hukum para pihak dalam transaksi elektronik yang dikeluarkan oleh penyelenggara sertifikasi elektronik".[143]

Selain menggunakan *public key* dan *privat key*, sertifikasi elektronik merupakan sarana otentikasi dari suatu dokumen elektronik yang menjamin keutuhan dokumen dimaksud selama proses transmisi sehingga dapat menjadi SET. Dalam pelaksanaan pembuatan sertifikasi elektronik, dapat digunakan sistem pengamanan informasi melalui enkripsi dengan menggunakan kriptografi simetris dan kriptografi asimetris.

### 4.4. Hubungan Antara *Electronic Certificate, Certificate Authority,* dan *Electronic Siganature*

Terkait dengan eksistensi tanda tangan elektronik dengan sertifikat elektronik. Sebagaimana dijelaskan sebelumnya bahwa tanda tangan elektronik

---

142 *Ibid.*
143 Pasal 1 angka 9 UU ITE

merupakan bagian yang melekat secara integrasi dalam sertifikat elekronik dan informasi elektronik yang dilekatkan dalam sertfikat tersebut tidak dapat dibantah keberadaannya (*non repudiation*), serta keaslian (autentik) tanda tangan yang dibubuhkan oleh pihak yang menanda tangan.

Sertifikat elektronik akan menampung tanda tangan elektronik, selain juga menunjukkan status hukum para pihak yang melakukan perbuatan hukum. Melalui sertifikat elektronik inilah jaminan keamanan terhadap suatu informasi elektronik dengan pembubuhan tanda tangan elektronik akan terjaga. Sehingga, hubungan antara sertifikat elektronik dan tanda tanga elektronik erat sekali karena terintegrasi dalam satu kesatuan organ. Sertifikat elektronik ini kemudian diproses dan dikeluarkan oleh suatu CA atau *Certification/Certificate Authority*.

CA merupakan sebuah badan hukum yang berfungsi sebagai pihak ketiga (*trusted third party*) yang layak dipercaya, yang memberikan dan mengaudit sertifikat elektronik serta menyediakan layanan keamanan yang dapat dipercaya oleh pengguna dalam menjalankan pertukaran informasi secara elektonis dan memenuhi 4 (empat) aspek keamanan (*confidentiality; authentification; integrity; non repudiation*).[144]

CA merupakan pihak ketiga yang berbentuk badan hukum, dipercaya sebagai pihak yang memberikan dan mengaudit sertifikat elektronik.[145] Selain itu CA juga mengesahkan pasangan kunci publik dan kunci privat milik orang

[144] Andiyono,dkk, *op.cit*, hal.2.
[145] Pasal 1 angka 10 UU ITE

tersebut. Proses sertifikasi untuk mendapatkan pengesahan dari CA dapat dibagi menjadi 3 (tiga) tahap:[146]

1. pelanggan/s*ubscriber* membuat sendiri pasangan kunci privat dan kunci publiknya dengan menggunakan software yang ada di dalam komputernya.
2. menunjukan bukti-bukti identitas dirinya sesuai dengan yang disyaratkan CA.
3. membuktikan bahwa dia mempunyai kunci privat yang dapat dipasangkan dengan kunci publik tanpa harus memperlihatkan kunci privatnya.

Tahapan di atas merupakan tahapan yang harus dilalui dalam memperoleh pengesahan sertifikat elektronik. Tahapan tersebut nantinya akan berkaitan dengan level atau tingkatan yang mempengaruhi kewenangan yang diperoleh pelanggan (subscriber) berdasarkan sertifikat yang diperoleh. Semakin besar kewenangannya yang diperoleh dari suatu *electronic certificate* yang diterbitkan oleh CA, semakin tinggi pula level sertifikat yang diperoleh serta semakin ketat pula persyaratan yang ditetapkan oleh CA.

