UNIVERSITAS INDONESIA

MANAJEMEN PENGAMANAN SISTEM INFORMASI PADA *MERCHANT* BANK PERMATA
(Studi Kasus : Fraud Banking Melalui Transaksi Elektronik Pada EDC di *Merchant* Bank Permata)

TESIS

Diajukan sebagai salah satu syarat untuk memperoleh gelar Magister Sains Kajian Ilmu Kepolisian

MUHAMMAD FIRMAN
NPM 0906595371

PROGRAM PASCASARJANA
PROGRAM STUDI KAJIAN ILMU KEPOLISIAN
KEKHUSUSAN MANAJEMEN SEKURITI
JAKARTA
JULI 2011

HALAMAN PERNYATAAN ORISINILITAS

Tesis ini adalah hasil karya sendiri,
dan semua sumber yang dikutip maupun dirujuk
telah saya nyatakan benar.

Nama : MUHAMMAD FIRMAN

NPM : 0906595371

Tanda tangan :

Tanggal : Juni 2011

HALAMAN PENGESAHAN

Tesis ini diajukan oleh	:	
Nama	:	**MUHAMMAD FIRMAN**
NPM	:	**0906595371**
Program Studi	:	**KAJIAN ILMU KEPOLISIAN**
Judul Tesis	:	**MANAJEMEN PENGAMANAN SISTEM INFORMASI PADA *MERCHANT* BANK PERMATA (Studi Kasus : Fraud Banking Melalui Transaksi Elektronik Pada EDC di *Merchant* Bank Permata)**

Telah berhasil dipertahankan di hadapan Dewan Penguji dan diterima sebagai bagian persyaratan yang diperlukan untuk memperoleh gelar Magister Sains pada Program Studi Kajian Ilmu Kepolisian, Fakultas Pascasarjana, Universitas Indonesia.

DEWAN PENGUJI

Pembimbing	:	Prof. Drs. Koesparmono Irsan, SH.MM.MBA	.....
Penguji	:	Prof. Dr. Sarlito W. Sarwono, Psi	.....
Penguji	:	Dr. dr. H. Hadiman, SH.M.Sc	.....

Ditetapkan di : Jakarta

Tanggal : Juli 2011

KATA PENGANTAR

Puji syukur kepada Tuhan Yang Maha Esa, karena atas segala limpahan rahmat dan karunia-Nya tesis ini berhasil diselesaikan. Selain itu, penulis menyadari tanpa bantuan dan bimbingan dari berbagai pihak akan sangat sulit untuk dapat terselesaikan. Untuk itu pada kesempatan ini, saya mengucapkan terima kasih dan penghargaan setinggi-tingginya, kepada :

1. Prof. Dr. Sarlito Wirawan Sarwono, Psi selaku Ketua Program Studi Kajian Ilmu Kepolisian Program Pascasarjana Universitas Indonesia, yang telah mau menyumbangkan tenaga dan pikirannya kepada penulis.
2. Dr.dr. H. Hadiman, SH. Msc selaku pengajar mata kuliah Sekuriti Fisik, sekaligus penguji satu dalam tesis ini, serta atas kesabaran dan keikhlasan yang diberikan selama ini.
3. Prof. Kusparmono Irsan, SIK., SH., MM.selaku pembimbing sekaligus penguji, yang telah mau mengorbankan waktu,tenaga dan pikiran untuk penulis.
4. Seluruh pengajar program Pascasarjana Kajian Ilmu Kepolisian Universitas Indonesia yang telah mau menyumbangkan tenaga dan pikirannya kepada penulis.
5. Seluruh rekan-rekan perkuliahan khususnya angkatan XV KIK UI yang telah memberikan sumbangsih referensi dan ilmu pengetahuan.
6. Seluruh staff KIK UI yang telah ikut andil besar dalam hal terlaksananya proses belajar mengajar di program Pascasarjana KIK UI.
7. Kedua orang tua HM. Syaita dan HJ. A.Norma yang telah memberikan dukungan baik materiil maupun moril dalam menyelesaikan perkuliahan dan penulisan tesis.
8. Kepada istriku tercinta : Renny setiawati, dan anak – anakku tersayang : M.Farhan Firman, Fara Bunga Firman, Fairous Permata Firman, yang telah memberikan andil yang sangat besar dan memberikan semangat dalam menyusun dan menyelesaiakan tesis ini.
9. Kepada kakanda Kombes Pol DR. H.Ryco Amelza Dahniel, adinda AKP Anwar Haidar S.iK, M.Si, dan AKP Ari Satmoko yang telah memberikan bantuan,

bimbingan dan motivasi untuk mengikuti pendidikan di program Pascasarjana KIK UI.

10. Pihak-pihak lain baik langsung maupun tidak langsung yang tidak mungkin disebutkan satu per satu yang turut andil dalam memberikan kontribusi kepada penulis dalam menyelesaikan perkuliahan dan tesis.

Dengan demikian, saya berharap Tuhan Yang Maha Esa berkenan membalas segala kebaikan saudara-saudara semua, serta senantiasa diberikan rahmat, hidayat, dan kesuksesan kepada kita semua, amin.

Jakarta, Juni 2011

Penulis

Muhammad Firman

HALAMAN PERNYATAAN PERSETUJUAN PUBLIKASI TUGAS AKHIR UNTUK KEPENTINGAN AKADEMIS

Sebagai sivitas akademik Universitas Indonesia, saya yang bertanda tangan di bawah ini :

Nama	:	Muhammad Firman
NPM	:	0906595371
Program Studi	:	Kajian Ilmu Kepolisian
Fakultas	:	Pasca Sarjana
Jenis Karya	:	Tesis

demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Indonesia **Hak Bebas Royalti Non_Eksklusif** ***(Non-exclusive Royalty-Free Right)*** atas karya ilmiah saya yang berjudul :

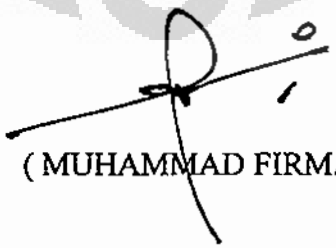
Manajemen Pengamanan Sistem Informasi Pada Merchant Bank Permata
(Studi Kasus : Fraud Banking Melalui Transaksi Elektronik Pada EDC di Merchant Bank Permata)

beserta perangkat yang ada (bila diperlukan). Dengan Hak Bebas Royalti Non-Eksklusif ini Universitas Indonesia berhak menyimpan, mengalihmedia/format-kan, mengelola dalam bentuk pangkalan data *(database)*, merawat, dan mempublikasikan tugas akhir saya tanpa meminta ijin dari saya selama tetap mencantumkan nama saya sebagai penulis/pencipta dan sebagai pemilik Hak Cipta.

Demikian pernyataan ini saya buat dengan sebenarnya.

Dibuat di : Jakarta
Pada tanggal : Juni 2011

Yang menyatakan



(MUHAMMAD FIRMAN)

ABSTRAK

Nama	:	Muhammad Firman
Nomor Mahasiswa	:	0906595371
Judul	:	Manajemen Pengamanan Sistem Informasi pada *Merchant* Bank Permata (Studi Kasus: Fraud Banking Melalui Transaksi Elektronik Pada Mesin *Elektronik Data Capture* di *Merchant* Bank Permata)

Tesis ini mencoba menganalisis sistem manajemen pangamanan informasi pada Merchant Bank Permata, atas terjadinya peristiwa fraud banking melalui mesin *elektronik data capture* di Merchant Bank Permata yang telah dilaporkan di Polda Metro Jaya pada 12 April 2010. Penelitiannya menggunakan penelitian kualitatif, dengan teknik pengumpulan data melalui wawancara mendalam, pengamatan, dan studi dokumen. Wawancara mendalam difokuskan terhadap sistem manajemen pengamanan pada proses akuisisi Merchant Bank Permata dan alur transaksi elektronik melalui mesin EDC di *Mechant* Bank Permata, faktor-faktor yang mempengaruhi terjadinya fraud Banking di Merchant Bank Permta, serta upaya untuk memperbaikinya. Sedangkan pengamatan di fokuskan terhadap cara melakukan transaksi elektronik dimulai dari transaski *on-line*, *of-line*, *settlement* dan *payment*. Selanjutnya studi dokumen difokuskan pada berkas perkara *fraud banking* yang dilaporkan di Polda Metro Jaya dan standar operasional prosedur sistem manajemen pengamanan informasi pada *Merchant* Bank Permata. Hasil penelitian membuktikan sistem manajemen pengamananan informasi di *Merchant* Bank Permata, tidak memilki sistem yang baik, karena pada proses akuisisi merchant informasi atau data tidak memenuhi aspek integritas, kerahasian, dan ketersediaan, begitu pula pada proses transaksi elektronik. Hal ini dipengaruhi faktor manusia, proses atau sistem, dan teknologi sistem manajemen pengamanan informasi. Adapun cara untuk memperbaikinya pada proses akuisisi merchant harus ada bagian atau unit yang menganalisa pemohon merchant dan pada proses transasksi elektronik menambah sistem untuk mengalisa validitas dimulai dari transaksi on-line, of-line, dan settlement, yaitu menambah sistem *terminal encryptions line*.

Kata Kunci : Transaksi elektronik, *fraud banking*, dan *Merchant*.

ABSTRACT

Name : Muhammad Firman
Student Number : 0906595371
Title : The Information System Security Management on Bank Permata's Merchants. (Case Study: Fraud Banking through Electronic Transaction on Electronic Data Capture Machine at Bank Permata's Merchants)

This thesis atempts to analyze information security management system on Bank Permata in regard with the casc of fraud banking through electronic data capture machine at Bank Permata's merchants which was reported to Jakarta Metropolitan Police on 12 April 2010. This research exercised a qualitative approach which data were collected through in-depth interview, observations and document study. The in-depth interview focussed on security management system during the acquistion of Bank Permata's merchants and electronic transaction chart through electronic data capture machine at those merchants, factors affecting fraud banking occured as well as all the restoration eforts taken. Observations focussed on the procedure of electronic transaction, which started from on line transaction, off line settlement and payment. Meanwhile, document study focussed on dossiers of fraud banking cases reported to Jakarta Metropolitan Police and Standard Operational Procedure of Information Security Management System on Bank Permata's Merchants. This research finds that the Information Security Management System was not well-established since information collected during the acquisition process and electronic transaction process were not qualified in the aspects of integrity, confidentiality and avaliability which was affected by several factors such as the human involved, the system it self as well as information security management system technology. The researcher proposes, that in order to restore the system, there should be a particular section during the acquisition process to analyze merchant requestor's validity whilst during the electronic transaction, a terminal encryptions line added to the system to analyze the validity of information both on-line transaction and off-line settlement as well as the payment.

Key words : Electronic transaction, fraud banking, and Merchant.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR SINGKATAN DAN AKRONIM

APC	:	*Acquiring Processing Control*
ATM	:	*Automated Teller Machine*
BI	:	Bank Indonesia
BPR	:	Bank Perkreditan Rakyat
BPR	:	*Bussines Processing Reengineering*
CCSL	:	*Center For Service Satisfaction And Loyalty*
CEO	:	*Chief Executive Officer*
CIA	:	*Confidentiality.Integrity, Availability*
CSR	:	*Corporate Social Responsibility*
CVC	:	*Card Validation Code*
CVV	:	*Card Validation Value*
DIP	:	*Digital Image Processing*
DIT KRIMSUS	:	Direktorat Criminal Khusus
EC	:	*Electronic Commerce*
EDC	:	*Electronic Data Capture*
HMA	:	*Head Of Merchant Acquiring*
ISO	:	*International Standardization For Organization*
KAMTIBMAS	:	Keamanan Dan Ketertiban Masyarakat
KAPOLRI	:	Kepala Kepolisian Negara Republik Indonesia
KITAS	:	Kartu Ijin Tinggal Sementara
KTP	:	Kartu Tanda Penduduk
MC	:	*Master Card*
MDF	:	*Merchant Data Form*
MI-ID	:	*Merchant Identity*
MRM	:	*Merchant Relation Manager*
MRO	:	*Merchant Relation Officer*
MSU	:	*Merchant Sales Unit*
NAC	:	*Network Access Control*
NHB	:	*Nationale Handles Bank*
NHM	:	*Nederland Handles Maarscapij*

NPWP	:	Nomor Pokok Wajib Pajak
PC	:	*Personal Computer*
PKS	:	Perjanjian Kerjasama
PMJ	:	Polda Metro Jaya
POLRI	:	Kepolisian Negara Republik Indonesia
PT	:	Perseroan Terbatas
S/N	:	*Serial Number*
SDLC	:	*System Development Security Framework*
SDN	:	Sekolah Dasar Negeri
SIM	:	Sistem Informasi Manajemen
SIUP	:	Surat Ijin Usaha Perdagangan
SKEP	:	Surat Keputusan
TBK	:	Terbuka
TI	:	Teknologi Informasi
T-ID	:	*Terminal Identity*
TLE	:	*Terminal Line Encryption*
TMC	:	*Traffic Management Center*
TS	:	*Technical Support*
UKM	:	Usaha Kecil Menengah
YDBA	:	Yayasan Dharma Bhakti Astra

DAFTAR LAMPIRAN

BAB 1
PENDAHULUAN

Tesis ini bermaksud menguraikan dan menganalisis tentang manajemen pengamanan sistem informasi pada *merchant* Bank Permata atas terjadinya *fraud banking* yang menyebabkan kerugian 70 milyar Rupiah. Pengamanan sistem informasi tersebut meliputi proses akuisisi *merchant* dan transasksi elektronik melalui mesin EDC pada *merchant* Bank Permata. Perlu dijelaskan sebelumnya Bank Permata telah menyediakan layanan elektronik untuk mempermudah transaksi perdagangan baik barang maupun jasa bagi nasabahnya, dengan mengeluarkan sebuah mesin *Electonic Data Capture* (EDC) disetiap *merchant* Bank Permata. Mesin EDC yang dimaksud dalam hal ini adalah alat atau mesin yang digunakan untuk transaksi kartu yang terhubung secara *online* atau *offline* dengan sistem jaringan Bank. Sementara *merchant* adalah orang perorangan atau badan umerchanta yang menjalankan umerchanta di bidang penjualan barang dan jasa yang dapat menerima pembayararan dengan menggunakan kartu kredit atau kartu debit setelah mendapat persetujuan dari pihak bank penerbit (Bank Permata). Sedangkan *fraud banking* dalam hal ini adalah proses transaksi yang dilakukan oleh orang yang tidak berhak menggunakan mesin EDC pada *merchant* Bank Permata sehingga menimbulkan kerugian bagi perusahaan sendiri.

1.1 Latar Belakang

Polri merupakan salah satu institusi yang mempunyai tugas dan wewenang untuk memelihara keamanan dan ketertiban. Sebagaimana UU No 2 Tahun 2002 tentang Kepolisian Negara Republik Indonesia, menyatakan bahwa Polri merupakan fungsi pemerintahan di bidang pemeliharaan keamanan dan ketertiban, penegakkan hukum, melindungi, melayani, dan mengayomi masyarakat. Selain itu fungsi Polri, menurut Suparlan (2004) merupakan alat yang dibangun dan dibentuk oleh negara untuk mencegah terjadinya kejahatan dan memerangi kejahatan.

Berdasarkan hal tersebut polisi merupakan lembaga yang bertanggung jawab (*leading sector*) dalam memelihara keamanan dan ketertiban masyarakat.

Namun bukan berarti harus melaksanakan tugas dan fungsinya sendiri (Djamin 2007), melainkan perlu ada peran dan partisipasi dari seluruh masyarakat. Tapi Polri harus memprakarsai terciptanya peran dan partisipasi masyarakat tersebut, karena ketika masyarakat berpartisipasi akan menggadakan kekuatan Polri dalam pemeliharaan kamtibmas. Sebagaimana Pasal 14 ayat 1 huruf f menyatakan Polri bertugas melakukan koordinasi, pengawasan, dan pembinaan teknis terhadap kepolisian khusus, penyidik pegawai negeri sipil, dan bentuk-bentuk pengamanan swakarsa.

Pengamanan swakarsa sendiri dalam UU No 2 tahun 2002 adalah " suatu bentuk pengamanan yang diadakan atas kemauan, kesadaran, dan kepentingan masyarakat sendiri yang kemudian mendapat pengukuhan dari Polri. Yang bertujuan untuk membentuk kekuatan keamanan dan ketertiban dari masyarakat, yang dikenal dengan istilah sistem keamanan Swakarsa (Siskamswakarsa), yang akan menjadi kekuatan kepolisian untuk memelihara keamanan dan ketertiban di lingkungan masyarakat. Siskamswakarsa sendiri menurut Djamin (2007) merupakan suatu sistem untuk memelihara keamanan dan ketertiban masyarakat perlu mengikut-sertakan secara aktif unsur-unsur keamanan masyarakat baik yang terorganisasi maupun tidak. Sedangkan Haidar (2010) mengemukakan Siskamswakarsa merupakan upaya membangun daya tangkal dan daya cegah untuk menciptakan keamanan dan ketertiban masyarakat dengan melibatkan potensi masyarakat baik yang dikelola masyarakat sendiri maupun diserahkan kepada pihak lain (penyedia jasa pengamanan).

Berkaitan dengan hal itu, Bank Permata merupakan badan usaha yang bergerak di bidang perbankan harus mempunyai sistem keamanan atau sekuriti sendiri yang menjamin keamanan, kenyamanan, dan ketentraman baik bagi masyarakat yang menjadi nasabahnya maupun Bank Permata. Sistem pengamanan tersebut ruang lingkupnya menurut Richard S. Post dalam Hadiman (2010) meliputi:

a. *Physical security*, adalah pengamanan fasilitas dan lingkungan organisasi (perumerchantaan) serta seluruh isinya, seperti mesin-mesin, laboratorium, gudang, tempat parkir dan bongkar muat barang,

kendaraan dan sebagainya. Untuk itu perlu adanya peralatan *security* yang sesuai dan jumlah satpam yang tepat.

b. *Personnel security*, adalah menyangkut pengaturan pegawai dan tamu untuk berbagai urusan. Pengawasan keluar masuk orang-orang kedalam wilayah perumerchantaan terutama ruangan-ruangan tertentu, *executive protection*, dan penelitian latar belakang pegawai, juga termasuk dalam *personnel security*.

c. *Infomation security*, adalah menyangkut komunikasi dalam perumerchantaan dan dengan luar perumerchantaan, baik lisan maupun tulisan. Bidang ini luas sekali, seperti *blue print* hasil penelitian, *record* kepegawaian dan keuangan, kontrak-kontrak, hasil penelitian laboratorium dan termasuk dalam pengamanan teknologi informasi.

Dalam hal pengamanan terhadap sistem transaksi atau pembayaran elektronik merupakan kapasitas perbankan, dalam hal ini Bank Permata, untuk mengembangkan manajemen pengamanan sistem informasi. Hal itu untuk memenuhi tuntutan masyarakat terutama kenyamanan dan keamanan dalam bertransaksi, serta penyalarasan dengan kemajuan teknologi informasi. Menurut Alter (1992) dalam Kadir (2003) teknologi informasi, kemudian disingkat dengan TI meliputi perangkat keras dan lunak untuk melakukan satu atau sejumlah tugas pemrosesan data, diantaranya: menangkap, mentransmisikan, menyimpan, mengambil, memanipulasi, atau menampilan data. Sedangkan perannya dijelaskan Kadir (2003, hlm. 15) sebagai berikut:

1) TI menggantikan peran manusia. Dalam hal ini melakukan otomatisasi terhadap suatu tugas atau proses;
2) TI memperkuat peran manusia, yakni dengan menyajikan informasi terhadap suatu tugas atau proses.
3) TI berperan dalam restrukturisasi terhadap peran manusia dengan melakukan perubahan-perubahan terhadap suatu tugas atau proses.