Kemutlakan persyaratan di atas merupakan proses yang harus dilalui oleh pemohon sertifikat elektronik untuk memperoleh pengesahan CA melalui pengujian-pengujian yang dilakukan oleh CA yang kemudian akan menerbitkan sertifikat pengesahan. Sebelum diumumkan secara luas, pemohon sertifikat (subscriber) memiliki hak untuk memeriksa kembali informasi yang melekat pada sertifikat tersebut, yang kemudian bila telah benar maka pemohon sertifikat dapat mengumumkan sertifikat tersebut dan dapat diwakilkan oleh CS atau badan lain

[146] Andiyono,dkk, *op.cit*, hal.2.

yang berwenang. Sebagai bukti keautentifikasi dan integritasnya, maka sertifikat tersebut harus dibubuhkan tanda tangan elektronik pada sertifikat tersebut.[147]

Informasi-informasi yang terdapat di dalam sertifikat tersebut diantaranya dapat berupa:[148]

1. identitas CA yang menerbitkannya.
2. pemegang/pemilik/s*ubscriber* dari sertifikat tersebut.
3. batas waktu keberlakuan sertifikat tersebut.
4. kunci publik dari pemilik sertifikat .

Fungsi CA sebagaimana digolongkan di atas meliputi:[149]

1. membentuk hierarki bagi penandatanganan elektronik.
2. mengumumkan peraturan-peraturan mengenai penerbitan sertifikat.
3. menerima dan memeriksa pendaftaran yang diajukan.

Pihak-pihak yang terlibat dalam *electronic commerce* selain dilihat dari statusnya, juga dilihat dari kedudukannya dalam perikatan, yaitu sebagai berikut[150]:

1. penjual (merchant)
2. pembeli (buyer)
3. *certification authority* (CA)

selanjutnya, ada juga para pihak yang andilnya tidak kalah penting, yaitu:

---

147 http://www.mti.ugm.ac.id , *op.cit,* hal.2
148 *Ibid.*
149 *Ibid.*
150 *Ibid.*

4. *account issuer* (penerbit rekening contoh: kartu kredit)
5. jaringan pembayaran (contohnya Visa dan Mastercard dalam scheme SET)
6. *internet service provider* (ISP)
7. *internet backbones*

## 4.5. Peran Lembaga Sertifikasi Elektronik (*Certification Authority*) dalam Menciptakan *Security Electronic Transaction* di Sektor Perbankan

Secara teknis *Certification Authority* (CA) akan menyediakan infrastruktur kunci publik (*public key infrastucture*/PKI) yang memiliki pedoman pengoperasian sertifikat atau dikenal dengan istilah *certification practice statement* (CPS), namun dalam pelaksanaannya CPS CA yang satu dengan CA lain dapat berbeda-beda.

Menurut Baker dan Kuner,[151] ada beberapa cara jenis standar pengakuan terhadap tanda tangan elektronik yang diakui negara, termasuk juga di sektor perbakan, yaitu mengenakan standar minimalistik (longgar), mengenakan standar ketat,atau penerapan beberapa standar.

### 4.5.1. Standar Minimalistik (longgar)

Pelaksanaan tanda tangan elektronik memiliki kemungkinan terjadi kekurang-otentik-an yang dilatarbelakangi oleh buruknya pengoperasian CA. Sebagaimana diatur dalam Pasal 14 UU ITE yang menyatakan bahwa penyelanggara sertifikasi elektronik (CA) harus menyediakan informasi mengenai

[151] Stewart Baker dan Chris Kuner, *An Analysis of International and Electronic signature Implementation Iniatives*, (Internet Law and Policy Forum, September 2000) http://www/ilpf.org/disig/analysis-IEDSII.htm

motode yang digunakan untuk mengidentifikasi penanda tangan, hal yang dapat digunakan untuk mengetahui data diri pembuat tanda tangan elektroni, dan hal yang dapat digunakan untuk menunjukkan keberlakuan dan keamanan tanda tangan elektronik. Uraian ini menunjukkan adanya sifat diversitas metode, pengidentifikasi tanda tangan, dan keberlakuan serta keamanan. Sehingga kemungkinan, perbedaan pedoman CA yang satu dengan CA yang lain sangat mungkin terjadi.

Keamanan tanda tangan elektronik yang menggunakan sistem kriptografi kunci publik memang lebih terjaga dibandingkan dengan penggunaan sistem operasi kriptografi kunci simetris. Namun, jika dibandingkan dengan sistem tanda tangan konvensional maka tanda tangan elektronik lebih dipertimbangkan keamananan terlepas dari adanya potensi pemalsuan terhadap tanda tangan elektronik, karena nantinya pemalsuan tersebut sudah masuk ke dalam domain tindak pidana komputer. Namun, pengadilan, misalnya, dengan berlakunya rezim UU ITE tidak tidak boleh menolak pembuktian melalui tanda tangan elektronik.

Beberapa negara *common law* (misalnya Kanada, Australia, dan Amerika Serikat) mengakui tanda tangan elektronik di pengadilan, terlepas apakah telah memenuhi standar baku atau belum. Negara-negara tersebut menerapkan sistem kebelakuan minimalistik, yakni tidak secara ketat hanya menerima pembuktian tanda tangan elektronik yang memenuhi standar baku.[152]

---

[152] Direktorat Jenderal Perdagangan Dalam Negeri, Departemen Perindutrian dan Perdagangan bekerja sama dengan LKHT UI, *Naskah Akademik RUU tentang Tanda Tangan Elektronik dan Transaksi Elektronik,* Jakarta, 2001, hal.134

### 4.5.2 Standar Ketat

Hanya tanda tangan elektronik yang sudah terjamin keamanannya yang dapat diterima di pengadilan pada negara-negara yang menerapkan standar ketat terhadap pemberlakuan tanda tangan elektronik. Tanda tangan yang terjamin keamanan dimaksud, yakni tanda tangan yang sulit dipaluskan dan terjamin keotentifikasiannya. Auditor yang dapat dipercaya akan melakukan audit terhadap CA dalam standar operasi pembuatan tanda tangan elektronik. Melalui audit ini kotentifikasi dan keamanan tanda tangan elektronik akan terjamin. Negara akan memberikan kepastian kelayakan dan keamanan melalui lisensi atau *designated CA/recognized CA* terhadap suatu CA yang setelah diaudit terbukti dapat menerapkan tanda tangan elektronik sesuai standar yang ditentukan. Melalui lisensi ini tanda tangan yang dikeluarkan CA dapat bersifat *presumption of authenticity*.[153]

### 4.5.3 Penerapan Beberapa Standar atau Dua Standar.

Selain penerapan pemberlakuan minimalis dan standar ketat. Dikenal pula penerapan pemberlakuan beberapa standar atau dua standar oleh negara. Penerapan ini dilakukan melalui pengakuan keberadaan tanda tangan elektronik yang dibuat oleh CA berlinsensi dan juga terhadap CA yang tidak berlisensi. Namun, CA yang berlisensi akan memiliki keuntungan dibanding yang tidak berlisensi. Keuntungan tersebut antara lain:[154]

---

[153] Maksudnya adalah tanda tangan elektronik tersebut tidak perlu lagi dibuktikan keotentifikasiannya oleh pengadilan.

[154] Naskah Akademik, *op.cit,* hal.135.

1. prinsip pembuktian terbalik atas tanda tangan elektronik di pengadilan. Tanda tangan elektronik berlisensi akan diakui langsung oleh pengadilan selama tidak ada yang membuktikan terbalik keotentikannya;
2. adanya *reliance limit* jia CA harus memberikan ganti rugi terhadap subscribernya ketika ada masalah; dan
3. adanya pemberian jaminan kepada pihak ketiga dari negara dan sebagainya.