Sementara itu, Boyet and Boyed (1997) dikutip Suyanto (2005) mengemukakan penggunaan TI merupakan perubahan dramatis dan menggambarkannya sebagai tekanan bisnis atau dorongan bisnis. Tekanan itu diwujudkan dengan melakukan inovatif seperti membuat produk baru atau

menyediakan layanan konsumen yang handal. Selain itu TI digunakan sebagai strategi perbankan yang kompetitif. Sebagaimana dikemukan O'brein (1996) dikutip oleh Kadir (2003, hlm. 18) TI digunakan untuk membentuk strategi menuju keunggulan yang kompetitif, antara lain:

a. Strategi biaya: meminamilisir biaya atau memberikan harga yang murah terhadap pelanggan, menurunkan biaya kepada pemasok, atau meningkatkan biaya pesaing untuk tetap betahan di industri.
b. Strategi diferensiasi: mengembangkan cara-cara untuk membedakan produk atau jasa yang dihasilkan perumerchantaan terhadap pesaing sehingga pelanggan menggunakan produk atau jasa karena ada manfaat atau fitur yang unik.
c. Strategi inovasi: memperkenalkan produk/jasa yang unik, atau membuat perubahan yang radikal dalam proses bisnis yang menyebabkan perubahan-perubahan yang mendasar dalam pengelolaan bisnis.
d. Strategi aliansi: membentuk hubungan dan aliasi bisnis yang baru dengan pelanggan, pemasok, pesaing, konsultan dan lain-lain.

Sebagaimana diketahui sistem perbankan telah mengalami perkembangan pesat, dengan mengembangkan sistem informasi atau TI, dalam hal ini sistem elektronik dalam bertransaksi. Menurut Alter (1992) sistem informasi adalah kombinasi antar prosedur kerja, informasi, orang, dan teknologi informasi yang diorganisasikan untuk mencapai tujuan dalam suatu organisasi. Sedangkan Bodnar dan Hopwood (1993) dikutip Kadir dan Triwahyuni (2003) mengemukakan sistem informasi adalah kumpulan perangkat keras dan lunak yang dirancang untuk mentrasformasikan data ke dalam bentuk informasi yang berguna. Kemudian Gelinas, Oram, dan Wiggins (1990) dikutip Kadir dan Triwahyuni (2003) berpendapat sistem informasi adalah suatu sistem buatan manusia yang secara umum terdiri atas sekumpulan komponen berbasis komputer dan manual yang dibuat untuk menghimpun, menyimpan, dan mengelola data serta menyediakan informasi keluaran kepada pemakai.

Pendapat lain dikemukakan Wilkinson (1992) dalam Mcleod (1998) sistem informasi adalah kerangka kerja yang mengkoordinasikan sumberdaya (manusia, komputer) untuk mengubah masukan (input) menjadi keluaran

(informasi), guna mencapai sasaran-sasaran perusahaan. Namun istilah sistem informasi juga sering dikacaukan atau dipertukarkan dengan sistem informasi manajemen (SIM). Kedua hal ini sebenarnya tidak sama. SIM merupakan salah satu jenis sistem informasi bagi pihak manajemen dan untuk mengambil keputusan.

Dari beberapa pendapat diatas penggunaan teknologi informasi merupakan tekanan atau dorongan bisinis, untuk mempermudah pekerjaaan, memberikan kenyamanan pada pemakai (nasabah), dan daya saing perusahaan sendiri. Sebagaimana Boyed and Boyed (1977) dalam Kadir (2003) menekankan perubahan dramatis ini dan menggambarkannya sebagai tekanan atau dorongan bisnis. Menurut Suyanto (2005) tekanan-tekanan bisnis yang kuat membutuhkan perubahan radikal.

Apabila dikaitkan dengan sistem informasi Bank Permata, diharapkan mempunyai manajemen pengamanan sistem informasi yang mampu mencegah risiko kehilangan, memberikan kemudahan kepada nasabah, teman bisnis, suplier, dan untuk meningkatkan daya saing bank itu sendiri. Selain itu harus mempunyai daya tangkal dan cegah terhadap kejahatan yang ikut berkembang baik modus maupun operandinya, dari yang bersifat konvensional ataupun kejahatan modern. Karena setiap pelaku kejahatan akan terus menerus mempelajari TI yang dikembangkan sistem informasi perbankan ini untuk mencari kelemahan sistem pengamanannya, sehingga TI ini belum sepenuhnya menjamin keamanan masyarakat atau nasabah dan bank itu sendiri.

Seperti halnya strategi Bank Permata yang mengembangkan sistem layanan *elektonic commerce* (EC) untuk memudahkan sistem pembayaran atau efisiensi transaksi keuangan. Nampaknya belum sepenuhnya memberikan perlindungan pada jenis transaksi itu. Sebagaimana telah terjadi *fraud banking* atau transaksi fiktif menggunakan kartu kredit atau debet di 49 *merchant* yang tersebar di Jakarta, Semarang, dan Bandung, sehingga menimbulkan kerugian 70 Milyar Rupiah (Dit Krimsus Pola Metro Jaya 2010).

Maka dari itu perlu manajemen pengamanan sistem informasi yang baik guna mencegah kerugian (*loss prevention*) dan kejahatan (*crime pervention*). Karena tanpa itu semua, keunggulan kompetitif yang dimaksud akan sulit di raih.

Kredibilitas, kepercayaan masyarakat, dan citra Bank Permata akan semakin terpuruk, selain itu akan menimbulkan kerugian baik yang berdampak pada Bank ataupun masyarakat sendiri.

1.2 Permasalahan

Berdasarkan latar belakang di atas, permasalahan yang diteliti adalah penerapan manajemen pengamanan sistem informasi pada *merchant* Permata Bank untuk mencegah terjadinya kerugian dan kejahatan. Untuk menjawab permasalahan itu, maka penulis menjabarkan ke dalam tiga pertanyaan berikut ini.

1. Bagaimana manajemen pengamanan sistem informasi pada *merchant* Bank Permata?
2. Apa faktor-faktor yang mempengaruhi manajemen pengamanan sistem informasi, sehingga terjadi *fraud banking* pada transaksi elektonik *merchant* Bank Permata?
3. Bagaimana upaya yang dilakukan untuk memperbaiki manajemen pengamanan sistem informasi pada *merchant* Bank Permata?

1.3 Ruang Lingkup

Fokus penelitan adalah manajemen pengamanan sistem informasi pada *merchant* Bank Permata. Sedangkan ruang lingkup tempat dan obyek penelitiannya, sebagai berikut :

1. Manajemen pengamanan sistem informasi pada pada penelitian ini meliputi cara memperoleh (akuisisi) *merchant* dan transaksi elektronik pada mesin EDC di *mechant* Bank Permata.
2. Penelitian dilakukan di Bank Permata Pusat Jakarta atas terjadinya *fraud banking* yang dilaporkan di Polda Metro Jaya yang melibatkan kelima *merchant* yaitu Pretty Mom, Hongkong Fashion, Toko San-san, Padma Collection, dan Rizky Boutiqe.
3. Modus operandi pelaku kejahatan dalam melakukan *fraud banking* pada mesin EDC di *merchant* Bank Permata, pada merchant yang telah disebutkan pada nomor 2 di atas.

1.4 Tujuan dan Manfaat Penelitian

Penelitian ini bertujuan untuk membuktikan transaksi elektronik melalui EDC pada *merchant* Bank Permata memerlukan manajemen pengamanan sistem informasi yang baik. Karena apabila sistem tersebut lemah maka akan dimanfaatkan pelaku kejahatan untuk menguntungkan dirinya, yang berdampak pada kerugian baik bagi Bank Permata maupun nasabahnya. Oleh karena itu peneliti akan menunjukkan cara untuk meminimalisir atau mencegah terjadinya kejahatan (*fraud banking* melalui transaksi elektronik melalui mesin EDC pada *merchant* Bank Permata) dengan memperbaiki manajemen pengamanan sistem informasi. Sementara manfaat penelitian ini akan dibagai kedalam tiga tataran. Yaitu:

1. Dalam tataran Akademis pada Kajian Ilmu Kepolisian: diharapkan berguna untuk memperkaya Ilmu Kepolisian, khususnya untuk memahami pengamanan sistem informasi pada usaha perbankan.
2. Dalam tataran organisasi kepolisian: diharapkan mampu memberikan kontribusi pemahaman dan pengetahuan bagi sumberdaya manusia Polri tentang sistem manajemen pengamanan teknologi informasi pada sistem Bank Permata, sebagai langkah antisipatif terjadinya kejahatan *froud banking*.
3. Dalam tataran Bank Permata sendiri, diharapkan dapat memberikan pemahaman dan pengetahuan mengenai beragam faktor modus dan operandi pelaku kejahatan yang menembus manajemen pengamanan sistem informasi. Sehingga dapat dilakukan perbaikan dalam sistem pengamanannya, dan bagi nasabah atau masyarakat luas diharapkan dapat memahami dan menambah pengetahuan untuk mengantisipasi kejahatan perbankan.

1.5 Metode Penelitian

1.5.1 Penelitian Dilapangan

Penelitian ini menggunakan penelitian kualitatif. Hal ini diharapkan dapat memperoleh gambaran secara jelas dan mendalam tentang penerapan sistem pengamanan informasi yang

diterapkan oleh Bank Permata. Untuk lebih jelasnya perlu dikemukakan beberapa definisi tentang penilitian kualitatif. Pertama, Bogdan dan Taylor yang dikutip Meleong (2001) penelitian kualitatif merupakan prosedur penelitian yang menghasilkan data deskriptif berupa susunan kata-kata secara tertulis ataupun lisan dari orang-orang dan perilaku yang diamati. Lebih lanjut dijelaskan penelitian diarahkan pada latar belakang individu atau organisasi secara holistik, dalam hal ini tidak boleh memandang individu atau organisasi itu kedalam variabel atau hipotesis melainkan memandangnya sebagai satu kesatuan yang utuh.

Kedua, Creswell (2002, hlm. 1) mengemukakan "penelitian kualitatif adalah sebuah proses penyelidikan untuk memahami masalah-masalah sosial secara holistik yang dibentuk dengan rangkaian kata-kata, mendeskripsikan pandangan informan secara terperinci, dan disusun berlatar belakang alamiah." Ketiga, Muhammad dan Djaali (2005) mengemukakan penelitian kualitatif bersifat eksploratif, artinya memberi gambaran secara khusus dan mendalam tentang suatu kasus (Djaali dan Muhammad 2005).

Keempat, Suparlan (1997, hlm. 6) mengemukakan "penelitian kualitatif sasaran kajiannya adalah pola-pola yang berlaku yang merupakan prinsip-prinsip yang secara umum dan mendasar berlaku serta menyolok berdasarkan atas perwujudan dari gejala-gejala yang ada dalam kehidupan manusia." Kelima, Sugiyono (2008, 223) mengemukakan: "dalam penelitian kualitatif, peneliti merupakan instrumen pokok."

Dari beberapa pendapat di atas dapat disimpulkan penelitian kualitatif merupakan penelitian yang keandalan dan kemerchantihan datanya banyak ditentukan oleh hubungan antara peneliti dan sasaran penelitiannya. Peneliti dituntut dapat menjelaskan fenomena yang ada, dengan mengetahui keragaman

calon infomannya serta kedudukanya dalam tatanan struktur dan interaksi sosial pada kejadian yang sebenarnya di lapangan.

Oleh sebab itu, penelitian kualitatif tampaknya tepat untuk meneliti manajemen pengamanan sistem informasi Bank Permata. Selain itu melalui studi kasus, peneliti ini mencoba memahami dan mendalami fenomena yang ada, dalam kurun waktu dan tempat tertentu agar mendapat kejelasan, yang kebenarannya dapat dipertanggung jawabkan, yaitu *fraud banking* yang dilakukan di Puri Apartemen Jakarta dengan mengakses sistem elektronik mesin EDC Bank Permata dan memasukan atau mengganti nomor T-ID dan M-ID mesin EDC seolah-olah ada transaksi. Sehingga menimbulkan kerugian 70 milyar rupiah kepada 49 *merchant* yang tersebar di Jakarta, semarang, dan Bandung. Padahal transakasi itu tidak pernah terjadi atau disebut dengan transaksi fiktif, tidak ada pembeli dan tidak ada barang yang dijual, serta serta tidak pernah ada *sales draft*. Karena kartu debet dan kartu kredit serta *settelment* tidak melalui proses otorisasi.

1.5.2 Instrumen Penelitian dan Teknik Pengumpulan Data

Dalam penelitian kualitatif instumen penelitian dan kualitas pengumpulan data mempengaruhi kualitas hasil penelitian. Menurut Sugiyono (2008, hlm. 222) " dalam penelitian kualitatif, yang menjadi instrumen dan alat penelitian adalah peneliti sendiri." Oleh karena itu Sugiyono lebih lanjut menjelaskan instrumen penelitian juga perlu divalidasi terkait pemahaman penelitian kualitatif, penguasaan terhadap bidang penelitiannya, dan kesiapan memasuki objek penelitiannya, baik secara akademik maupun logistiknya. Selain itu peneliti sendiri harus menetapkan informan dan fokus penelitian sebagai sumber data dengan beberapa teknik, diantaranya: wawancara kepada informan, observasi dan studi dokumen yang berkaitan dengan permasalahan penelitian.

Dalam penelitian ini wawancara kepada informan, saya bedakan menjadi tiga informan, yaitu informan kunci, penting, dan tambahan. Informan kunci adalah manajer PT. Bank Permata, khususnya yang menangani TI. Sedangkan infoman penting adalah karyawan yang menangani IT tersebut. Sementara itu informan tambahan adalah pelaku kejahatan transaksi fiktif pada Bank Permata.

Selanjutnya observasi atau disebut dengan pengamatan. Pengamatan dalam hal ini adalah pengamatan terhadap fenomena atau gejala sehari-hari terhadap orang, tempat, atau organisasi yang ditelitinya, dalam hal ini dalah PT. Bank Permata terkait sistem manajemen pengamanan informasi yang diselenggarakan untuk mengamankan asetnya dari kejahatan dan kerugian dari sebab apapun. Dengan menghubung-hubungkan dan mengelompokan dari gejala satu dengan gelaja lainnya (Suparlan 1997), agar mempunyai makna bagi PT. Bank Permata yang diteliti. Selain itu peneliti juga menggunakan pengamatan, dengan cara mempelajari manajemen pengamanan sistem informasi di Bank Permata, kemudian menganalisanya. Hal ini peneliti ingin memperoleh kejelasan dan kedalaman tentang pelaksanaan manajemen pengamanan tersebut.

Selanjutnya untuk melengkapi, peneliti juga menggunakan studi dokumen. Dengan cara mengumpulkan dokumen-dokumen yang berkaitan dengan permasalahan penelitian, mengkaji, dan menganalisanya. Seperti standar manajemen pengamanan sistem informasi Bank Permata, laporan-laporan hasil tugas, dan berkas perkara tentang transaksi fiktif yang dilaporkan ke Polda Metro Jaya.

1.5.3 Jenis Data

Data dalam penelitian ini terdiri dari data primer dan sekunder. Data primer adalah data yang digali dan diambil

langsung dari sumbernya tanpa perantara oleh peneliti. Sumber data ini diambil dari: wawancara dengan informan, direkam menggunakan recorder, dan dicatat dalam bentuk tulisan; pengamatan dengan mencatat seleruh kejadian atau gejala-gejala yang ditemukan di tempat penelitian dalam bentuk catatan lapangan. Akan tetapi untuk menjaga privasi dalam penelitian ini informan atau objek yang diamati, apabila mempunyai nama akan disamarkan dengan nama jabatan, kode ataupun inisial.

Sedangkan data sekunder adalah data yang diambil dari orang lain atau telah dirubah oleh peneliti untuk mendukung data primer tersebut. Hal ini bermanfaat sebagai pembuktian atau argmumentasi peneliti atau teori yang digunakannya, yang berasal dari *flowchart* Bank Permata dan laporan perbankan serta dokumen lainnya yang masih ada hubungan dengan penelitian ini.

1.5.4 Teknik Analisa Data

Menurut Bogdan dikutip Sugiyono (2008) Analisis data adalah suatu proses untuk mencari dan menyusun data secara sistematis yang diperoleh dari hasil wawancara, catatan lapangan dan bahan bahan lainnya. Maka dari itu peneliti akan mengorganisasi data yang diperoleh dari hasil wawancara, pengamatan yang disajikan dalam bentuk catatan lapangan, dan dokumentasi dengan cara mengorganisasi data, memilih dan mengelompokan mana yang penting, serta menarik kesimpulan.

Model analisis data dalam penelitian ini menggunakan model Miles dan Huberman (Sugiyono 2008). Lebih lanjut Miles dan Huberman menjelaskan aktivitas dalam analisis data dilakukan secara interaktif dan terus-menerus sampai selesai, sehingga datanya jenuh, yaitu, *data reduction*, *data display*, dan *conclusion drawing/ verfication.*

Reduksi data, peneliti mengumpulkan data sebanyak-banyaknya di Bank Permata ataupun di Polda MetroJaya, sehingga akan mendapatkan data yang kompleks. Selanjutnya dilakukan

reduksi data dengan cara merangkum, mengelompokkan hal-hal yang pokok, sesuai dengan tema untuk mendapatkan polanya.

Penyajian data, peneliti menyajikan data dalam bentuk tabel, grafik, dan sejenisnya. Melalui penyajian data ini maka data akan terorganisasi dan terpola yang dituangkan dalam bentuk narasi.

Penarikan kesimpulan (*conclusion drawing/verification*), peneliti menarik kesimpulan awal dari data-data yang dikumpulkan. Apabila data tersebut belum valid dan konsisten maka peneliti kembali ke tempat penelitian untuk mengumpulkan data sampai data tersebut valid dan konsisten, yang pada akhirnya akan mendapat kesimpulan yang kredibel.

1.5.5 Tata Urut Penulisan

Penelitian ini memerlukan tata urut penulisan, agar tersusun secara runtun dan sistematis. Tata urut ini akan dibagi kedalam 6 bab yang terkait satu sama lainnya. Keenam bab tersebut akan diuraikan sebagai berikut:

Bab 1 Pendahuluan

Bab ini merupakan penjelasan dari kerangka pembahasan penelitian. Yang akan diuraikan oleh peneliti meliputi latar belakang, permasalahan, ruang lingkup, tujuan dan manfaat penelitian, metode penelitian dan tata urut penulisan.

Bab 2 Tinjauan Kepustakaan

Bab II memaparkan tinjauan kepustakaan yang dijadikan sebagai landasan kepustakaan penelitian, konseptual dan teori penelitian. Kepustakaan penelitian berisi tentang penelitian terdahulu , konseptual berisi tentang konsep yang ada kaitannya dengan penelitian, dan teori berisi tetnang teori-teori yang akan dijadikan pisau analisis dalam menjawab permasalahan penelitian.

Bab 3 Gambaran Umum Bank Permata

Gambaran umum berisi tentang Sejarah perbankan di Indonesia yang akan memuat jenis bank. Kemudian memuat tentang profil Bank Permata sebagai bahan untuk mengantarkan pemahaman tetang karateristik dan ruang lingkup umerchanta Bank Permata sebagai objek penelitian

Bab 4 Manajemen Pengamanan Sistem Informasi *Merchant* Bank Permata

Pada bab ini memaparkan tentang karakteristik pengamanan sistem informasi merchant yang terdiri dari proses akuisisi merchant dan alur transaksi elektronik pada EDC. Sedangkan penyebab terjadinya *fraud banking* ditinjau dalam aspek akuisisi *merchant* dan alur transaksi elektronik pada EDC.

Bab 5 Analisa dan Pembahasan.

Dalam bab ini peneliti akan menganalisis hasil penelitian dengan pisau analisis berupa konsep-konsep dan teori-teori yang dikemukakan pada bab 2.

Bab 6 Penutup

Bab ini merupakan intisari dari penelitian. Yaitu menjawab permasalahan penelitian yang telah diuraikan pada bab 1. Sedangkan saran berupa rekomendasi sebagai bahan masukan untuk memperbaiki manajemen pengamanan sistem informasi *Merchant* Bank Permata.