Sebaliknya, tanda tangan elektronik melalui CA yang tidak berlisensi harus melalui pembuktian di persidangan terhadap PKI (termasuk CPS). Negara yang menetapkan standar ganda ini diantaranya Singapura dan Hongkong.

Secara teori dikenal dua penetapan standar pengakuan CA, yakni standar pengakuan yang ditetapkan oleh masyarakat (customary law) dan standar pengakuan yang ditetapkan oleh Pemerintah melalui pemberian lisensi (izin) terhadap CA.

Di Indonesia, kemungkinan penetapan standar pengakuan akan dilakukan oleh Pemerintah[155] sebagaimana diatur dalam Pasal 18 draf RPP tentang Sertifikasi Elektonik yang menyatakan bahwa Menteri[156] menetapkan Badan Pengawas Penyelenggara Sertifikasi Elektronik yang bertugas mengawasi, mengendalikan dan mengeluarkan atau menghentikan izin operasi penyelenggara sertifikasi elektronik. Badan pengawas inilah yang akan memberikan lisensi/izin kepada CA setelah CA tersebut memenuhi kualifikasi dan syarat. CA dalam

---

155 Hingga kini belum ada Peraturan Pemerintah tentang Sertifikat Elektronik yang diundangkan, namun dalam darf RPP tentang Sertifikat Elektronik diatur bahwa Pemerintah-lah yang menetapkan standar pengakuan terhadap CA.

156 Menteri dalam RPP ini adalah Menteri yang menyelenggarakan urusan pemerintahan di bidang teknologi informasi

melaksanakan penyelenggaraan sertifikasi selain berhubungan dengan badan pengawas, juga akan diaudit oleh akuntan publik.

Sebagai pemberi lisensi/izin, badan pengawas juga mempunyai wewenang untu mencabut lisensi/izin CA, apabila Badan Pengawas Penyelenggara Sertifikasi Elektronik dapat menarik kembali atau menghentikan izin operasi penyelenggara sertifikasi elektronik apabila:[157]

a. penyelenggara sertifikasi elektronik tidak melaksanakan kewajiban-kewajiban berdasarkan Peraturan Pemerintah tentang Sertifikasi Elektronik;
b. penyelenggara sertifikasi elektronik atau para pemegangsahamnya dinyatakan pailit;
c. penyelenggara sertifikasi elektronik menyalahgunakan izin yang diberikan;
d. penyelenggara sertifikasi elektronik tidak dapat melaksanakan kegiatan usahanya sebagaimana tercantum dalam izin yang telah diberikan;
e. penyelenggara sertifikasi elektronik melanggar profesionalitasnya dalam melakukan kegiatan usahanya;
f. penyelenggara sertifikasi elektronik melanggar peraturan perundang-undangan yang berlaku.

Melalui pembahasan di atas, terlihat bahwa skim pemberian lisensi dan proses audit diatur sedemikian ketat oleh negara sebagai pemberi izin/lisensi CA dalam penyelenggaraan sertifikasi elektronik.

CA sebagai *trusted third party* (TTP) di sektor perbankan memiliki peran yang sama dengan CA di luar sektor perbankan. Bank sebagai *subcriber* sama kedudukan hukumnya dengan perorangan atau korporasi yang melakukan

[157] Pasal 23 ayat (1) RPP tentang Sertifikasi Elektronik

perbuatan hukum dengan menggunakan komputer, jaringan komputer, atau media lainnya secara elektronik.

Sistem keamanan CA (TTP) di sektor perbankan hingga saat ini masih banyak menggunakan sistem kriptografi simetrik, pengaman transaksi melalui EDI. CA yang di dalamnya terdapat tanda tangan elektronik yang menggunakan sistem kunci publik (PKI) hingga kini masih menjadi sistem terbaik dibanding sistem kunci simetrik.

## 4.6. Penerapan Manejemen Resiko dalam Penggunaan Teknologi Informaasi oleh Bank

Perkembangan teknologi dan informasi mengharuskan bank untuk dapat meningkatkan kegiatan operasional bank berbasis teknologi informasu sebagai pemenuhan kebutuhan nasabah yang telah secara luas memiliki pemahaman dan kebutuhan akan teknologi informasi di sektor perbankan.

Di sisi lain, perkembangan teknologi informasi yang pesat ini pun menimbulkan efek samping terhadap operasionalisasi bank, yakni resiko munculnya dampak negatif dari penggunaan teknologi informasi di sektor perbankan. Aset teknologi infomrasi ini merupakan potensi bagi bank untuk dapat meningkatkan pelayanan prima terhadap nasabah, namun manajemen resiko yang baik harus diterapkan agar potensi tersebut tidak menjadi potensi kerusakan bagi bank dikarenakan kekurang-maksimal-an dalam memanajemen resiko bank.

Sebagaimana implementasi Basel II[158] yang memberikan kerangka terhadap kerangka perhitungan modal bank yang lebih sensitif terhadap resiko dan memberikan insentif terhadap penerapan peningkatan kualitas manajemen resiko di bank, termasuk resiko operasional teknologi informasi.

Untuk menghindari dampak negatif teknologi informasi dimaksud, bank wajib menerapkan secara efektif penggunaan teknologi informasi sebagaimana yang diamanatkan dalam Pasal 2 ayat (1) Peraturan Bank Indonesia Nomor 9/15/PBI/2007. Ruang lingkup penerapan manajemen paling sedikit mencakup:[159]

a. atas penggunaan teknologi informasi.
b. kecukupan kebijakan dan prosedur penggunaan teknologi informasi; dan
c. kecukupan proses identifikasi, pengukuran, pemantauan dan pengendalian risiko penggunaan teknologi infomrasi;

Komisaris dan direksi memiliki peran sangat penting dalam menjaga resiko yang mungkin timbul. Wewenang dan tanggung jawab jabatan tersebut

[158] Mengingat pentingnya modal pada bank, pada tahun 1988 BIS mengeluarkan suatu konsep kerangka permodalan yang lebih dikenal dengan the 1988 accord (Basel I). Sistem ini dibuat sebagai penerapan kerangka pengukuran bagi risiko kredit, dengan mensyaratkan standar modal minimum adalah 8%. Komite Basel merancang Basel I sebagai standar yang sederhana, mensyaratkan bank-bank untuk memisahkan eksposurnya ke dalam kelas yang lebih luas, yang menggambarkan kesamaan tipe debitur. Eksposur kepada nasabah dengan tipe yang sama (seperti eksposur kepada semua nasabah korporasi) akan memiliki persyaratan modal yang sama, tanpa pengawasan aktif dewan komisaris dan direksi;sistem pengendalian intern memperhatikan perbedaan yang potensial pada kemampuan pembayaran kredit dan risiko yang dimiliki oleh masing-masing individu nasabah. Sejalan dengan semakin berkembangnya produk-produk yang ada di dunia perbankan, BIS kembali menyempurnakan kerangka permodalan yang ada pada the 1988 accord dengan mengeluarkan konsep permodalan baru yang lebih di kenal dengan Basel II. Basel II dibuat berdasarkan struktur dasar the 1988 accord yang memberikan kerangka perhitungan modal yang bersifat lebih sensitif terhadap risiko (risk sensitive) serta memberikan insentif terhadap peningkatan kualitas penerapan manajemen risiko di bank. Hal ini dicapai dengan cara penyesuaian persyaratan modal dengan risiko dari kerugian kredit dan juga dengan memperkenalkan perubahan perhitungan modal dari eksposur yang disebabkan oleh risiko dari kerugian akibat kegagalan operasional (http://www.bi.go.id/web/id/Perbankan/Implementasi+**Basel**+**II**/)