BAB 2
TINJAUAN KEPUSTAKAAN

2.1 Kepustakaan Penelitian

Penelitian sistem pengamanan informasi pernah dilakukan oleh Santosa (2010) yang berjudul "Penerapan Manajemen Keamanan Informasi Pada *Traffic Management Center* Direktorat Lalu lintas Polda Metro Jaya Dengan Pengendalian ISO 27001: 2005". Penelitian Santosa ini memfokuskan pada upaya terciptanya keamanan informasi dalam operasional *Traffic Management Center* (*TMC*) Polda Metro Jaya (PMJ) dengan mengimplementasikan ISO 27001: 2005 sebagai standar desain internasional pengamanan informasi dalam mengamankan aset-aset informasi untuk meminimalisir ancaman kejahatan dan kerugian dari semua sebab. Hasil penelitiannya menjelaskan tindakan kebijakan keamanan yang dilaksanakan oleh Direktorat Lalu lintas Polda Metro Jaya terhadap personel, bangunan fisik, dan informasi TMC belum optimal dan sering terjadi gangguan. Hal ini disebabkan oleh belum adanya struktur organisasi yang permanen karena pengaruh terhadap pengembangan organisasi dan belum ada dokumentasi standar operasional prosedur pengamanan informasi atas layanan-layanan aplikasi informasi. Namun perbedaan dengan penelitian ini memfokuskan kepada sistem pengamanan informasi untuk mencegah terjadinya kerugian dan kejahatan transaksi fiktif melalui mesin EDC pada *merchant*. Selain itu tempat, waktu, dan lokasi yang diteliti berbeda dengan penelitian terdahulu.

2.2 Kepustakaan Konseptual

Kepustakaan konseptual ini berisi tentang konsep-konsep yang ada kaitannya dengan penelitian. Sehingga dapat memberikan gambaran dan menjelaskan fenomena yang akan diteliti. Adapun kepustakaan konseptual sebagai berikut

2.2.1 Sistem Informasi Manajemen

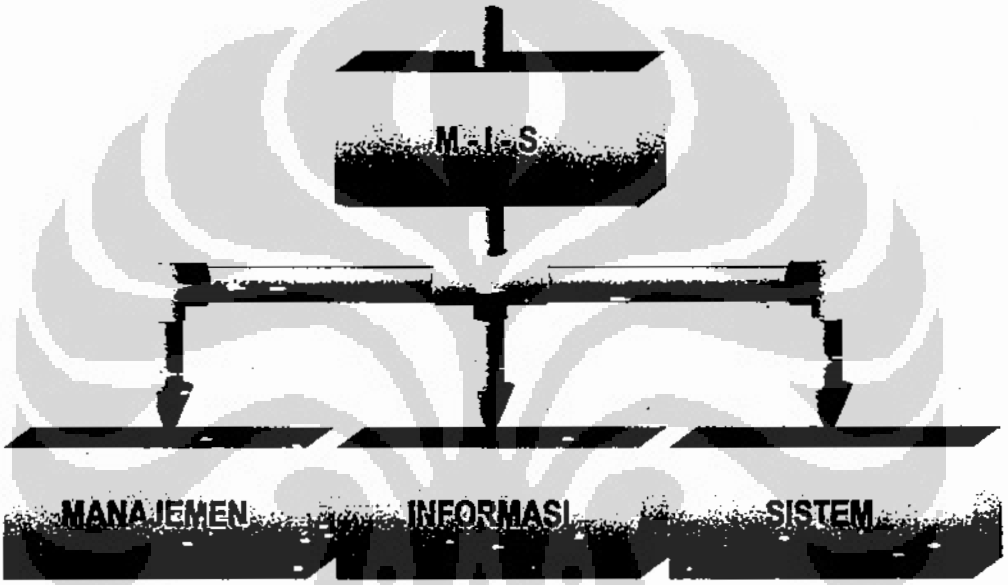
Dewasa ini, setiap perusahaan menggunakan sistem informasi manajemen untuk mendukung keberlangsungan bisnisnya. Sehingga sistem itu bukanlah hal

yang baru, melainkan sudah menjadi kebutuhan bagi perumerchantaan untuk menjalankan bisnis mereka. Kebutuhannya adalah sistem informasi terkini, akurat dan mutakhir.

Sistem informasi Manajemen (SIM) merupakan perpaduan dari 3 subjek yang berbeda. Menurut Murdick, Ross, dan Claggett (1984, hlm. 5) ruang lingkup SIM dapat dimengerti bila setiap istilah didefinisikan, sebagi berikut

Gambar 1

Sistem Informasi Manajemen



Sumber: Murdick, Ross, dan Claggett (1984, hlm. 5)

Lebih lanjut Murdick, Ross, dan Claggett (1984) mengemukakan manajemen merupakan proses kegiatan manajer dapat mengoperasikan organisasi mereka meliputi: perencanaan, pengorganisasian, melaksanakan dan mengendalikan operasi. Pendapat lain dikemukakan Gibson, Donnelly, dan Invancevich dikutip Winarsih dan Ratminto (2008, hlm. 1–2), "Suatu proses yang dilakukan oleh satu atau lebih individu untuk mengkoordinasikan berbagai aktivitas lain untuk mencapai hasil-hasil yang tidak bisa dicapai apabila suatu individu bekerja sendiri." Sementara itu Terry (1986, hlm. 4) mengemukakan manajemen sebagai berikut:

> Proses yang khas, yang terdiri dari tindakan-tindakan: perencanaan, pengorganisasian, menggerakan dan pengawasan, yang dilakukan untuk

menentukan serta mencapai sasaran-sasaran yang telah ditetapkan melalui pemanfaatan sumberdaya manusia dan sumberdaya lainnya.

Dari ketiga pendapat tentang manajemen diperoleh intisari manajemen merupakan suatu proses kegiatan atau tindakan tindakan dari sekompok orang dalam suatu organisasi atau wadah melalui tahapan perencanaan, pengorganisasian, pelaksanaan dan pengendalian.

Sedangkan sistem dapat diartikan secara sederhana sebagai perangkat elemen yang digabungkan satu sama lainnya untuk satu tujuan (Murdick, Ross, dan Claggett 1984). Mcleod (1998) berpendapat sistem merupakan sekelompok elemen yang integrasi dengan maksud yang sama untuk mencapai satu tujuan yang sama. Kedua pendapat tersebut dapat disimpulkan sistem adalah perangkat elemen yang saling terkait dan bekerja sama satu sama lainnya untuk mencapai satu tujuan.

Selanjutnya informasi adalah adalah salah satu jenis utama sumberdaya yang tersedia bagi organisasi. Sebagaimana Raymond Mcleod (1998) berpendapat informasi adalah salah satu jenis sumberdaya utama bagi manajer. Dalam pada itu Richard J. Hopeman (tujuan (Murdick, Ross, dan Claggett 1984) manajer mengelola lima jenis sumber daya utama, yaitu:

1) Manusia
2) Material
3) Mesin
4) Uang
5) Informasi (termasuk data)

Pendapat dari Kadir (2003) informasi tidak hanya digunakan untuk kepentingan internal organisasi, melainkan digunakan juga untuk kepentingan eksternal (diluar organisasi). Lebih lanjut dijelaskan oleh Kadir (2009) pemakai internal meliputi manajemen paling bawah sampai kepada majemen tingkat atas, sedangkan eksternal dapat berupa pelanggan, pemegang merchant, pemasok, mitra kerja, pegawai pajak, dan *stakeholder* lainnya yang terkait dengan organisasi tersebut (Simanjutak 2009). Apabila digambarkan dalam bentuk lingkaran, maka penulis mendeskripsikannya sebagai berikut:

Gambar 2

Kegunaan Informasi

Sumber: Penulis 2011

Mcleod (1998) berpendapat sebuah sistem dihubungan dengan lingkungan melalui arus sumber daya disebut dengan sistem tebuka (*open system*). Contohnya Sistem Transaksi elektronik pada mesin EDC *Merchant* Permata Bank, inputnya dapat melakukan transaksi dengan menggunakan mesin EDC dan menycdiakan persetujuan atau otorisasi untuk pembayaran di merchant Bank Permata. Sedangkan sistem yang tidak dihubungkan dengan lingkungannya disebut dengan sistem tertutup (*closed system*).

Gambar 3

Proses Informasi

Sumber: Mcleod 1998

Sementara Siagian (2005, hlm. 2) mengemukakan sistem informasi dilakukan melalui tujuh tahap. Yang terdiri dari: (a) pengumpulan data; (b) klasifikasi data; (c) pengolahan data supaya berubah bentuk, sifat dan kegunaanya menjadi informasi; (d) interprestasi informasi; (e) penyimpanan informasi; (f) penyampaian informasi atau transmisi kepada pengguna; dan (g) penggunaan informasi untuk kepentingan manajemen organisasi. Sekarang ini, pengembagan dan peningkatan atau inovasi informasi telah menggunakan terobosan teknologi, dalam hal ini adalah penggunaan komputer atau *end-using computer*. *End using computer* yang dimaksud adalah pengembangan seluruh atau sebagian dengan berbasis komputer (Raymond Mcleod 1988).

2.2.2 Transaksi Elektronik

Transaksi elektronik merupakan konsep baru di bidang perbankan yang ditawarkan kepada nasabah atau konsumennya untuk mempermudah jual beli barang atau jasa. Shim,Queresy, Siegel, dan Siegel (2001) yang dikutip Suyanto (2005) menjelaskan transaksi ekektronik atau *electronic commerce* (EC) menggambarkan proses jual beli barang atau jasa pada *world wide web internet*, atau Turba, Lee, King, Chung (2000) dikutip Suyanto (2005) menjelaskan EC merupakan proses jual beli atau pertukaran produk, jasa dan informasi melalui jaringan informasi termasuk internet. Sama halya dengan pendapat Golose (2008) EC merupakan transaksi melalui internet, yang merupakan proses komunikasi antar komputer melalui pertukaran data elektronik (*elektronic data interchange*).

Sedangkan Kalokota dan Whinston (1997) dikutip Suyanto (2005, hlm. 8) mendefinisikan EC sebagai berkiut:

a. Dari perspektif komunikasi, EC merupakan pengiriman informasi produk/ layanan, atau pembayaran melalui telpon, jaringan komputer dan sarana elektonik lainnnya
b. Dari perspektif bisnis, EC merupakan aplikasi teknologi menuju otomatisasi transaksi dan aliran kerja perumerchantaan.
c. Dari perspektif layanan, EC merupakan suatu alat untuk mememuhi keinginan perusahaan, konsumen dan manajemen dalam memangkas *service cost* ketika berupaya meningkatkan mutu barang dan kecepatan pelayanan
d. Dari perspektif online, EC meningkatkan kapasitas jual beli produk dan informasi internet dan jasa *online* lainnya.

Dari beberapa pendapat di atas, yang dimaksud transaksi elektonik oleh penulis adalah transaksi jual beli baik produk, informasi internet maupun jasa *online* lainnya yang dikembangkan oleh perbankan, dengan memanfaatkan sistem teknologi informasi jaringan internet untuk mempermudah atau memberikan pelayanan konsumen.

Transaksi elektronik merupakan sistem transaksi pembayaran yang diselenggarakan secara *online* yang dikelola sepenuhnya oleh layanan perbankan dengan memanfaatkan fasilitas serta jaringan internet yang dibangun dan dikembangkan oleh masing-masing bank. Sehingga para konsumen dapat memperoleh kemudahan dan keamanan dalam melakukan transaksi. transaksi pembayaran dengan memanfaatkan seluruh fasilitas yang disediakan bank, antara lain melalui *Autodebet*, *ATM*, *Phone banking*, dan *Internet Banking*, serta *Merchant*.

2.2.3 Toko (*Merchant*)

Toko atau *Merchan*t yang dimaksud dalam hal ini adalah orang perorangan, badan perusahaan, atau badan hukum yang menjalankan usaha di bidang penjualan barang dan jasa yang dapat menerima kartu pembayaran dengan menggunakan kartu kredit atau kartu debit. *Merchant* juga merupakan suatu bisnis bank untuk memberikan pelayanan kepada nasabahnya dengan menempatkan mesin *elektronic data capture* (EDC) dan atau *intepreter* ditempat usaha *merchant*.

Sedangkan mesin EDC adalah alat yang dipergunakan untuk transaksi yang terhubung secara *online* dengan sistem jaringan Bank. Sementara itu dalam bisnis merchant ini bank bertindak sebagai acquiring dari visa dan mastercard yang dapat menerima dan memproses transaksi yang dilakukan dengan menggunakan kartu plastik yang dikeluarkan oleh Bank.

2.2.4 Kartu Plastik

Kartu Plastik yang dimaksud dalam hal ini adalah semua jenis kartu yang diterbitkan bank atau penerbit (*Issuer*). Bank telah mengeluarkan beberapa kartu plastik yang dikeluarkan untuk calon nasabahnya, beberapa contoh kartu tersebut adalah Kartu *Automated Teller Machine* (*Card ATM*), Kartu Debit (*Debit Card*), Kartu Charge (*Charge Card*), dan Kartu Kredit (*Kredit Card*) (Bank Permata 2011). Lebih lanjut dijelaskan sebagai berikut:

a. Kartu ATM (*Automated Teller Machine*)

   Kartu yang diterbitkan oleh Issuer Bank kepada seseorang jika orang itu menjadi nasabahnya. Kartu ini bersifat tidak wajib, akan tetapi hampir seluruh nasabah mengharapkan untuk memperolehnya karena mendatangkan kemudahan akses atas berbagai fasilitas bank yang bisa dilakukan melalui mesin ATM. Sementara itu ATM berfungsi menarik uang tunai dan untuk melakukan berbagai transaksi pembayaran atau transfer setiap saat disejumlah ATM yang tersebar di segala tempat.

b. Kartu Cash (*Cash Card*)

   Kartu yang digunakan untuk menarik sejumlah uang baik di depan *Teller* Bank maupun di sejumlah ATM, bahkan pada sejumlah merchant. Sehingga kegunaannya lebih efektif dari pada Kartu ATM. Selain itu kartu ini juga berfungsi sebgai identitas diri jika tidak ditemukan mesin ATM maupun EDC Pada *Merchant*.

c. Kartu Debit (*Debit Card*)

   Kartu debit adalah kartu plastik yang dapat digunakan dalam transaksi yang dananya milik dari pemegang kartu sendiri. Penggunaan jenis kartu ini secara otomatis akan memotong saldo tabungan begitu dipergunakan untuk bertransaksi. Ditinjau dari daya penerimannya disejumlah *merchant*, kartu debit ada yang bersifat lokal, regional

ataupun internasional. Jenis lokal hanya dapat dipergunakan dinegara tempat bank didirikan dan dikota-kota tertentu. Jenis regional biasanya digunakan di negara-negara tertentu dan penerbit kartu juga buka umerchanta di Negara itu. Untuk jenis internasional dapat diterima di seluruh belahan dunia, misalnya kartu *visa Electron*, *MasterCard Electronic*, Maestro dan Cirrus.

d. Kartu Kredit (*Credit Card*)

Kartu plastik yang dipergunakan sebagai alat pembayaran transaksi, yang dananya merupakan fasilitas pinjaman dari penerbit. Pemilik akan dikenakan iuran tahunan yang besarnya ditetapkan bank. Kelebihan kartu kredit ini tidak harus membayar secara penuh jumlah tagihan ketika jatuh tempo karena boleh menyicil dengan jumlah minimal tertentu. Sisanya termasuk bunga ditagihkan pada bulan berikutnya.

e. Kartu Cas (*Charge Card*)

Charge Card ini mirip kartu kredit. Namun untuk mendapatkannya perlu syarat-syarat tertentu dan sulit. Karena begitu memiliki *charge card* diberikan kebebasan penuh untuk menggunakan dana dari bank yang tidak terbatas. Tentunya hal ini berbeda dalam setiap individu nasabah tergantung perhitungan sesuai kondisi *financial* masing-masing. Uniknya lagi kartu jenis ini tidak dikenakan bunga kepada mereka yang memilikinya, melainkan hanya *late charge* (biaya keterlambatan pembayaran). Penerbit akan memebrikan jangka waktu biasanya satu bulan untuk melunasi semua tagihan. Jika tidak bisa melunasi, bisa dengan cara menyicil, seperti pada kartu kredit. Dalam pada itu jika tidak bisa membayar penuh otomatis kartu akan diblokir sampai seluruh tagihan dilunasi.

Di bawah ini adalah contoh kartu plastik yang diterbitkan oleh Issuer Bank, sebagai berikut:

Gambar 4

Kartu Debit Tampak Depan

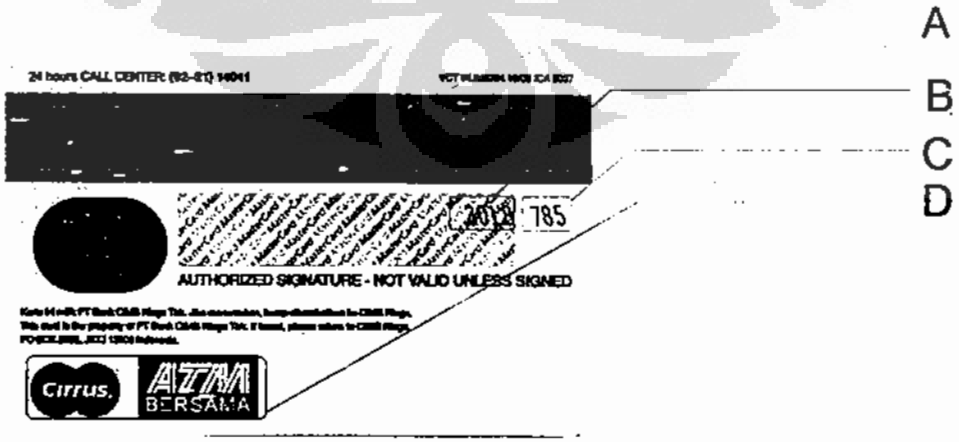
Sumber: Kartu Debit Cimb Niaga Syariah 2011

Keterangan:

a. Nama bank penerbit kartu kredit (*Issuer Card*)
b. Nomor kartu kredit yang berjumlah 16 digit
c. Bulan dan tahun nasabah (*customer*) menjadi pemegang kartu (*member since*)
d. Bulan dan tahun kartu kredit berlaku (*expired data*)
e. Logo jaringan kartu kredit (master card)

Gambar 5

Kartu Debit Tampak Belakang



Sumber: Kartu Debit Cimb Niaga Syariah 2011

Keterangan:

a. Pita magnetik penyimpanan data.
b. Nomor kartu kredit dan tempat pemegang kartu kredit tanda tangan.
c. Pada bagian belakang nomor kartu kredit ditambah tiga digit lagi nomor verifikasi
d. Logo jaringan ATM, biasanya tertera logo Alto, Cirrus, Plus.

Gambar 6

KARTU KREDIT TAMPAK DEPAN

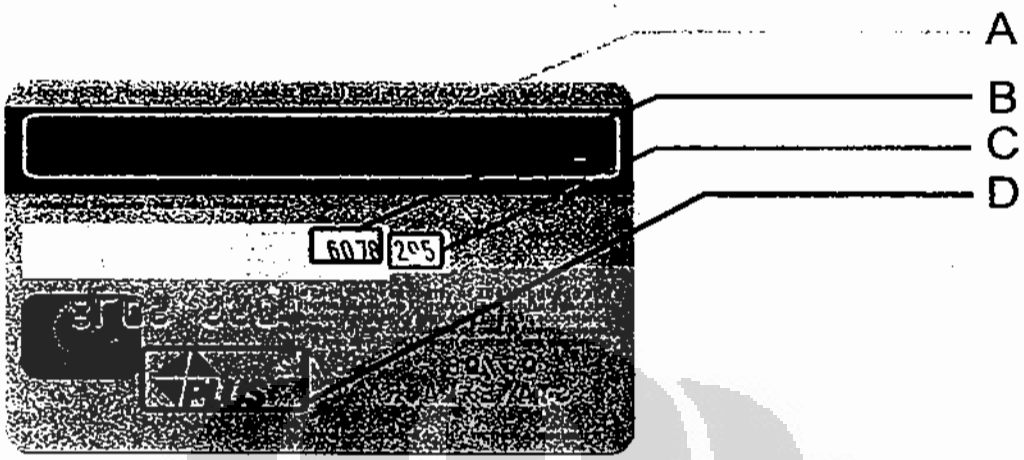
Sumber: Kartu Kredit HSBC 2011

Keterangan:

a. Nama bank penerbit kartu kredit (*Issuer Card*)
b. Chip penyimpanan data nasabah (*customer*), sebagai alternatif pita magnetik bila rusak.
c. Nomor kartu kredit yang berjumlah 16 digit
d. Bulan dan tahun nasabah (*customer*) menjadi pemegang kartu (*member since*)
e. Bulan dan tahun kartu kredit berlaku (*expired data*)
f. Nama Pemilik kartu
g. Logo jaringan kartu kredit (master card)

Gambar 7

Kartu Kredit Tampak Belakang



Sumber: : Kartu Kredit HSBC 2011

Keterangan pada gambar 7 ini sama dengan gambar 5.