[159] Pasal 2 ayat (2) Peraturan Bank Indonesia Nomor 9/15/PBI/2007 tentang Penerapan Manajemen Resiko dalam Penggunaan Teknologi Informasi oleh Bank Umum.

didasari oleh peran masing-masing jenjang jabatan, yakni komisaris sebagai pengarah, pengawasan dan pengevaluasi rencana strategi teknologi informasi dan kebijakan bank dalam penggunaan teknologi informasi. Sedangkan Direksi sebagai eksekutor kebijakan-kebijakan bertanggung jawab terhadap penetapan rencana strategis teknologi infomrasi dan kebijakan bank terkait penggunaan teknologi informasi.

Melalui tugas dan tanggung jawab di atas, maka kepastian akan penggunaan teknologi informasi yang digunakan bank dapat mendukung perkembangan usaha, pencapaian tujuan bisnis bank dan kelangsungan pelayanan kepada nasabah; mengupayakan peningkatan kompetensi sumber daya manusia yang terkait dengan penggunaan teknologi informasi; penerapan proses manajemen risiko dalam penggunaan teknologi informasi yang dilaksanakan secara memadai dan efektif; serta tersedianya kebijakan dan prosedur teknologi informasi yang memadai dan dikomunikasikan serta diterapkan secara efektif baik pada satuan kerja penyelenggara maupun pengguna teknologi informasi.

Pelaksanaan hal tersbut di atas, selanjutnya akan diukur melalui sistem pengukuran kinerja proses penyelenggaraan teknologi informasi yang paling kurang dapat mendukung proses pemantauan terhadap implementasi strategi; mendukung penyelesaian proyek; mengoptimalkan pandayagunaan sumber daya manusia dan investasi pada infrastruktur; dan meningkatkan kinerja proses penyelanggaraan teknologi informasi dan kualitas layanan penyampaian hasil proses kepada pengguna.

Selain organ pengendali risiko melalui komisaris dan direksi, bank wajib memiliki komite teknologi informasi (*information technology steering commite*)

yang bertanggung jawab memberikan rekomendasi kepada direksi yang paling kurang terkait dengan:

a. rencana strategi teknologi informasi *(information technology strategic plan)* yang searah dengan rencana strategis usaha bank;
b. kesesuaian proyek-proyek teknologi informasi yang disetujui dengan rencana teknologi informasi;
c. kesesuaian antara pelaksanaan proyek-proyek teknologi informasi dengan rencana proyek yang disepakati;
d. kesesuaian teknologi informasi dengan kebutuhan sistem informasi manajemen dan kebutuhan kegiatan usaha bank;
e. efektifitas langkah-langkah meminimalkan risiko atas investasi bank pada sektor teknologi informasi agar investasi tersebut memberikan kontribusi terhadap tercapainya tujuan bisnis bank;
f. pemantauan atas kinerja teknologi informasi dan upaya peningkatannya;
g. upaya penyelesaian berbagai masalah terkait teknologi informasi, yang tidak dapat diselesaikan oleh satua kerja pengguna dan penyelenggara, secara efektif, efisien dan tepat waktu.

Selain kewajiban menyusun rencana strategi teknologi informasi, bank wajib memiliki kebijakan dan prosedur pengaturan teknologi informasi yang meliputi aspek:

a. manajemen;
b. pengembangan dan pengadaan;
c. operasional teknologi informasi;

d. jaringan komunikasi;
e. pengamanan informasi;
f. *business continuity plan*;
g. *end user computing;*
h. *eletronoic bangking;*dan
i. penggunaan pihak penyedia jasa teknologi informasi.

Tidak hanya kewajiban pihak bank dalam upaya penerapan teknologi informasi dan upaya manajemen risiko terhadap kemungkinan terjadinya kesalahan penerapan. Pihak penyedia jasa teknologi informasi sebagai mitra bank dalam penerapan teknologi informasi (jika bank tidak membuat sistem teknologi sendiri) pun memiliki kewajiban dalam penyelanggaraan teknologi informasi di bank.