Sementara itu pemilik kartu dalam istilah perbankan disebut dengan *Card Holder*. Artinya orang yang namanya atau nomor yang terdaftar di bank tersebut terletak pada kartu, yang mempunyai kewenangan penuh untuk menggunakan baik kartu kredit maupun kartu debet itu. Pemilik kartu dapat melakukan transaksi pada setiap *merchant* untuk membayar barang atau jasa setelah menggesekan kartu tersebut pada mesin EDC. Hal itu terjadi karena kartu debit atau kredit mempunyai chip, yaitu komponen elektronik yang dirancang untuk menjalankan fungsi penyimpanan dan pemrosesan data, dan pada EDC sendiri terdapat *chip reader*, yaitu EDC atau terminal yang mampu membaca dan mengkomunikasikan dan memproses data transaksi dari kartu *chip*.

Gambar 8

Mesin *EDC*

Sumber: Bank Permata 2011

Lebih lanjut dijelaskan tentang penggunaan EDC, yang sering disebut juga sebagai mesin gesek. Untuk menggunakan mesin EDC ada dua cara, yaitu kartu yang menggunakan pita magnetik (*magnetic stripe*) dan yang sudah menggunakan *chip*. Sedangkan cara mengopersionalkannya kartu yang menggunakan pita magnetik adalah sebagai berikut:

a. Mesin EDC sebelum digunakan harus dalam kondisi on atau koneksi LAN baik melalui jaringan telepon ataupun *wireless*.
b. Kartu digesek sekali dari atas ke bawah pada EDC
c. Setelah digesek akan muncul data kartu pada layar (display).
d. Bila nomor kartu kredit tersebut cocok maka masukkan nomunal transaksi yang dikehendaki atau yang akan dibayarkan
e. Tekan enter

Sementara itu untuk kartu yang menggunakan chip atau *europe mastercard Visa* (EMC) langkahnya hampir sama, hanya saja mengoperasionalkannya dengan cara *digital image proccsesing*, untuk selanjutnya disebut DIP:

a. Masukan (*Insert card*) pada mesin EDC.
b. Pada layar display muncul data kartu kredit.
c. Bila cocok nomor kartu kreditnya, masukkan nominal transaksi.
d. Tekan Enter.
e. Cabut kartunya.

2.2.5 *Cyber Crime*

Cybercrime tidak mudah didefinisikan. Menurut Golose (2008,25) *Cyber crime* adalah "kegiatan illegal dengan perantara komputer yang dapat dilakukan melalui jaringan elektronik global." Sedangkan Sipior dkk (2003) mengemukakan "kegiatan kriminal yang melibatkan penggunaan satu atau lebih komputer." Dari kedua definisi tersebut, sebenarnya dalam kejahatan komputer, harus bisa membedakan mana kegiatan yang hanya mengganggu aktivitas komputer, mana yang melanggar hukum. Lebih lanjut Sipior dkk menjelaskan biasanya kejahatan ini, dalam bentuk penipuan; pencurian; penghancuran; gangguan; konspirasi. Lebih jelasnya sebagai berikut :

a. Penipuan adalah informasi yang keliru. Tujuan akhir dari penipuan adalah mendapatkan uang atau beberapa jenis keuntungan tertentu

lainnya, atau dapat memberikan keuntungan yang lebih umum untuk si pelaku.

b. Pencurian adalah jenis kejahatan komputer yang paling dikenal, bahkan, pencurian identitas telah menjadi sebuah kata rumah tangga. Pencurian tidak banya terbatas pada jenis ini, namun. Pencurian yang berkaitan dengan komputer juga dapat mencakup pencurian dana, pencurian informasi, pencurian properti fisik, atau pencurian kekayaan intelektual.

c. Kehancuran adalah salah satu yang paling dikenal sebagai salah satu bentuk kejahatan komputer. Sebagian besar kerusakan dalam keamanan informasi komputer virus dan jenis *malware* lainnya. Ancaman *malware* merupakan salah satu yang paling merusak dan mahal di bidang kejahatan komputer karena ancaman malware keduanya banyak dan beragam. Walaupun virus, Trojan, worm, dan jenis malware lainnya memiliki definisi tertentu (tergantung cara mereka disebarluaskan dan menyebar), semakin banyak ancaman malware diklasifikasikan sebagai ancaman *multivector* atau dicampur, karena mereka memiliki karakteristik lebih dari satu jenis spesifik.

d. Gangguan dapat terfokus (terhadap individu-individu tertentu atau terhadap perumerchantaan tertentu), atau mungkin relatif *unfocussed* dan target masyarakat luas. Jenis yang paling umum dari gangguan dalam kejahatan komputer adalah serangan *denial of service* (DoS). Serangan jenis ini biasanya melumpuhkan atau sistem *crash* dengan mengirimkan sejumlah besar lalu lintas jaringan sedemikian rupa sehingga tidak dapat memproses permintaan merchant, atau serangan dengan menggunakan serangkaian datagrams yang dibuat untuk mengeksploitasi kerentanan layanan yang diketahui atau hanya mengisi sistem disk.

e. Konspirasi merupakan salah satu yang paling sedikit dipahami pada kejahatan komputer. Di tingkat konseptual, sebuah konspirasi hanya perjanjian antara dua atau lebih individu untuk melakukan tindakan ilegal. Secara hukum, konspirasi telah diperluas untuk mencakup

perjanjian dan konsultasi, serta tindakan yang ilegal atau merugikan baik kepada masyarakat atau individu tertentu. Kejahatan jenis ini bisa menjadi kejahatan komputer setiap kali komputer, jaringan, sistem *e-mail, chat room*, pesan instan agen, dan sistem lain yang digunakan untuk memfasilitasi semacam kesepakatan atau konsultasi.

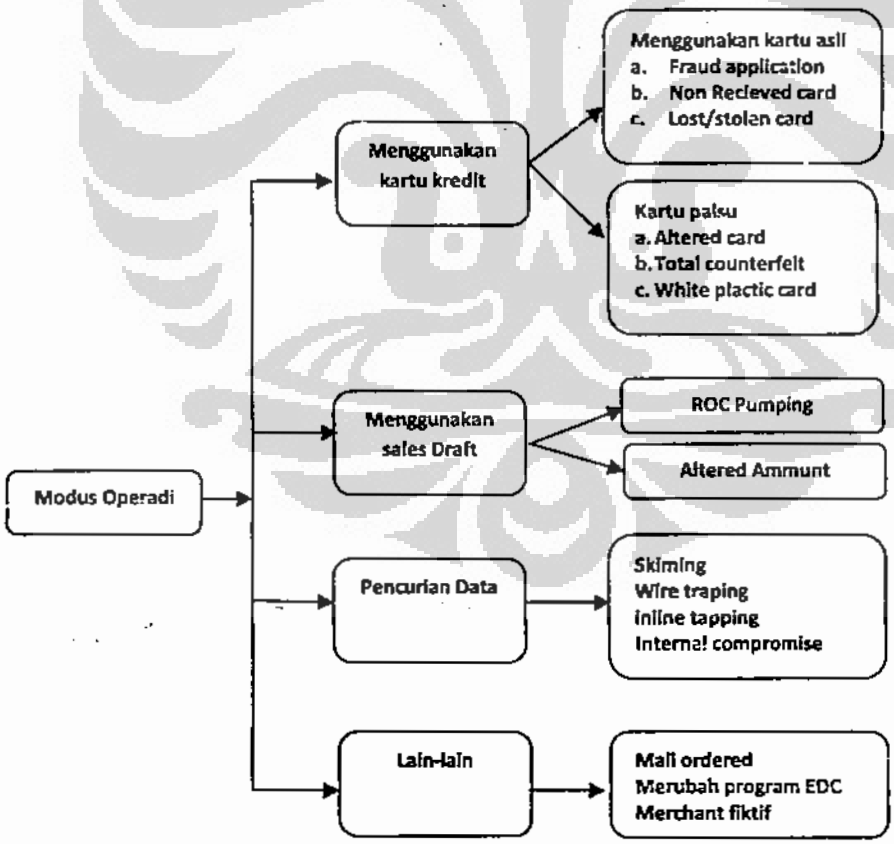
Kelima bentuk kejahatan tersebut, bukan kejahatan konvesional seperti biasanya, melainkan sudah menggunakan Teknologi Informasi. Nitibaskara (Golose 2008, 27) mengemukakan karateristik *cyber crime* dibanding tindak pidana lain, " (1) penggunaan TI dalam Modus Operandi; (2) korban dapat menimpa siapa saja mulai dari perorangan sampai negara;(3) besifat tanpa kekerasan; (4) karena tidak kasat mata *fear crime* (ketakutan atas kejahatan) tidak mudah timbul." Sedangkan menurut Pike (2006) kejahatan ini termasuk adalam *organized crime*, yaitu "kegiatan llegal dilakukan oleh satu orang atau lebih dibantu oleh kejahatan yang mempunyai keahlian khusus sesuai dengan kebutuhan. Kadang-kadang organisasinya mempunyai hirarki dan manajemen, dan biasanya kegiatan illegal yang mereka lakukan telah direncanakan dari awal." Lebih lanjut Pike (2006) menjelaskan bahwa Kejahatan terorganisir tersebut, sebenarnya masih dalam tahap awal. Orang yang memiliki keahlian dalam kriminal tersebut, biasanya merekrut orang yang memiliki keahlian, sehingga kejahatan ini cukup cerdas, dan pimpinannya sangat ingin memanfaatkan teknologi baru, dalam hal ini komputer.

Menurut Pike (2006) ada dua tipe dasar dari kejahatan komputer, yang paling menonjol adalah pemakaian oleh orang yang tidak berhak dan penipuan. Lebih lanjut Pike (2006) menjelaskan pemakaian oleh orang yang tidak berhak adalah memodifikasi komputer atau merubah sistem yang bukan hak mereka. Hal tersebut di atas biasanya digunakan untuk pemerasan, pencurian, memata-matai perumerchantaan, dan biasanya pelaku tidak perlu memakai sistem perumerchantaan tersebut. Sehingga mengakibatkan tercurinya informasi, misalnya informasi *credit card* yang bisanya mempunyai nilai dalam pasar gelap (*black market*) atau informasi tentang *custumer* dan produknya yang bisa dijual kepesaing, dan memasukan data yang merusak sistem, meskipun sudah ada *back tapes*, sehingga dapat merugikan *financial* perusahaan.

Sedangkan penipuan bisanya terjadi dalam beberapa bentuk. Misalnya berpura pura memesan barang tertentu kepada perusahaan. Padahal itu adalah dilakukan penjahat, dan biasanya korban harus bertanggung jawab hutang atas nama mereka, dan penyalahgunaan kartu kredit: pelaku memperoleh akses terhadap satu sistem *online* yang dimiliki Bank yang merubahnya sehingga pelaku dapat masuk dengan leluasa ke sistem transaksi elekronik melalui mesin *EDC* di *merchant* bank penerbit. Hal ini yang disebut dengan *fraud banking* atau penyalahgunaan kartu pada bisnis perbankan yang merupakan tindak kejahatan. Jika merujuk pada Surat Keputusan Kapolri No. Pol: Skep/507/VII/1998 tentang Buku Petunjuk Lapangan Penyidikan Yang Berhubungan Kartu Kredit, bentuk dan cara penyalahgunaan kartu kredit atau debit dapat lihat dalam bagan sebagai berikut:

Gambar 9

Modus Operandi Penyalahgunaan Kartu



Sumber: Surat Keputusan Kapolri No. Pol: Skep/507/VII/1998

Modus operandi kejahatan tersebut dapat dijelaskan sebagai berikut:

a. *Fraud Application*: pelaku kejahatan memalsukan data seperti KTP, pasport, rekening koran, surat keterangan penghasilan, dan memohon kepada bank penerbit untuk mengajukan kartu kredit. Selanjutnya setelah diterima sebagai pemegang kartu kredit mengadakan transaksi berkali-kali yang nilainya semakin besar. Kemudian menghilang tanpa memnuhi kewajibannya membayar kartu kredit.

b. *Non Received Card*: modus ini terjadi karena peluang yang berikatan dengan pengiriman kartu kredit, dimana kartu kredit yang dikirim penerbit tidak sampai kepada pemegang merchant, dan digunakan oleh orang yang tidak berhak.

c. *Stolen Card*: pelaku menggunakan kartu yang hilang atau curian dengan jumlah di bawah *floor limit* dan meniru tanda tangan pemilik kartu.

d. *Alterd Card*: pelaku menggunakan kartu asli hasil curian atau penggelapan kemudian kartu tersebut reliefnya dipanaskan lalu diratakan. Setelah rata relief tersebut dicetak ulang dengan data baru (*embosed*), sedangkan *magnegtic stripe* diisi dengan data baru (*re-encoded*), data itu didapat dari *point of compromise* (oknum pedagang, oknum bank, dan lain lain).

e. *Totally counterfeit*: pelaku mencetak dan membuat kartu tiruan bergambar atau logo fisik 100 % palsu, dibubukan data nomor dan nama pemegang kartu yang masih bonafid dan valid, hal ini dilakukan dengan cara mencetak ulang data baru (*embosing*) dan memasukan data baru pada *magnegtic stripe* (*ecoding*).

f. Kartu Plastik Polos (*White Plastic Card*): nomor-nomor yang tercetak timbul pada kartu dicatat lalu dicetak pada kartu plstik polos seukuran kartu kredit asli, tanpa *login* dan tanda visual lainnya, selain itu *magnegtic stripe* dibalik kartu diisi pemegang kartu dengan cara *ecodin*g.

g. *Record of Charge Pumping*: oknum pedagang melakukan pencetakan *sales draft* lebih dari satu kali, selanjutnya *sales draft* hasil penggandaan dijual atau diserahkan kepada oknum *merchant* lainnya untuk diisi dengan data transaksi fiktif kemudian dibubuhi tanda tangan dengan meniru tanda tangan pemegang kartu yang syah.

h. *Altered Amount*: modus ini terjadi dimana oknum pedagang mengganti nilai nominal yuang tercantum pada *sales draft* dari kartu yang digunakan dalam transaksi di tokonya.

i. *Internet atau Mail Order*: pelaku melakukan pemesanan suatu barang melalui surat atau *telephone* dengan memberikan kartu pemegang kartu kredit. Modus ini terjadi karena mengetahui data pemegang kartu baik nama dan nomornya, kemudian pelaku bertindak seolah-olah sebagai pemegang kartu yang syah.

j. Mengubah atau merusak mesin EDC: modus ini dapat terjadi karena oknum pedagang merusak atau mengubah program alat otorisasi EDC milik pengelola yang dititipkan atau dipinjamkan kepada *merchant*, alat ini direkayasa (*clone*) agar dapat dilakukan otorisasi atau dioperasikan tanpa ada kartu kredit secara fisik.

k. *Fictitious Merchant*: pedagang mengajukan untuk *merchant* di bank pengelola dengan data palsu, kemudian melakukan transaksi seolah-olah terjadi transaksi di tokonya. Modus ini berhasi karena pelaku melakukan teknik:

   1) Split Change: cara memecah transaksi untuk menghidari otorisasi atau jumlah minimal belanja tidak melebihi *floor limit*;

   2) Common Purchases Point: tempat-tempat dimana data pemegang kartu disalin atau dicuri selanjutnya diberikan kepada sindikat kartu kredit.

l. Pencurian Data: teknik penyadapan data pemegang kartu teridiri dari

   1) *Generate Account*: cara untuk mendapatkan data nomor-nomor kartu kredit dengan menggunakan *software* tertentu yang dirancang secara khusus;

   2) *Phantom terminal*: cara melakukanya dengan menguji kartu kredit yang didapat dari sumbernya, termasuk dari *generate account*;

   3) *Skiming*: pencurian seluruh data pemegang kartu kredit yang terdapat dalam pita magnet kartu kredit secara elektronik, kemudian dipindahkan ke kartu yang hilang atau dicuri;

4) *Inline tapping*: pencurian data melalui kabel telepon yang tersambung dengan EDC;
5) *Wire tapping*: pencurian fatra melalu jalur atau line komunikasi antar teminal EDC dengan sistem yang ada pada akuisisi bank untuk mendapatkan data pemengang kartu.

2.3 Kepustakaan Teori

2.3.1 Teori Triad atau CIA

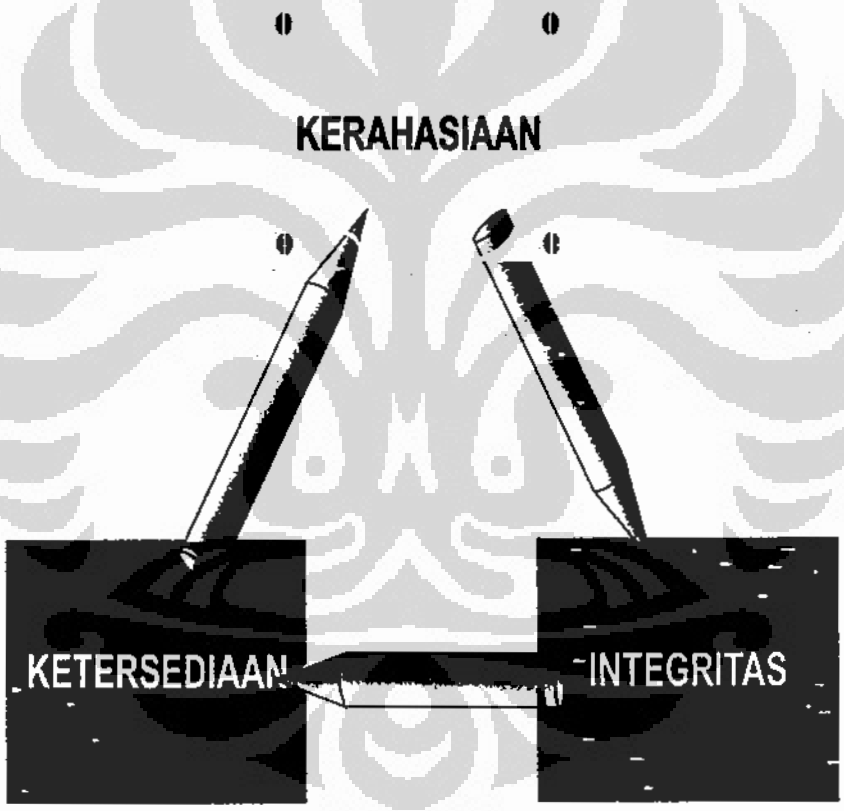
Prinsip yang utama sistem informasi harus dapat mengidentifikasi pengguna, mengisolasi sumberdaya, dan kegiatan pemantauan secara umum atau universal terdahadap masalah perlindungan, dalam hal ini adalah manajemen keamanan sistem informasi (Hacker 2000). Manajemen keamanan sistem informasi merupakan suatu manajemen atau pengelolaan yang komprehensif meliputi pengaman terhadap aset perusahaan dengan menggunakan metode atau cara pegumpulan, analisis, melaporkan kegiatan terhadap yang dianggap berbahaya bagi perumerchantaan (Mcbride 2006). Seperti adanya kemungkinan kelamahan-kelemahan baik yang bersumber dari manusia (karyawan), administrasi, sistem dan lain sebagainya. Informasi yang berada di dalam dan luar lingkup perusahaan harus dilindungi di manapun. Keamanan informasi harus dievaluasi seperti proses bisnis dengan menentukan berapa banyak keamanan yang dibutuhkan untuk melindungi aset informasi perusahaan.

Sistem informasi saat ini merupakan sumberdaya penting, mempunyai nilai strategis dan mempunyai peranan penting sebagai daya saing, kompetensi utama dan keberlangsungan hidup suatu organisasi. Walaupun kemudahan dan keuntungan dijanjikan pada setiap implemetasi dan pengembangan suatu sistem informasi, namun dibalik semua itu harus disadari tanpa manajemen pengamanan sistem informasi akan menjadikan atau menempatkan sistem informasi semakin rentan dan berpotensi ancaman (*threats*). Sehingga menjadi prisip dasar dalam pengelolaan sistem informasi yang harus diimbangi dengan perhatian serius terhadap keamanan sistem informasi. Karena keamanan sistem informasi merupakan salah satu bagian yang penting untuk pengelolaan sistem informasi.

Menurut Ken M. Shaurette (2006) cara mudah untuk menentukan berapa banyak risiko yang kita miliki dan apa dampaknya sehingga kita dapat membuat dengan mengelola risiko, meliputi tiga aspek yaitu prinsip integritas (*integrity*), kerahasiaan (*confidentiality*) dan ketersedian (*availability*), yang dikenal dengan teori Triad atau CIA. Ketiga aspek tersebut harus saling terkait dan sinergis satu sama lainnya, agar tujuan dari keamanan jaringan informasi tercapai dan mencegah kerugian dari sebab apapun (Hadiman 2010). Tiga aspek tersebut dapat digambarkan dan dijelaskan sebagai berikut :

Gambar 10

Teori CIA



Sumber: Ken M. Shaurette (2006) dikembangkan penulis.

I : *Integrity* adalah menjaga keakuratan dan kelengkapan informasi serta cara memproses informasi tersebut.

C: *Confidentiality* (nilai tinggi) adalah mengutamakan kerahasian agar memiliki nilai tinggi, yaitu dengan memastikan bahwa informasi hanya dapat diakses oleh orang-orang yang benar-benar berhak

A: *Availability* (ketersedian) adalah menjamin ketersedian data atau informasi pihak yang berwenang dapat mengakses data yang akurat pada saat dibutuhkan.

Selanjutnya ketiga aspek tersebut menjadi penting karena seiring dengan perkembangan pengetahuan dibidang informasi dan teknologi telah menjadikan beranekaragamnya bentuk informasi. Adapun bentuk informasi tersebut misalnya *Computer Based Information*: Penciptaan informasi dengan menggunakan komputer, memuat tentang komunikasi surat lewat *email*, penyimpanan administrasi kantor, hal tersebut berpotensi bagi kerawanan keamanan jaringan informasi *formal document*: produk tertulis dari suatu perusahaan dalam bentuk rencana anggaran, strategi, dan lainnya, yang rawan juga akan kebocoran. Maka dengan stategi CIA yang sinergis dan terkait satu sama lainnnya akan mencegah kebocoran, penyalahgunaan wewenang, pencurian internal maupun dari pihak luar.

Lebih lanjut dijelaskan Mcbride (2006) organisasi yang menggunakan pendekatan ini akan mendapatkan manfaat penting, yang dapat dikelompokan di bawah ini.

a. Perbaikan keamanan sistem informasi
b. Pengurangan dampak bisnis yang kurang baik, sebagai contoh gangguan dan kerugian keuangan yang disebabkan oleh suatu insiden sistem informasi
c. Penguatan fokus dari pencegahan keamanan informasi
d. Penguatan prioritas dan bukti
e. Memberikan konstribusi terhadap justifikasi anggaran dan sumberdaya.
f. Penyediaan masukan untuk kebijakan keamanan informasi dan tinjauan terhadap dokumentasi terkait.

2.3.2 Manajemen Keamanan Sistem Informasi

Sistem informasi merupakan sumber daya utama organisasi, maka harus dikelola dengan menggunakan sistem pengamanan informasi yang baik. Jika infromasi tidak dikelola dengan baik, kecenderungan atau berdampak disalahgunakan atau diselewengkan penggunaannya oleh seseorang atau

kelompok orang, dapat mendatangkan bencana bagi suatu organisasi atau perusahaan. Seseorang akan hilang pekerjaan, masyarakat dan organisasi akan dirugikan. Sehingga untuk mencegah hal itu diperlukan pengamanan terhadap informasi secara efektif dan efisien dengan menggunakan manajemen pengamanan.

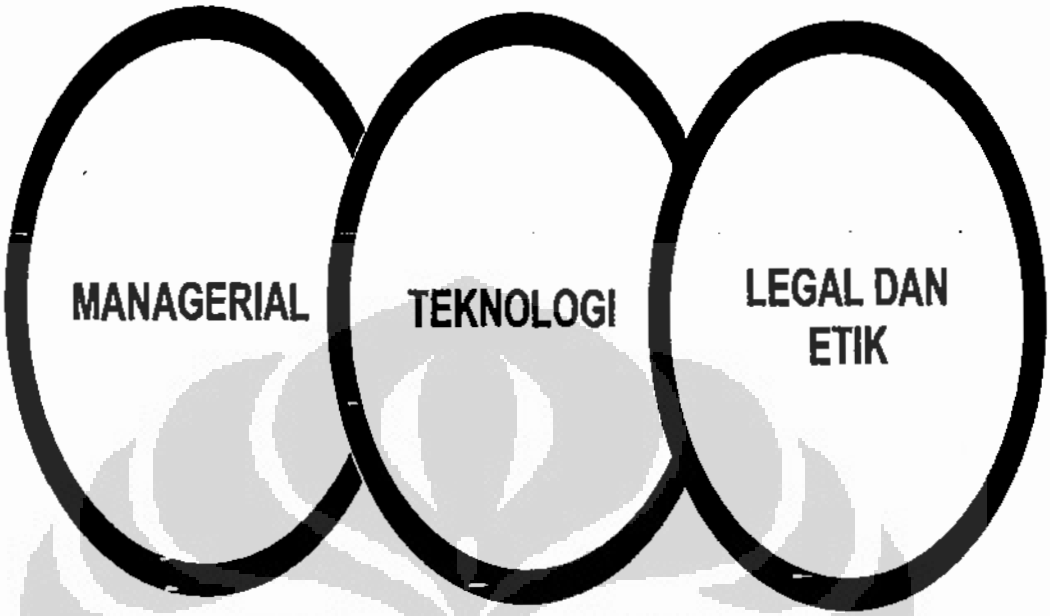
Green dan Fischer (1998, hlm. 3) mendefinisikan keamanan "*security implies stable, relatively predictable environment in wich an individual or group may pursue its ends without disruption or harm and without fear of disturbance or injury.*" Artinya Keamanan merupakan keadaan lingkungan yang stabil sehingga individu atau kelompok dapat mengejar tujuannya tanpa gangguan atau kejahatan dan terbebas dari rasa takut akan bahaya atau yang dapat mencederai. Pendapat dari Mcrie (2001, hlm. 5) "*security is defined as the protection of asset lost*". Artinya keamanan atau sekuriti merupakan perlindungan terhadap kehilangan aset. Sedangkan sekuriti dalam proses bisnis didefinisikan oleh Hacker (2000, hlm. 14) berikut ini.

> *Security is the process of reducing risk or the likelihood of harm, security tends to be a weak link problem. Where the total security is no better than the weakcst point in the organization. Security therefcre must be evaluated broadly across the entire organization to understand where these weal links may be.*

Kaitannya dengan pengamanan sistem informasi adalah proses untuk mengurangi risiko atau kemungkinan bahaya, karena suatu sistem infomasi mempunyai titik lemah yang harus terus dievaluasi untuk menghindari kehilangan asset. Merujuk pendapat Price (2006), sistem informasi yang dimaksud dalam hal ini adalah komposisi dari orang atau sekelompok orang (sumber daya manusia dalam organisasi), proses dan produk. Untuk menguatkan pendapat tersebut Suryadi (2010) mengemukakan pengamanan sistem informasi terdiri dari tiga komponen yaitu manajerial, teknologi, legal dan etik.

Gambar 11

Tiga Komponen Sistem Manjemen Pengamanan Informasi



Sumber: Suryadi 2010

Manajerial berisi tentang konsep kebijakan manajemen pengamanan yang mempuyai perencanaan, pengorganisasian, pelaksanaan dan pengedalian. Teknologi melakukan perawaratan , peningkatan kualitas teknologi, dan validasi dengan dukungan anggaran yang memadai. Legal dan etik merupakan perangkat peraturan atau standar pengamanan yang dimiliki oleh suatu organisasi. Namun Suryadi (2010) mengemukakan bahwa hal itu harus mempertimbangkan faktor manusia, proses dan teknologi.

Berdasarkan uraian di atas sistem pengamanan informasi merupakan stategi atau kebijakan pengamanan dengan menggunakan teknologi muktahir agar sumberdaya informasi tetap terjaga untuk kelangsungan bisnis. Dalam penelitian ini manageuen pengamanan sistem informasi ini meliputi sumberdaya manusia yang memanfaatkan informasi, data, sistem atau teknologi informasi dalam hal melakukan transaksi elektronik.

Sebagaimana secara teoritis menurut pendapat Wiliam Stalling dikutip Mcleod (1998) manajemen keamanan sistem informasi menitikberatkan kepada:

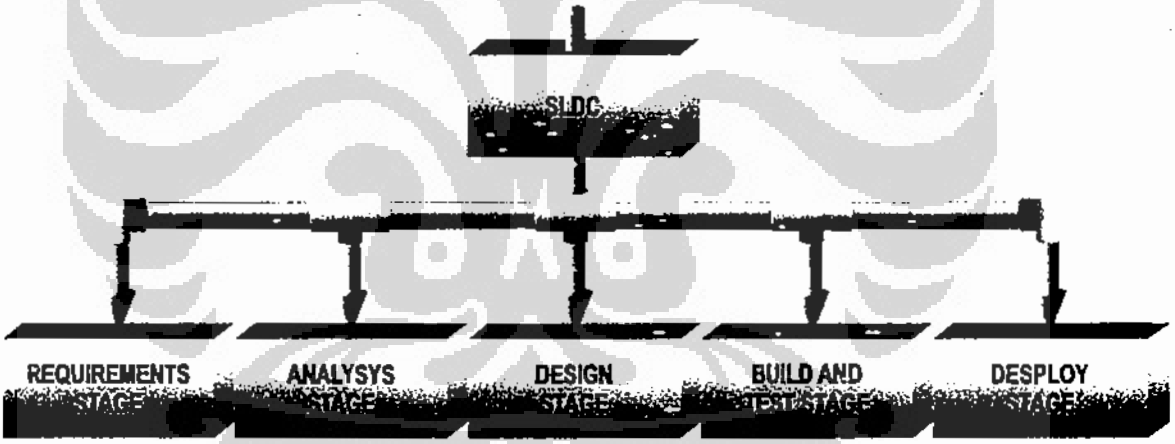
a. Keamanan jaringan tergantung dari kekuatan dari jaringan yang terlemah.
b. Penerapan kebijakan dan prosedur pada sebuah jaraignan

c. Implementasi teknologi untuk dan teknik yang digunakan untuk mengamankan jaringan.

Berdasarkan hal itu maka manajemen keamanan informasi harus memiliki *System Development Security Lifecycle* (SDLC). SDLC secara teoritis dikemukan oleh *Lim and Bazavan* (2006) adalah suatu proses pengembangan yang memberikan kepastian terhadap proses pengembangan agar terencana dan dapat digunakan berulang kali. Lebih lanjut dijelaskan oleh *Lim and Bazavan* (2006, hlm. 309-324) SDLC biasanya mencakup tahapan tahapan yang membatu dalam pengajuan untuk mendapatkan persetujuan, menentukan kebutuhan, mendesain, membuat, melakukan testing, mengembangkan dan memelihara suatu sistem. SDLC ini apabila dibuat dalam bentuk bagan adalah sebagai berikut:

Gambar 12

SDLC



Sumber: Ian Lim and Ioana V. Bazavan 2006 yang dikembangkan penulis

a. Tahap persyaratan (Requirements Stage): objek dari tahap pesyaratan ini adalah sebagai berikut:
   1) Memperkirakan persyaratan keamanan informasi dari persyaratan bisnis;
   2) Menentukan ketentuan keamanan yang dapat digunakan, standarisasi dan kebijakan antar organisasi.
   3) Menentukan peraturan yang dapat digunakan untuk keperluan audit.
   4) Membuat dan menghasilkan persyaratan keamanan

b. Tahap Analisa (*Analysis Stage*): membuat semua dari realitas kedalam kata-kata yang ideal dari persyaratan. Tim proyek harus menentukan kelangsungan desain dari implementasi persyaratan keamanan, dan menyesuaikan dengan batasan anggaran, tenaga, dan waktu. Secara urutan lingkup akhir harus ditentukan menjadi : hasil proyek, ketepatan waktu, titik poin, anggaran dan tenaga yang harus diidentifikasi, dan perencanaan sistem keamanan harus dibuat sebagai kesatuan didalam proyek SDLC secara keseluruhan. Yaitu:
   1) Mengidentifikasi biaya dan resiko;
   2) Analisa resiko versus biaya;
   3) Mengidentifikasi Ruang Lingkup Keamanan dan Menyelesaikan Syarat- syarat Keamanan harus memenuhi:
      (1) Evaluasi kebutuhan sumber daya;
      (2) Perencanaan proyek keamanan;
      (3) Dokumen jalan keluar terhadap resiko yang ada.
c. Tahap Desain (*Design Stage*):
   1) Bagaimana komponen komponen dari keamanan dibuat dan dimasukan kedalam keseluruhan desain sistem.
   2) Menetapkan kondisi lingkungan untuk mengembangkan keamanan.
   3) Melakukan seleksi terhadap kemampuan vendor.
   4) Membuat contoh-contoh desain dan penyelesain keputusan terhadap penyelenggaraan barang dan jasa.
   5) Memformulasikan rencana pengujian keamanan
   6) Melewati sertifikasi *check point*.
d. Tahap Uji Coba dan Pengembangan Sistem Pengamanan (Build and Test Stage): urutan-urutan fungsi yang digunakan sering mengandung kekurangan dan yang dapat di eksploitasi dengan cara:
   1) Membuat daftar tuntutan: Pendekatan yang masuk akal untuk melakukan uji coba harus dimulai dari membuat dari daftar tuntutan. Dibuat dengan mengidentifikasi hubungan yang relevan dari komponen komponen kemanan, meninjau kembali syarat keamanan dan dokomentasi desain, mengidentifikasi kondisi lingkungan yang

sesuai dengan sistem keamanan dan dapat dilakukan pengujian. Contoh pergantian pasword yang tersedia untuk pengguna.

2) Membedakan perbedaan tipe pengujian:
   (1) Prosedur dari pegujian kemanan dapat dibedakan dari beberapa tipe tes;
   (2) Uji coba komponen untuk memvalidasi paket, penggunaan ulang, modifikasi testing komponen kemanan.
   (3) Integrasi uji coba untuk memvalidasi fungsi *security* dalam uji integrasi dan produk.
   (4) Jumlah testing untuk memastikan bahwa sistem akan memproses data melalui batasan fisikal dan logika.
   (5) Pengujian yang ketat untuk memastikan transaksi yang efektif setelah sistem dimatikan.
   (6) Uji data *recovery* untuk menyelidiki kemampuan data *recovery* dan sistem *restart* dari kegagalan dan duplikasi.
   (7) Uji keamanan *data base* untuk memastikan akses tidak diberikan pada pihak luar.
3) Menekankan pelaksanaan *coding* yang aman dan membuat komponen- komponen Pengamanan: Pembuat *software* harus dididik dengan terbiasa mengamankan coding untuk menjamin bahwa hasil akhir akan memenuhi fungsi dari syarat keamanan.
4) Enkripsi dan membuat nomer secara acak :
   (1) Kriteria cukup acak untuk menghidari pola dan kedekatan;
   (2) Harus memiliki priode yang besar;
   (3) Tidak Membuat strings yang di sukai, seperti 010101;
   (4) Merupakan algoritma yang sederhana dan performa yang baik;
   (5) Tidak akan memberitahu beberapa *output* yang bisa memprediksi *output* masa lalu dan masa akan datang;
   (6) Memiliki peryataan internal yang cukup besar dan tidak bisa di prediksi untuk mencegah hasil pencarian
5) Validasi input dan pemeriksaan pengecualian: selalu memvalidasi masukan (pengguna dan aplikasi) biasanya kelemahan sistem beberapa

tahun disebabkan dari lemahnya dari kesalahan dari validasi input atau kesalahan terhadap prosess pengecualian.

6) Otentikasi: kekuatan otentikasi puncak dari keamanan aplikasi dan sistem dikarenakan kontrol keamanan yang lain seperti: otorisasi, enskripsi, audit, berdasarkan pada identifikasi dari otentifikasi dari pengguna.

7) Autorisasi: di dalam membuat model otorisasi sangat kritikal untuk memformulasikan kekuatan dari link dalam mengidentifikasi melalui siklus hidup dari sesi otentikasi. Hal ini sangat penting pada penerapan web aplikasi atau sistem *multi layer*, yang biasanya identitas sangat berhubungan dengan konteks lain.

e. Tahap Penyebaran (*Deploy Stage*): tahap ini adalah migrasi pengembangan keamanan produksi memastikan dan menjaga kerahasiaan, integritas, dan ketersediaan lingkungan produksi.

1) Dokumen mitigasi risiko secara menyeluruh adalah dokumen hidup yang dibuat di dalam fase analisa dan di perbaharui melaui proses SDLC untuk menelusuri risiko informasi keamanan. Dokumen mitigasi risiko secara komplit harus di selesaikan sebagai bagian dari proses sertifikasi.

2) Kerangka sertifikasi untuk memastikan kelangsungan dan perbaikan dari dasar organisasi keamanan informasi. Objeknya adalah:

(1) Memastikan interprestasi yang benar dari peraturan dan standar keamanan.

(2) Analisa dan mengelola resiko melalui siklus kemampuan mengembangkan siklus hidup

(3) Memformulasikan konfirmsi dari komplain untuk pengaturan dan standar keamanan

(4) Memformalisasi pemberitahuan dan tanda terima dari resiko keamanan informasi.

(5) Memfasilitasi resolusi, usulan alternatif, dan aturan untuk mencapai komplain.

(6) Otorisasi dan menulusuri surat pernyataaan melepaskan tuntutan dan penundaan .

(7) Inisial Peninjauan kembali Sertifikasi dilakukan setelah fase persyaratan , analisa, dan desain.

(8) *Check point* pemeriksaan Sertifikasi: sertifikasi *chek point* dilakukan setelah fase desain dan sebelum fase pembuatan dan pengujian. Maksud dari *check point* ini untuk membuat chanel komunikasi, dan membuka masukan antara sertifikasi tim dan *project* tim selama fase desain.

(9) Analisa kegagalan: tujuan dari sertifikasi dari analisa kegagalan adalah untuk melakukan uji coba dan mengidentifikasi area yang tidak standar sebelum pengembangan.

Selain itu, ada juga sistem atau bentuk untuk mengendalikan TI yang disebut dengan Cobit. Menurut Brand dan Boonen (2007) Cobit ini mendukung pengendalian TI yang baik dengan menyediakan penjelasan yang komperehensif mengenai tujuan pengendalian proses TI dan menawarkan kemungkinan penilaian atas suatu proses untuk memahami, mendapatkan, dan mengatur resiko serta keuntungan yang berhubungan dengan sistem informasi dan TI dalam proses bisnis.

ISACA dalam Brand dan Boonen (2007) menjelaskan Cobit ini tujuan atau target utamanya adalah kelompok atau grup *manager*, *end user*, dan *auditor*. Manager dalam organisasi merupakan orang yang bertangung jawab dalam pengoperasian perumerchantaan, yang membutuhkan informasi untuk mengendalikan operasi dan mengarahkan proses bisnis. Karena TI terkait dengan operasional bisnis yang membantu manajer untuk menyeimbangkan risiko, mengendalikan dan mengamankan investasi bisnis.