Kewajiban-kewajiban tersebut, yaitu:

a. pihak penyedia jasa harus menerapkan prinsip pengendalian teknologi informasi (IT control) secara memadai yang dibuktikan dengan hasil yang dilakukan pihak independen;
b. pihak penyedia jasa harus menyediakan akses bagi auditor intern bank, auditor eksternal yang ditunjuk bank, dan auditor Bank Indonesia untuk memperoleh data dan informasi yang diperlukan secara tepat waktu setiap kali dibutuhkan;
c. pihak penyedia jasa harus menyatakan tidak berkeberatan bila Bank Indonesia hendak melakukan pemeriksaan terhadap kegiatan penyediaan jasa tersebut;
d. sebagai pihak terafiliasi, pihak penyedia jasa harus menjamin keamanan seluruh informasi termasuk rahasia bank dan data pribadi nasabah;

e. pihak penyedia jasa hanya dapat melakukan subkontrak sebagain kegiatannya berdasarkan persetujuan bank yang dibuktikan dengan dokumen tertulis;
f. pihak penyedia jasa harus melaporkan kepada bank setiap kejadian kritis yang dapat mengakibatkan kerugian keuangan yang signifikan dan/atau mengganggu kelancaran operasional bank;
g. pihak penyedia jasa harus menyampaikan secara berkala hasil audit teknologi informasi yang dilakukan auditor independen terhadap penyelanggaraan pusat data (data center), *disaster recovery center* dan/atau pemrosesan transaksi berbasis teknologi, kepada Bank Indonesia melalui bank yang bersangkutan;
h. pihak penyedia jasa harus menyediakan *disaster recovery plan* yang teruji dan memadai; dan
i. pihak penyedia harus bersedia untuk kemungkinan penghentian perjanjian sebelum berakhirnya jangka waktu perjanjian (*early termination*).

Teknologi informasi di bank yang paling bersentuhan dengan nasabah sebagai pengguna jasa bank, termasuk jasa bank berbasis teknologi informasi, yaitu pelayanan berbasi *electronic banking*. Setiap bank yang akan menerbitkan produk *electronic banking* harus memuat rencana bisnis bank dan dilaporkan ke Bank Indonesia. Laporan tersebut dilakukan sepanjang tidak terdapat ketentuan Bank Indonesia yang secara khusus mengatur persyaratan persetujuan produk tersebut.

Laporan rencana penerbitan bank harus memuat bukti-bukti kesiapan yang berisikan hal-hal sebagai berikut:

a. struktur organisasi yang mendukung termasuk pengawasan dari pihak manajemen;
b. kebijakan,sistem, prosedur dan kewenangan dalam penerbitan produk *electronic banking;*
c. kesiapan infrastruktur teknologi informasi untuk mendukung produk *electronic banking;*
d. hasil analisis dan identifikasi risiko yang melekat pada produk *electronic banking;*
e. kesiapan penerapan manajemen risoko khususnya pengedalian pengamanan (*security control*) untuk memastikan terpenuhinya prinsip kerahasiaan (*confidentiality*), integritas *(integrity*), keaslian (*authentification*), *non repudiation* dan ketersediaan (*availibiality*);
f. hasil analisis aspek hukum;
g. uraian sistem informasi akuntansi; dan
h. program perlindungan dan edukasi nasabah.

Semua jenis upaya di atas merupakan mekanisme penerapan risiko penggunaan teknologi informasi oleh Bank agar terhindar dari penyalagunaan (kejahatan siber) oleh pelaku kejahatan, sehingga bank akan mengalami kerugian bila tidak memperhatikan pengamanan penggunaan teknologi informasi melalui manajemen risiko. Upaya preventif tersebut akan berdampak pada adanya *security electronic transaction* (SET) di sektor perbankan Indonesia.