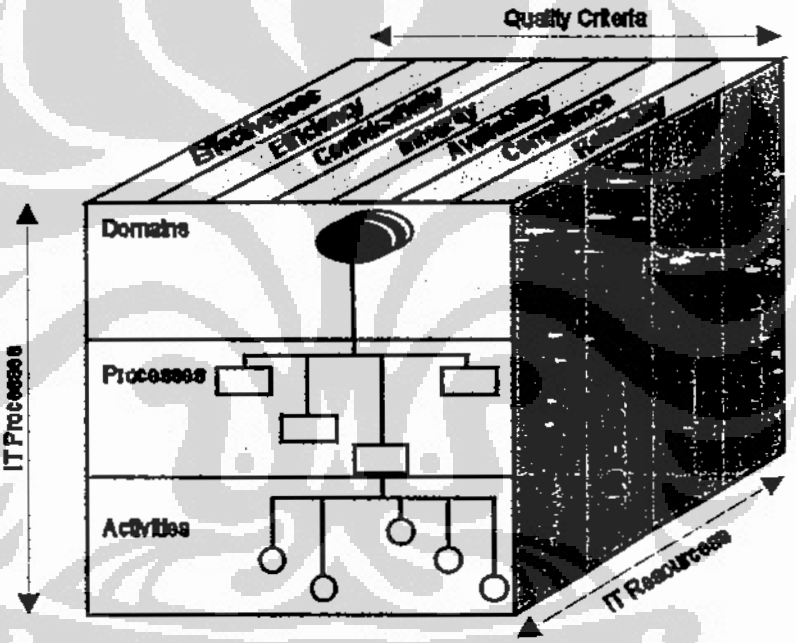
Sedangkan *end user* yang dimaksud dalam hal ini, menyadari bahwa suatu organisasi perumerchantaan harus memiliki layanan TI yang baik, yaitu tanggung jawab dalam proses kepemilikan bisnis, termasuk dalam layanan TI yang didelegasikan kepada penyedia layanan baik internal maupun eksternal organisasi. Cobit ini menawarkan suatu sistem untuk menjamin keamanan dan pengendalian dari layanan TI yang disediakan dari pihak dalam maupun luar. Sementara auditor

merupakan suatu badan atau lembaga penyedia jaminan yang mandiri dari kualitas dan kendali yang dapat diaplikasikan. Cobit dapat membatu auditor untuk menstrukturisasi dan mensubstansi serta memberikan saran kepada manajemen dalama rangka meningkatkan kontrol internal.

Selanjutnya Brand dan Boonen (2007) mengemukakan Cobit memiliki 3 pandangan yang berkait. Pandangan tersebut dijelaskan dalam bentuk struktur berikut ini.

Gambar 13

Cobit Structure



Sumber: Brand dan Boonen (2007, hlm. 25)

Proses TI dalam COBIT terbagi dalam 4 faktor penting yang menyatu dalam bentuk siklus. Sebagaimana Hipstaken dan Krenendank dalam Brand dan Boonen (2007) mempresentasikan 4 kelompok proses sebagai berikut:

a. Perencanaan: mencakup sartegi dan taktik serta cara TI untuk memberikan konstribusi sebaik-baiknya dalam mencapai tujuan bisnis
b. Realisasi: merealisasikan tujuan TI, mengindentifikasi, dan mengembangkan TI sebagai solusi dalam proses bisnis.

c. Penyampaian dan dukungan: Domain ini melalui keamanan dan kelanjutan melalui pelatihan dan termasuk pemrosesan data dengan sistem aplikasi yang rahasia.
d. Pengawasan dan evaluasi: Semua proses TI perlu diadakan pengawasan dan evaluasi secara berkala untuk meningkatkan kualitas, dan merupakan kebutuhan pengendalian.

Sumberdaya TI terdiri dari manusia, aplikasi, informasi dan infrastuktur. Sumberdaya manusia perlu direncanakan, diorganisasikan dan disediakan, didukung, diawasi dan dievaluasi dalam TI ini. Aplikasi merupakan sistem penggunaan dan prosedur dalam memproses sistem informasi atau TI. Informasi merupakan data sebagai *input* dan *output* sebuah sistem informasi, dalam segala bentuk yang digunakan dalam bisnis. Infrastruktur merupakan fasilitas yang mendukung proses sistem informasi.

Sedangkan kriteria kualitas merupakan konsep yang mendorong kebutuhan bisnis. Cobit yang dimaksud meliputi: kebutuhan kualitas (kualitas, biaya, dan penyampaian); kebutuhan hukum (opersional yang efektif dan efisien, informasi yang reliabel, dan sejalan dengan hukum dan aturan); dan kebutuhan keamanan (kerahasiaan, integritas, dan ketersediaan). Kriteria yang efektif mencakup kebutuhan kualitas. Aspek kualitas bersamaan dengan aspek ketersediaan atau kebutuhan keamanan, efektivitas, dan efisiensi, serta aspek biaya termasuk dalam efisiensi. Sementara kriteria kualitas juga didefinisikan sebagai berikut:

a. Efektifitas : mengetahui informasi mana untuk menyajikan definisi tujuan sistem informasi
b. Efisiensi: mengetahui aktivitas mana yang berkaitan dengan provisi informasi dan menghasilkan biaya serta umerchanta yang dapat diterima.
c. Kerahasiaan: mengetahui data mana yang hanya dapat di akses oleh kelompok dan orang tertentu.
d. Integritas: untuk mengetahui data mana yang berkoresponden dengan situasi aktual yang terwakilkan dengan data itu.

e. Ketersediaan: untuk mengetahui sistem atau layanan yang mana yang tersedia untuk pengguna dalam waktu tertentu.

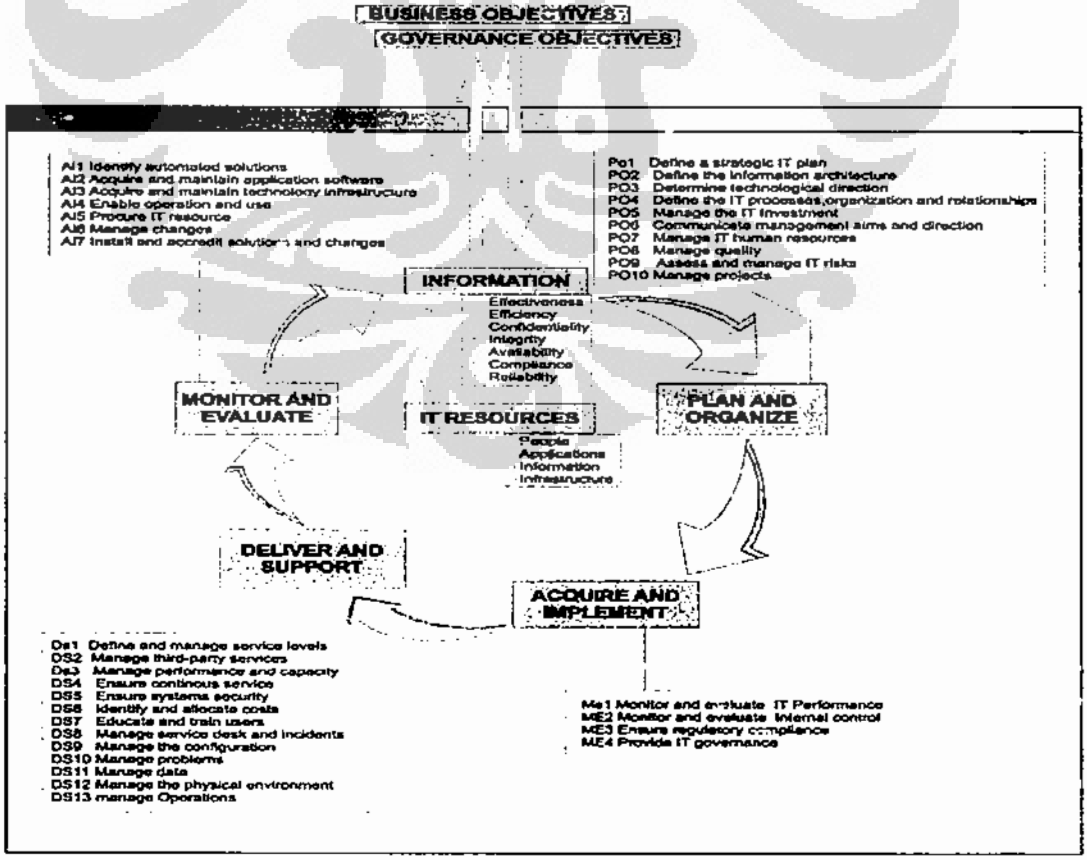
f. Sesuai aturan: untuk mengetahui proses mana yang bertindak sesuai dengan hukum, aturan dan perjanjian yang mana proses itu sebagai subjeknya.

g. Ketersediaan informasi: Untuk mengetahui informasi mana yang layak yang disediakan untuk manajemen dalam pengoperasian TI, dan kesesuaian hukum serta dapat dipertanggungjawabkan.

Selanjutnya Cobit juga merupakan kerangka tata kelola TI (*Cobit is an IT Governance Framework*). Cobit ini berfungsi sebagai pengendalian, fokus bisnis, orientasi proses, penerimaan secara umum, kebutuhan yang berkaitan dengan peraturan, pimpinan dari organanisasi TI, pengawasan dan pengendalian, *responsibility*, dan akuntabilitas. Apabila dalam bentuk gambar dijelaskan sebagai berikut:

Gambar 14

Cobit is an IT Governance Framework



Sumber: Brand dan Boonen (2007)

Beberapa teori yang dikemukan tersebut, akan menjadi pisau analisis untuk menentukan standar manajemen pengamanan sistem infomasi dalam penelitian ini. selain itu bertujuan untuk mendekati standar dari ISO 27001: 2005, yang terdiri dari 11 golongan, 39 tujuan pengendalian, dan 134 pengendalian tentang pengendalian dan pengawasan dalam bentuk standar operasional prosedur (Snare & Kuper 2005). 11 golongan dalam ISO tersebut akan diuraiakan sebagai berikut:

1) Kebijakan keamanan (*security police*).
2) Organisasi keamanan informasi (*organization of information sekurity*).
3) Manajemen aset.
4) Kemananan sumberdaya manusia (*human resources sekurity*).
5) Keamaan fisik dan lingkungan.
6) Komunikasi dan manajemen informasi.
7) Kendali akses.
8) Akusisi sistem informasi, pengembangan, dan pemeliharaan.
9) Manajemen insiden keamanan informasi.
10) Manajemen kesinambungan bisnis (*busisness continuity management*).
11) Pemenuhan (*compliance*).

BAB 3
GAMBARAN UMUM BANK PERMATA

Istilah bank atau perbankan bukan merupakan sesuatu hal yang asing bagi masyarakat Indonesia. Bank sudah merupakan penopang hidup manusia dalam memenuhi kebutuhannya. Namun secara umum mayarakat hanya mengetahui bank sebatas tempat penyimpanan uang, tempat pengiriman uang, tempat meminjam modal usaha, tempat perkreditan rumah, dan lain sebagainya. Akan tetapi peranan perbankan juga mempengaruhi kegiatan ekonomi suatu negara, sebagaimana Kasmir (2002) bank dapat dikatakan sebagai darahnya perekonomian suatu negara, karena kemajuan bank di suatu negara dapai dijadikan tolok ukur kemajuan negara yang bersangkutan.

Berdasarkan Undang-undang No. 10 Tahun 2008 bank adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kemasyarakat dalam bentuk kredit atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup orang banyak. Dari definisi tersebut bank merupakan lembaga keuangan yang kegiatannya menghimpun dana, menyalurkan dana dan memberikan jasa-jasa lainnya.

Menghimpun dana dari masyarakat dalam bentuk simpanan atau sebagai investasi bagi masyarakat. Tujuan masyarakat menyimpan dan berinvestasi di bank untuk mendapatkan bunga dari hasil simpanannya, selain itu untuk mengamankan uang dan investasi serta mempermudah transaksi dan sifatnya simpanan ini merupakan uang kelebihan masyarakat, yang dimaksud adalah dana atau uang yang tidak digunakan oleh masyarakat, dan bisa juga dikatakan masyarakat yang sudah mempunyai kelebihan uang menurut standar hidupnya. Sedangkan menyalurkan dana dalam bentuk pinjaman atau kredit kepada masyarakat bagi yang memerlukan modal atau membutuhkan uang. Kemudian memberikan jasa lainnya seperti pengiriman uang, Transaksi dalam sejumlah pembelian, penagihan surat berharga.

3.1 Sejarah Perbankan di Indonesia

Pada awalnya seseorang melalukan transaksi untuk memenuhi kebutuhan hidupnya menggunakan sistem yang dikenal sistem barter. Sistem barter adalah

perdagangan dengan saling tukar menukar barang atau jasa dengan barang dan jasa, misalnya ingin mendapatkan beras menukarkan dengan ikan. Kemudian seiring dengan perkembangan manusia sistem barter ini mulai ditinggalkan karena manusia mengalami kesulitan dalam hal tukar menukar untuk memenuhi hidupnya, dan mengembangkan sistem transaksi dengan menggunakan uang sebagai alat pembayaran.

Uang adalah alat pembayaran terhadap barang atau jasa yang diperlukan. Sebagaimana dikemukakan Kasmir (1998, hlm. 13) "pengertian uang secara luas adalah sesuatu yang dapat diterima secara umum sebagai alat pembayaran dalam suaut wilayah tertentu atau sebagai alat pembayaran utang atau sebagai alat untuk pembelian barang dan jasa." Uang mempunyai peranan penting bagi semua kegiatan masyarakat, walaupun sistem barter masih digunakan dalam perdagangan tertentu seperti antar negara, dan di daerah pedesaan. Uang juga dapat dijadikan suatu ukuran tingkat ekonomi seseorang dan kemajuan atau stabilitas suatu negara.

Perkembangan sistem pembayaran dengan uang seiring dengan perkembangan sistem perbankan yang dikenal pada zaman Babylonia sampai masuk ke Indonesia. Menurut Kasmir (2002, hlm 14) Bangsa Indonesia mengenal dunia perbankan berasal dari negara penjajah yaitu Belanda. lebih lanjut dijelaskannya, pada saat itu terdapat beberapa bank yang memegang peranan penting dalam pemerintahan Hindia Belanda, yaitu:

a. De Algemenevolks Crediet Bank
b. De Escompto Bank NV
c. De Javasche NV
d. De Post Paar Bank
e. Nederland Handles Maarscapij (NHM)
f. Nationale Handles Bank (NHB

Selain itu ada juga terdapat bank-bank lain milik pribumi, jepang, dan negara eropa lainnya, yaitu:

a. Bank Abuan Saudagar
b. Batavia Bank
c. Bank Negara Indonesia
d. NV Bank Boemi

e. The Charterd Bank Of India

f. The Yokohoma species Bank

g. The Matsui Bank

h. The Bank Of Cina

Namun kemerdekaan Indonesia 17 Agustus 1945 telah mengubah pemetaan perbankan di Indonesia. Perbankan di Indonesia bertambah baik dari segi kuantitas dan kualitas pelayanannya, beberapa bank milik pemerintah Belanda dinasionalisir oleh pemerintah Indonesia (Kasmir 2002). Selain itu juga pemerintah Indonesia membuat regulasi untuk mengatur perbankan di Indonesia yaitu Undang-undang No 14 tahun 1967, kemudian UU Pokok Perbankan No.. 7 tahun 1992 dan terakhir dikeluarkannya Undang-udang Perbankan No. 10 Tahun 1998. Yang mana dalam undang-undang tersebut memuat kegiatan utama bank sebagai lembaga keuangan yang menghimpun dana dari masyarakat dan menyalurkannya kepada masyarakat dalam bentuk kredit maupun bentuk-bentuk lainnya.

Gambar 15

PERBANKAN DI INDONESIA

Sumber: Kasmir 2002

Apabila perbankan di Indonesia dilihat fungsinya dapat dikelompokan menjadi tiga jenis: Bank Central, Bank Umum, dan Bank Perkreditan Rakyat. Bank Central merupakan bank yang mengatur dunia perbankan di Indonesia dalam hal ini adalah bank Indonesia. Bank Umum adalah bank yang melaksanakan

kegiatan usaha secara konvensional dan atau berdasarkan prinsip syariah yang dalam kegiatannya memberikan jasa dalam lalu-lintas pembayaran. Sifat jasa yang diberikan adalah umum, artinya dapat memberikan jasa perbankan yang ada. Begitu pula dengan wilayah operasinya dapat dilakukan di seluruh wilayah Indonesia (UU No 10 Tahun 1998). Bank Perkreditan Rakyat (BPR) adalah bank yang melaksanakan kegaitan usaha secara konvensional atau berdasarkan prinsip syariah. Dalam kegiatannya BPR tidak memberikan jasa dalam lalu lintas pembayaran. Artinya jasa-jasa perbankan yang ditawarkan BPR lebih sempit jika dibandingkan dengan kegiatan atau jasa Bank Umum (UU No 10 Tahun 1998).

Sedangkan berdasarkan kepemilikannya Bank di Indonesia di bagi 5 jenis: bank milik pemerintah, swasta nasional, asing, koperasi, dan campuran. Kasmir (2002, hlm 20-23) menjelaskan kelima jenis bank di Indonesia sebagai berikut:

a. Bank milik pemerintah merupakan bank yang akte pendirian maupun modal bank sepenuhnya milik pemerintah Indonesia.
b. Bank milik swasta nasional merupakan bank yang seluruh atau sebagian usahanya milik swasta dan akte pendiriannya juga dimiliki swasta nasional.
c. Bank milik koperasi merupakan bank yang usaha- usahanya dimililki oleh perusahaan yang berbadan bukum koperasi.
d. Bank milik asing merupakan bank cabang yang ada di luar negeri baik milik swasta maupun milik pemerintah asing.
e. Bank milik campuran merupakan bank yang usahanya dimiliki oleh pihak asing dan pihak swasta nasional.

3.2 Profil Bank Permata

Berdasarkan uraian di atas Bank Pemata dalam penelitian ini merupakan jenis bank umum dan kepemilikannya adalah swasta nasional yang mempunyai perwakilan di seluruh Indonesia. Bank Permata merupakan suatu perusahaan berbentuk Perseroan Terbatas (PT) yang bergerak dibidang penyedia jasa keuangan. Kegiatan secara umum adalah menghimpun dana (giro, tabungan, dan deposito), menyalurkan dana (kredit investasi, modal kerja, perdagangan,

produktif, kumsumtif, dan profesi), dan jasa lainnya (kiriman uang, klearing, inkaso, *safe deposite box*, kartu kredit, menerima setoran dan lain sebagainya).

Bank ini merupakan hasil merger 5 Bank, yaitu PT. Bank Bali Tbk, PT. Bank Universal Tbk, PT. Bank Artamedia, PT. Bank Patriot dan PT. Bank Prima Ekspress pada 2002. Pada 2004, Standard Chartered Bank dan PT Astra International Tbk mengambil alih Bank Permata dan memulai proses transformasi secara besar-besaran didalam organisasi. Selanjutnya, sebagai wujud komitmennya terhadap Bank Permata, kepemilikan gabungan pemegang usaha utama ini meningkat menjadi 89,01% pada tahun 2006.

Kombinasi unik dari kedua pemegang merchantam strategis merupakan salah satu kekuatan utama Bank Permata. PT Astra International Tbk merupakan perusahaan Indonesia yang besar dan memiliki pengalaman kuat di pasar domestik. Standard Chartered Bank dengan keahlian dan pengalaman global terkemuka yang dimilikinya menjadikan Permata Bank berada dalam posisi yang unik. Dan saat ini Bank Permata telah berkembang menjadi sebuah bank swasta utama yang menawarkan produk dan jasa inovatif serta komprehensif terutama disisi *delivery channel*-nya termasuk *Internet Banking* dan Mobile *Banking*. Bank Permata memiliki aspirasi untuk menjadi penyedia jasa keuangan terkemuka di Indonesia, dengan fokus di segmen Konsumer dan Komersial. Melayani sekitar 1,9 juta nasabah di 55 kota di Indonesia, Bank Permata memiliki 278 cabang (termasuk 10 cabang Syariah) dan 631 ATM dengan akses tambahan di lebih dari 40.000 ATM (VisaPlus, Visa Electron, MC, Alto, ATM Bersama dan ATM Prima).

Untuk mendukung serta menjalankan aktivitasnya, Bank Permata mempunyai visi dan misi untuk mencapai tujuannya. Visi dan misi itu adalah sebagai berikut:

a. Visi: menjadi penyedia jasa keuangan terkemuka di Indonesia, yang memiliki fokus pada segmen *Consumer* dan *Commercial*.
b. Misi:
   - Nasabah menjadi mitra pilihan melalui kesempurnaan pelayanan dan pemberian solusi yang optimal.

- Karyawan turut serta mendorong pengembangan profesionalisme dan kepribadian.
- Masyarakat aktif berpartisipasi dalam upaya mewujudkan kontribusi yang bermanfaat.
- Pemegang usaha memberikan hasil investasi terbaik bagi pemegang usaha.
- Pemerintah menjadi panutan dalam penerapan tata kelola perusahaan dan asas ketaatan yang baik.

Selanjutnya, pemegang saham per 31 desembet 2007 terdiri dari: PT. Astra Internasional Tbk 44,505 %, Standard Caharted Bank 44, 505%, dan publik atau masyarakat 10,990 % dengan jumlah keseluruahan adalah 100%. Sementara itu pengurus bank terdiri dari dewan komisaris dan direksi. Dewan komisaris terdiri dari komisaris utama : Raymod J. Ferguuson, wakil komisari utama: Gunawan Geniumerchantardja, Komisaris Independen: Lukita D. Towo dan I Sopomo, David Allen Worth, John A. Prasetio, A.Tony Praseiantono, Komisaris: Mark Sepencer Greenberg dan Ajay Chamanial Kanwai. Sedangkan dewan direksi terdiri dari: Direktur utama, wakil direktur dan 5 direktur.

Nilai-nilai budaya kerja Bank Permata adalah *way life* bagi setiap Bank Permataer. Budaya Kerja Bank Permata adalah seperangkat nilai dan perilaku yang harus diamalkan dan dijalankan oleh setiap Bank Permataer selama berkarya di Bank Permata. Budaya kerja bank permata terdiri dari nilai-nilai budaya Bank Permata dan 8 Perilaku Bank Permataer, sebagai berikut:

1) Kepercayaan: keyakinan seluruh *stakeholder* yang perlu dibangun dan dijaga bahwa kita sebagai pribadi atau institusi dalam melakukan sesuatu selalu dilandasi itikad baik, jujur dan handal;
2) Integritas: senantiasa memiliki keselarasan niat, pikiran, perkataan dan perbuatan baik dan benar yang sesuai dengan nilai-nilai perumerchantaan, masyarakat dan prinsip-prinsip *good corporate governance*;
3) Pelayanan: senantiasa memberikan layanan yang melebihi ekspektasi kepuasan *stakeholder* dan memberikan pengalaman interaksi terbaik,

serta memiliki kualitas prima dengan menekankan pada aspek kecepatan, ketepatan dan keramahan;

4) Kesempurnaan: Senantiasa berupaya secara maksimal dan selalu bercermin pada standar-standar unggul untuk secara berkesinambungan mencapai hasil yang terbaik;
5) Profesionalisme: Senantiasa melaksanakan peran dan fungsi berdasarkan kompetensi yang handal, terus menerus meningkatkan kemampuan dan bertanggung jawab.

Untuk dapat mengamalkan nilai-nilai budaya Bank Permata dalam keseharian kerja, diperlukan perilaku-perilaku yang mampu mengarahkan tindakan ke pengamalan nilai tersebut. Perilaku-perilaku tersebut kemudian dirumuskan kedalam 8 Perilaku Bank Permataer, sebagai berikut:

1) Disiplin: menjalankan aktivitas kerja berdasarkan ketepatan ukuran-ukuran peraturan perusahaan, ketepatan waktu dan komitmen dalam menjalankan janji yang diucapkan;
2) bertanggung jawab: tindakan-tindakan individu yang didasarkan pada niat atau motivasi yang baik dan benar, dijalankan dengan cara-cara yang baik dan benar, serta dengan kesadaran pribadi bersedia menerima konsekuensi atas tindakannya tersebut;
3) cepat, tanggap dan berinisiatif: Perilaku Cepat terkait dengan penggunaan waktu yang efisien tercermin pada kemampuan dan kemauan untuk menyelesaikan tugas dengan kecepatan waktu seoptimal mungkin tanpa mengurangi kualitas hasil kerja. Sedangkan perilaku Tanggap dilandasi kepedulian karyawan untuk memperbaiki hal-hal yang dipandang tidak benar atau kurang etis atau kemauan untuk membantu/menolong pihak lain yang memerlukan bantuannya. Perilaku Berinisiatif dilandasi kemampuan antisipatif atas situasi atau persoalan yang potensial muncul di masa datang, inisiatif terdapat pada perilaku, gagasan yang berujung pada perbaikan yang diperlukan organisasi;
4) ahli di bidangnya: kemauan untuk selalu mengembangkan diri yang selaras dengan tuntutan pekerjaan dan organisasi.sehingga menjadi ahli

dalam bidangnya. Keahlian sangatlah penting agar tiap kali persoalan muncul, sehingga sanggup mengatasinya dan menjadikannya sebagai media perbaikan berkelanjutan;

5) mampu bekerjasama: kemampuan karyawan untuk bekerjasama dalam arti terus-menerus mengupayakan terjadinya kerjasama secara baik dan benar, dan meminimalkan kecenderungan untuk mementingkan kepentingan pribadi.
6) efektif dalam berkomunikasi: perilaku efektif dalam berkomunikasi adalah kemauan untuk mendengarkan pendapat pihak lain, memahaminya dengan benar dan kemudian meresponnya secara tepat. Kondisi-kondisi pihak yang diajak berkomunikasi dan norma yang berlaku di tempat kita melakukan komunikasi juga merupakan hal yang harus dipertimbangkan saat mengemukakan gagasan atau pendapat.
7) peka dan peduli untuk kebaikan: peka mengandung arti memiliki ambang batas optimal atas rangsangan lingkungan yang memerlukan reaksi kita untuk perbaikan, pengembangan. Sedangkan peduli adalah bentuk sikap yang dimunculkan dalam perilaku dimana seseorang menunjukkan perhatian khusus pada kondisi-kondisi yang dipandang kurang semestinya, perlu dibenahi, dan yang bersangkutan bereaksi membenahinya;
8) tidak menyalahgunakan jabatan: tidak menyalahgunakan jabatan adalah perilaku untuk tidak memanfaatkan fasilitas atau sumber daya perusahaan untuk kepentingan pribadi, serta tidak meminta imbalan dari pihak lain yang memerlukan jasanya atas jabatan tersebut.

Perilaku Bank Permataer, bila dilaksanakan dengan konsisten, akan membentuk seorang Bank Permata sejati, dapat dipercaya, berintegritas tinggi, mengutamakan pelayanan, selalu berupaya secara optimal dan memiliki kompetensi di bidang kerjanya.

Sekilas operasionalnya, Bank Permata dapat dilihat dari lokasi cabang , syariah, ATM dan *mobile cash.* Lokasi cabang terdiri dari: Balikpapan, Banda Aceh, Bandar Lampung, Bandung, Banjarmasin, Banyuwangi, Batam, Bekasi,

Blitar, Bogor, Bojonegoro, Cianjur, Cilacap, Cilegon, Cirebon, Denpasar, Depok, Garut, Gresik, Jakarta Barat, Jakarta Pusat, Jakarta Selatan, Jakarta Timur, Jakarta Utara, Jambi, Jember, Jombang, Karawang, Kediri, Klaten, Kudus, Madiun, Magelang, Makassar, Malang, Manado, Medan, Mojokerto, Padang, Palembang, Pasuruan, Pekalongan, Pekanbaru, Pontianak, Probolinggo, Purwokerto, Salatiga, Samarinda, Semarang, Serang, Sidoarjo, Solo, Sukabumi, Surabaya, Tangerang, Tasikmalaya, Tegal, Tulungagung, Yogyakarta. Total secara keseluruhan 265 lokasi dan 59 kota di seluruh Indonesia. Sedangkan lokasi cabang syariah meliputi Banda Aceh, Bandung, Banyuwangi, Blitar, Cianjur, Cilacap, Cirebon, Garut, Jakarta, Jember, Kabanjahe, Kediri, Kudus, Madiun, Magelang, Makasar, Malang, Medan, Pasuruan, Padang Sidempuan, Pekalongan, Pekanbaru, Probolinggo, Purwokerto, Salatiga, Semarang, Serang, Solo, Sukabumi, Surabaya, Tasikmalaya, Tegal, Tulungagung. Total keseluruhan cabang syariah 42 cabang. Selanjutnya lokasi ATM dan *mobile cash* meliputi Balikpapan, Bandung, Banjarmasin, Banyuwangi, Batam, Blitar, Bogor, Bojonegoro, Cianjur, Cilacap, Cirebon, Denpasar, Garut, Jakarta, Jambi, Jember, Jogjakarta, Jombang, Kediri, Klaten, Kudus, Lampung, Madiun, Magelang, Makasar, Malang, Manado, Medan, Mojokerto, Nagroe Aceh, Padang, Palembang, Pasuruan, Pekalongan, Pekanbaru, Pontianak, Probolinggo, Purwokerto, Salatiga, Samarinda, Semarang, Serang, Solo, Sukabumi, Surabaya, Tasik, Tegal, Tulungagung. Dengan total 623 unit atm di 48 kota seluruh Indonesia.

Sedangkan sekilas produk Bank Permata terdiri dari *liabities product*, kredit usaha kecil menengah, kredit konsumer, layanan investasi, dan produk lainnya. Hal ini dapat dijelaskan sebagai berikut:

a. Liabilities Produk:
    1) PermataTabungan;
    2) PermataTabungan OPTIMA;
    3) PermataTabungan BEBAS;
    4) PermataFamillionaire;
    5) PermataBintang;
    6) PermataGiro;
    7) PermataPayroll;

8) PermataSmart Point.

b. Kredit Usaha Kecil Menengah:
   1) PermatasExpress Trade;
   2) Permata Griya Bisnis;
   3) Permata KTA Bisnis.

c. Kredit Konsumer:
   1) Permata Shopping Card;
   2) Permata Personal Loan;
   3) PermataKPR "Jaminan Proses KPR 5 Hari" ;
   4) PermataKPR Keluarga;
   5) PermataKPR Bijak;
   6) PermataHome *Ready Cash*;
   7) PermataKPR Cicilan Tetap.

d. Layanan Investasi:
   1) Galeri Reksa Dana;
   2) Tabel NAB;
   3) Sukuk Negara Ritel Seri 002.

e. Produk lain-lain:
   1) Bank Permata KENCANA (Kesempurnaan layanan bagi pribadi bernilai);
   2) PermataTel (Layanan perbankan tanpa batas ruang dan waktu);
   3) Bank Permata ATM (Fasilitas transaksi 24-jam dengan jangkauan lebih luas);
   4) PermataMobile (Kemudahan dan kenyamanan bertransaksi tanpa batas);
   5) PermataNet (Transaksi online leluasa dan tetap aman);
   6) PermataMini ATM atau *Merchant Acquiring.*

Selain itu, Bank Permata juga memiliki tanggung jawab sosial. Aktivitasnya menjangkau berbagai lapisan masyarakat di seluruh Indonesia, sehingga dapat berkontribusi efektif pada peningkatan kualitas hidup masyarakat. Bank Permata memiliki komitmen untuk terus berusaha lebih giat dalam

mewujudkan konsep dasar tanggung jawab sosial perusahaan (*Corporate Social Responsibility* - CSR) melalui beberapa kegiatan yang berfokus pada pendidikan dan kepedulian terhadap komunitas. Bank Permata Peduli didirikan tahun 2002, sebagai bentuk tanggung jawab sosial Bank Permata kepada masyarakat dengan menjalankan berbagai kegiatan bermanfaat bagi lingkungan dan masyarakat.

Bank Permata Peduli percaya bahwa pendidikan dan pemberdayaan masyarakat merupakan salah satu sarana terbaik untuk membantu meningkatkan kualitas hidup masyarakat secara nyata. Untuk itu, Bank Permata Peduli telah merancang dan melakukan berbagai program seperti *Book for Thought*, *Banking for Students*, *Care to Community*, dan pemberdayaan Usaha Kecil Menengah (UKM). Dalam pelaksanaan program, Bank Permata Peduli, tidak hanya mengupayakan partisipasi aktif dari masyarakat sebagai penerima manfaat program, namun juga mengajak keterlibatan para Bank Permataers untuk aktif menjadi relawan dalam berbagai kegiatan CSR. Adapun bentuk CSR Bank Permata adalah berikut ini:

a. Ciptakan asa lebih berseri, tebar ilmu untuk sesama (*Book for Thought*).

   Membaca buku memungkinkan seseorang untuk menambah pengetahuan dan memperluas wawasan. Melalui program peduli buku, Bank Permata berharap dapat membantu mempermudah akses kepada bahan bacaan berkualitas dan menumbuhkan minat baca, terutama di kalangan masyarakat yang kurang mampu.

   Program ini mulai dilakukan sejak tahun 2006 melalui aktivitas *Book Collection*, yaitu pengumpulan buku bekas dari Bank Permataers, dan *Book Donation*, yaitu penggalangan dana dari Bank Permataers dan nasabahnya, yang kemudian digunakan untuk membeli buku-buku berkualitas. Buku-buku tersebut kemudian disumbangkan kepada berbagai taman bacaan dan perpustakaan yang membutuhkan. Di tahun 2009, tercatat sekitar 7,000 buku telah disumbangkan kepada 107 taman bacaan, perpustakaan, atau yayasan.

   Salah satu fokus program peduli buku Bank Permata adalah untuk membantu perpustakaan sekolah dan taman bacaan di berbagai

wilayah yang mengalami musibah bencana alam. Bank Permata Peduli bekerja sama dengan Dompet Dhuafa Republika untuk membangun kembali perpustakaan di SDN 25 Sungai Sarik, Padang Sago, Kabupaten Padang Pariaman - Sumatera Barat.

Sebagai kelanjutan dari program rekonstruksi bangunan yang dilakukan Bank Permata Peduli pada tahun 2006 di SDN 1 Pundong, Jogjakarta, Bank Permata Peduli kembali melakukan pembangunan perpustakaan hingga menjadi taman bacaan yang layak bagi para siswa, ditambah dengan kegiatan ekstrakurikuler *Marching Band* untuk peningkatan mutu sekolah.

Untuk mendukung karya sastra yang berkualitas, meningkatkan daya apresiasi masyarakat terhadap bahan bacaan, serta bagian dari program *Book Sharing*, Bank Permata menggelar pentas seni fragmen sebagai visualiasi drama dari buku '9 dari Nadira' karya Leila S. Chudori bekerja sama dengan Kepustakaan Populer Gramedia dan Yayasan Dian Sastrowardoyo. Acara yang dihadiri oleh lebih dari 250 budayawan dan sastrawan ini juga merupakan peresmian kerjasama antara ketiga belah pihak untuk berkomitmen menyumbangkan buku-buku kepada taman-taman bacaan dan perpustakaan sekolah yang membutuhkan di seluruh Indonesia.

Aktivitas lain yang dilakukan dalam program peduli buku adalah Lomba Dongeng Anak Se-Jabodetabek yang dilangsungkan di Museum Nasional dan Taman Mini Indonesia Indah, melibatkan masing-masing 200 anak dari lebih 102 taman bacaan dibawah binaan Komunitas 1001 Buku.

b. Ciptakan Pola Hidup Terencana, Cintai Gemar Menabung Sejak Dini (*Banking for Students*)

Bank Permata Peduli telah melaksanakan program *Banking for Students* sejak tahun 2006, guna menanamkan pola hidup lebih terencana melalui kegiatan menabung sejak usia dini. Tujuan dari program ini adalah untuk memperkenalkan institusi bank dan produk dan layanan bank sejak dini kepada para murid sekolah dasar. Dalam

jangka panjang nantinya, hal ini diharapkan dapat turut membantu akselerasi pembangunan perekonomian bangsa.

Program Banking for Students memberikan pengenalan dasar layanan perbankan, termasuk simulasi cara menabung dan praktik mengenal teknologi perbankan, kepada para pelajar dari berbagai tingkatan. Sampai dengan saat ini, sejumlah 62 sekolah di 62 cabang Bank Permata telah menjadi sasaran dari program ini.

c. *Care of Community*

Program ini bertujuan membantu mengatasi permasalahan sosial di masyarakat, terutama di wilayah-wilayah korban bencana alam. Bank Permata Peduli aktif melakukan penggalangan dana serta donasi barang-barang kebutuhan sehari-hari untuk korban bencana alam di Tasikmalaya serta Sumatera Barat.

d. Pemberdayaan Usaha Kecil Menengah

Bank Permata Peduli percaya bahwa program pemberdayaan yang tepat merupakan salah satu sarana efektif untuk membantu menghantarkan masyarakat menuju taraf hidup yang lebih baik. Untuk membantu menciptakan perekonomian yang tangguh dan mandiri, Bank Permata melakukan aktivitas program Pemberdayaan UKM di berbagai daerah. Bekerjasama dengan Yayasan Dharma Bhakti Astra, Bank Permata melakukan seminar dan penyuluhan terhadap UKM di tiga kota, yaitu Jakarta, Waru-Sidoarjo (Jawa Timur) serta Balangan (Kalimantan Selatan). Melalui program kerja sama dengan YDBA ini, Bank Permata memberikan kredit tanpa agunan berbunga sangat ringan dibandingkan tingkat suku bunga nominal untuk jangka waktu maksimal 3 tahun dengan kemudahan administrasi dan bebas provisi.

e. Keterlibatan Aktif Karyawan

Karyawan-karyawan Bank Permata diharapkan tidak hanya memberikan kontribusi terhadap perusahaan, tetapi juga terhadap masyarakat dan lingkungan. Untuk itu, dalam setiap kesempatan kegiatan tanggung jawab sosial perusahaan, Bank Permata Peduli selalu melibatkan karyawannya. Suatu survei internal yang dilakukan

pada bulan September 2009 memperlihatkan bahwa mayoritas responden memiliki aspirasi untuk aktif melakukan kontribusi sosial kepada masyarakat. Aspirasi tersebut diwujudkan dengan cara menyisihkan waktu dan tenaga mereka dalam berbagai kegiatan Bank Permata Peduli, antara lain sebagai pembina dan *story teller* pada program *Book for Thought*, serta sebagai pengajar dan pembina pada program *Banking for Students* dan pemberdayaan UKM. Tercatat sekitar 1.000 orang karyawan Bank Permata aktif terlibat sebagai relawan dalam berbagai kegiatan Bank Permata Peduli sepanjang tahun 2009.

Atas bisnis yang dilakukan ini Bank Permata memperoleh beberapa penghargaan. Penghargaan yang diterima Bank Permata adalah pengakuan, penghargaan atas kinerja, layanan dan prestasi dari kerjasama dan kerja keras seluruh *stakeholder* mulai dari pemegang saham, manajemen, karyawan dan serta nasabah. Berikut penghargaan yang diterima Bank Permata selama 3 (tiga) Tahun terakhir:

a. Tahun 2009
   1) *Annual Report Award 2008 (Overall Winner and First Place Winner - listed private financial institution category) - Organized by Bapepam-LK, Indonesia Stock Exchange, Bank Indonesia, Ministry of State Owned Enterprises, National Committee on Governance, Indonesia Accountant Association and Directorate General of Taxation*;
   2) *E-Company Award 2009 (1st position in The Banking category) Organized by Warta Ekonomi magazine*;
   3) *Investor Magazine Sharia Award 2009 (Best Sharia Unit) - Organized by Investor magazine*;
   4) *Islamic Finance Award 2009 (Overall Winner for Financial and Service Quality - six different categories) - Organized by Karim Business Consulting*;

5) *Service Quality Award 2009 (Diamond Award for Bank Permata KENCANA) - Organized by Carre - Center for Customer Satisfaction and Loyalty (CCSL)*;
6) *Banking Service Excellence Award 2009 (17 Awards total in two categories - conventional and sharia banking) - Organized by Marketing Research Indonesia (MRI) and Infobank magazine*;
7) *Annual Call Center Award for Service Excellence 2009 (1st position famong all industries - fourth consecutive year) - Organized by Carre - Center for Customer Satisfaction and Loyalty (CCSL)*;
8) *Annual Call Center Award for Service Excellence 2009 (1st position for Credit Card category) - Organized by Carre - Center for Customer Satisfaction and Loyalty (CCSL)*;
9) *Annual Call Center Award for Service Excellence 2009 (1st position for Banking category) - Organized by Carre - Center for Customer Satisfaction and Loyalty (CCSL).*
10) *Exemplary Good Corporate Governance of Best Managed Company (8ih rank) - Organized by Finance Asia publication*;
11) *Best CEO of Best Managed Companies (2nd rank) - Organized by Finance Asia publication*;
12) *Tax Awards for Taxpayers 2008 (3rd position for taxpayers in Jakarta area) - Organized by Directorate General of Taxes - Ministry of Finance*;
13) *GCG Award 2009 (Best Individual Indicators - Equitable Treatment of Shareholders) - Organized by OECD, IICD and Business Review magazine*;
14) *Tax Awards for Taxpayers 2008 (3rd position for taxpayer in Jakarta area) - Organized by Directorate General of Taxes - Ministry of Finance*;
15) *5th National Customer Service Championship 2009 (3rd position) - Organized by Carre - Center for Customer Satisfaction and Loyalty (CCSL)*;

16) *Top 5 Bank of Choice for Mortgages in Indonesia - Organize by Housing Estate publication.*

b. Tahun 2010

1) *Consumer Banking Annual Awards for Excellence in group alignment and strategy execution from Standard Chartered Bank (November)*;
2) *Indonesian Employers of Choice Award 2010 by Swa Magazine and Hay Group (November)*;
3) *Two Business Record Awards for Permata KPR Bijak and Permata KPR Keluarga in Business Record Recognition Night 2010, organized by Tera Foundation and Seputar Indonesia Newspaper (November)*;
4) *Second Rank in Banking Intermediation Award for organized by Bank Indonesia (October)*;
5) *Third winner in listed financial institution category in Annual Report Award 2009 organized by Ministry of Finance, Bapepam-LK, Tax General Directorate, Indonesian Stock Exchange and Indonesian Accountant Association (September)*;
6) *The Most Profitable Sharia Unit and The Most Efficient Sharia Unit in the 2010 Islamic Award by Karim Business Consulting (August)*;
7) *Best Bank in the National Banks category in the Business Indonesia Award (July)*;
8) *Ranked no. 3 in Medium-sized banks category of 50 most admired companies in Indonesia by Business Week (June)*;
9) *Diamond Award for Permata Priority and Gold Award for Regular Banking in Service Quality Award 2010, organized by Carre - Center for Service Satisfaction & Loyalty (CCSL) (May)*;
10) *Awards in 8 different categories in Bank Service Excellence Monitor (BSEM) by MRI-InfoBank 2009/2010 (May)*;

11) *Best Bank for Cash Management in Indonesia by Asian Bankers Magazine (April)*;

12) *1st position among all industries at CSSL's Annual Call Center Award for Service Excellence 2009 (5th Consecutive Award) (March)*;

13) *Conventional Service Excellence from #8 to #5 and Syariah Service Excellence from #5 to #3 (Infobank and MRI) (March).*

c. Tahun 2011

1) *Conventional Service Excellence from #5 to #4 and Syariah Service Excellence from #3 to #1 (Infobank and MRI) (April)*;

2) *Best Mobile Phone Banking Award in Asia Pacific in the 2010 International Excellence in Retail Financial Services Awards Programme by The Asian Banker (March)*;

3) *Service to Care Champion (ServCare Award) for Conventional Bank category with asset > IDG 65 tn, organized by Marketplus Insight and Marketing magazine (January).*

BAB 4
MANAJEMEN PENGAMANAN
SISTEM INFORMASI MERCHANT BANK PERMATA

Berdasarkan gambaran umum penelitian, untuk mendukung aktivitas usahanyanya Bank Permata mempunyai layanan dengan bentuk produk-produk yang menggunakan sistem informasi atau TI. Hal itu agar mempunyai: 1) nilai jual atau menarik para pelanggan (nasabah atau Customer); 2) mampu bersaing dengan bank milik pemerintah, swasta nasional, asing serta campuran; dan 3) terutama mendapatkan keuntungan (*profitable*) bagi keberlangsungan Bank Permata itu sendiri. Akan tetapi bukan ketiga aspek itu saja yang harus diperhatikan oleh Bank Permata, aspek pengamanan juga harus diperhatikan, dalam hal ini adalah keamanan sistem informasi yang mempunyai daya cegah terhadap *loss prevention* dan *crime prevention*. Karena tanpa pengamanan sistem informasi akan menimbulkan kerugian bagi perusahaan sendiri, masyarakat, kehilangan kepercayaan publik dan lemahnya bersaing dengan bank-bank lain.

Sebagaimana peristiwa *fraud banking* yang yang terjadi di *Merchant* Pretty Mom, Padma Collecttion, Hongkong Fashion, Rizky Boutiqe, dan Kharisma Collection pada 16 Nopember sampai dengan 30 Desember 2009 yang dilaporkan ke Polda Metro jaya (Dit Reskrimsus Polda Metrojaya 2010). *Fraud banking* tersebut dilakukan dengan cara mengakses sistem komputer Bank Permata secara tidak syah, dan atas peristiwa itu Bank Permata dirugikan kurang lebih Rp. 70.000.000.000,- atau 70 milyar rupiah (Manajer *Froud Control*, wawancara 3 April 2011).

Berdasarkan hal itu peneliti akan menggali peristiwa ini dengan melihat dan menguraikan sistem pengamanan informasi yang dimiliki Bank Permata. Namun dalam penelitian ini hanya difokuskan kepada layanan produk *Merchant* dimulai dari sistem pengamanan informasi proses akuisisi *merchant*, proses transaksi, dan *settlement* oleh *merchant* kepada Bank Permata. Sehingga dapat memperoleh gambaran secara jelas dan mendalam untuk dianalisis dengan

menggunakan pisau analisis konsep dan teori yang telah disebutkan pada bab 2. Adapun hasil penelitian akan dijabarkan berikut ini.

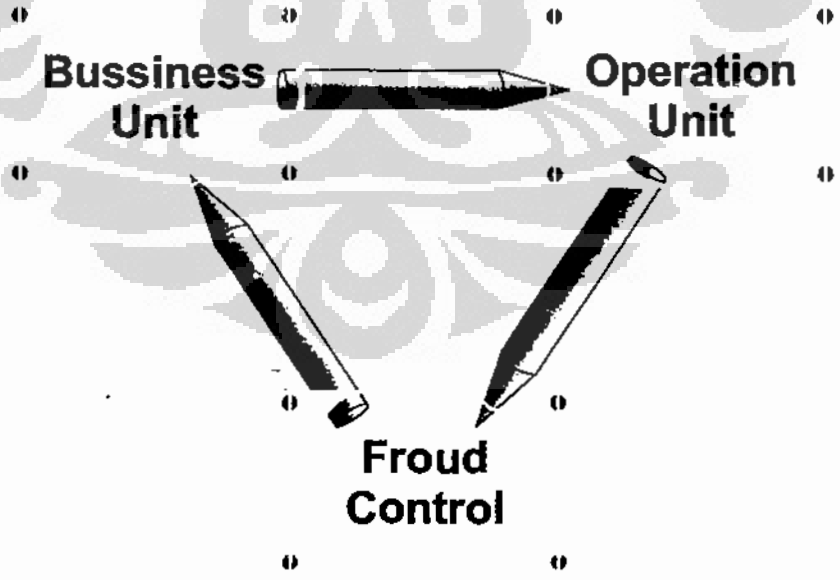
4.1 Pengamanan Sistem Informasi Pada Proses Akuisisi Merchant

Proses memperoleh *merchant* atau disebut dengan akuisisi *merchant* (*acquiring merchant*) adalah rangkaian kegiatan seseorang atau badan usaha mendapatkan persetujuan dari pihak bank untuk memperoleh mesin *elektoronik data capture* (EDC) pada suatu *merchant*. Sedangkan sistem pengamanan yang dimaksud dalam proses pengajuan *merchant* adalah kesesuaian antara prosedur yang diterapkan oleh bank dengan implementasi atau pelaksanaan dari mulai permohonan sampai kepada persetujuan mendapatkan EDC pada suatu *merchant*.

Menurut *Manager Froud Control* (wawancara, 6 April 2011) Pada proses akuisisi *merchant* ini "walaupun merupakan tanggung jawab *merchant* akuisisi, namun melibatkan beberapa unit terkait, dimana satu sama lainnya saling berhubungan." Adapun unit tersebut adalah *Business Unit*, *Operation Unit*, dan *Risk Manajemen Unit* (*Froud Control*).

GAMBAR 16

Unit Yang Terkait Dalam Akuisisi Merchant

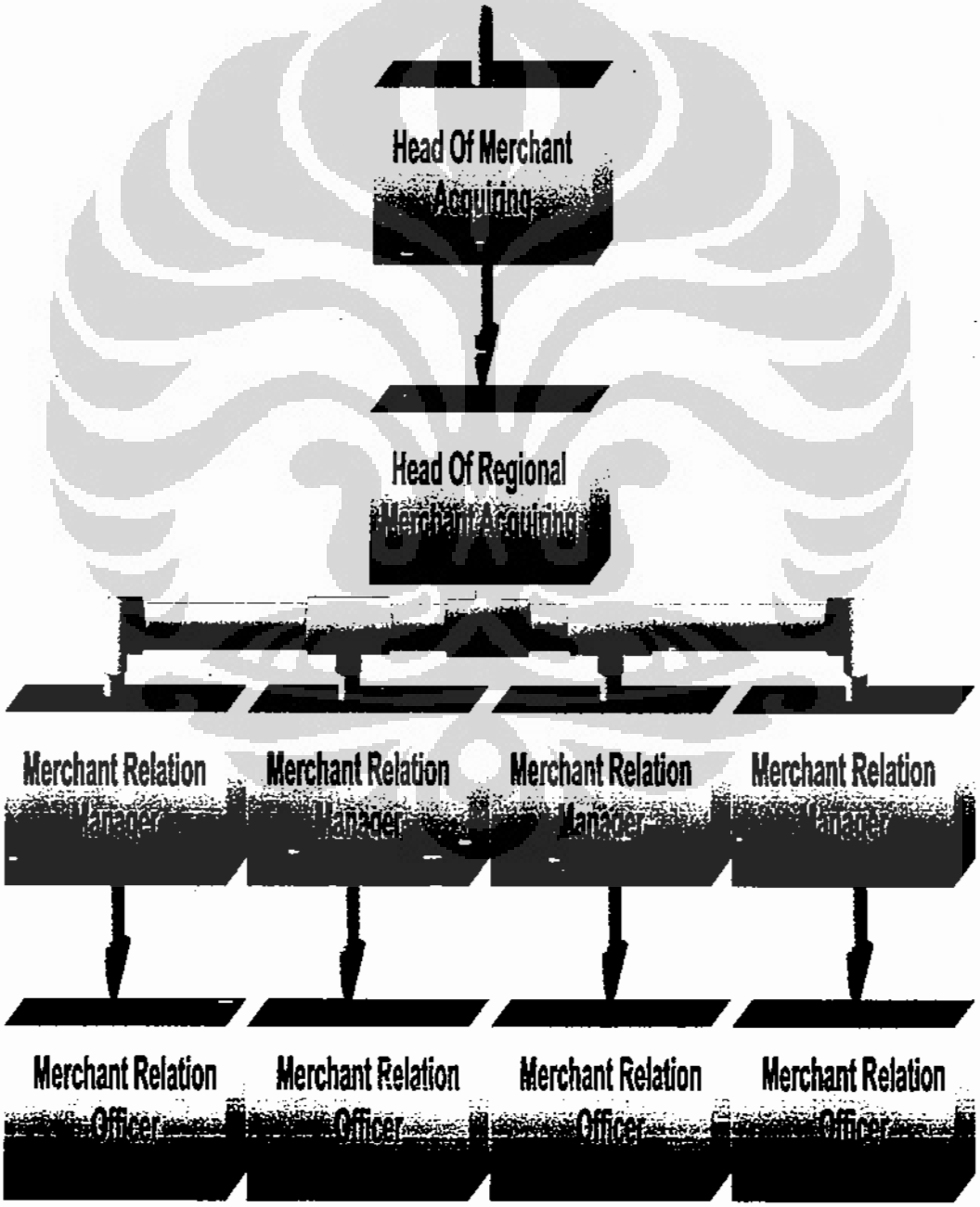


Sumber: Peneliti 2011

Business Unit ini membawahi *Merchant Acquiring Unit* yang secara khusus menangani akuisisi *merchant*. *Business Unit* terdiri dari *merchant acquiring Head*, *head of regional merchant acquiring* , *merchant relation manager*, dan *merchant relation officer*, atau dikenal dengan *merchant sales unit*. Apabila digambarkan dalam bentuk bagan struktur organisasi, seperti dibawah ini.

Gambar 17

STRUKTUR ORGANISASI MERCHANT ACQUIRING BANK PERMATA

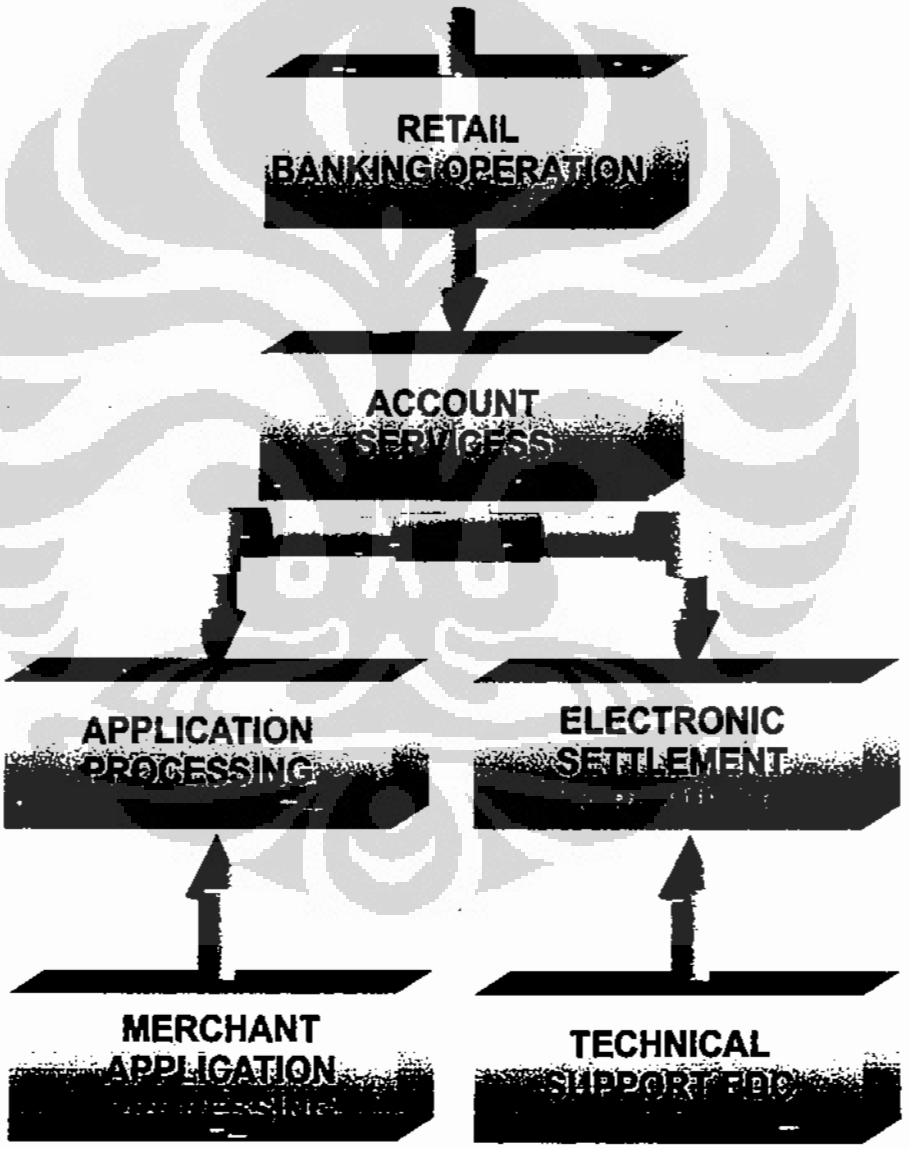


Sumber: Bank Permata 2011

Sedangkan *Operation Unit* membawahi *Retail Banking Operation*, yang terdiri dari *account services*, *application processing*, *electronic settlement & payment*, *merchant aplication processing* dan *technical support EDC-management*. Apabila digambarkan dalam bentuk bagan organisasi, seperti di bawah ini.

Gambar 18

STRUKTUR ORGANISASI RETAIL BANKING BANK PERMATA



Sumber: Bank Permata 2011

Kemudian *Risk Manajemen Control* Unit membawahi *Risk Retail Bangking*. Terdiri dari *froud control and authorization*, dan *merchant froud control*. Apabila digambarkan dalam bentuk bagan struktur organasasi, berikut ini.

Gambar 19

STRUKTUR ORGANISASI RISK RETAIL BANKING BANK PERMATA

Sumber: Wawancara dengan Manager Froud Control, 13 April 2011

Lebih lanjut dijelaskan unit-unit terkait alur proses akuisisi *merchant*, dalam hal ini cara pemohon untuk memperoleh *merchant* Bank Permata. Pada awalnya *Merchant Relation Officer* (untuk selanjutnya disebut dengan MRO), menghubungi atau bisa juga dihubungi oleh calon *merchant* melalui *call centre* Bank Permata. Apabila calon pemohon *merchant* berminat, maka *sales officer* akan menyiapkan "formulir aplikasi *merchant*" dan "Perjanjian Kerja Sama" sebelum melakukan kunjungan. Setelah mengisi "formulir aplikasi *merchant*" dan menyepakati "Perjanjian Kerja Sama" sales officer akan melakukan kunjungan dan mengiformasikan dokumen serta persyaratan lain yang dibutuhkan. Persyaratan yang dimaksud adalah pemohon memiliki Surat Ijin Umerchanta Perdangan (SIUP), Kartu Tanda Penduduk, Nomor Pokok Wajib Pajak, dan kartu tabungan atau rekening koran pemohon dan menyerahkan *fotocopy* nya. Hal ini dikuatkan oleh Nasabah 1 (wawancara 2 April 2011) tentang

mengajukan atau proses akuisisi *merchant* yang menjelaskan "Pemohon adalah pemilik toko, yang harus memiliki SIUP, NPWP, KTP, dan Nomor Rekening Bank Permata. Nomor rekening yang saya buka adalah rekening Giro, yang digunakan untuk menampung hasil transaksi pada mesin EDC yang dibayarkan oleh Bank Permata." Setelah semua terpenuhi, menurut *Staf MRO* (wawancara, 4 April 2011) akan dilakukan verifikasi terhadap kelayakan persyaratan calon *merchant* melalui beberapa tahapan.

Pertama, melakukan verifikasi tersebut adalah *Merchant Relation Officer* (MRO) setelah menerima *fotocopy* persyaratan dari pemohon *merchant*. MRO akan mendatangi dan melakukan pemeriksaan terhadap kelengkapan persyaratan pemohon, serta meminta "formulir aplikasi *merchant*" dan "Perjanjian Kerja Sama" di isi oleh MRO kemudian ditandatangani oleh pemohon. Kedua, kelengkapan akan diteruskan kepada *Manager Relation Merchant* (MRM) untuk dilakukan verifikasi kembali dan ditanda tangani, kemudian diserahkan *kepada Head of Regional Merchant Acquiring* . Ketiga, *Head of Regional Merchant Acquiring* melakukan verifikasi kembali dan menandatangi, kemudian diserahkan kepada *Head of Merchant Acquiring* . Keempat, *Head of Merchant Acquiring* menandatangi permohonan yang sudah diverifikasi kepada unit *Aplication Processing Centre* (APC)-*Merchant*.

Sedangkan tugas Unit APC sendiri adalah melakukan penginputan data *merchant* ke (JHA, ON/2, Asscend). Unit APC juga melakukan pemeriksaan (*cheking blacklist*) status nasabah apakah bermasalah atau tidak ke Bank Indonesia (BI), jika terindikasi pemohon masuk dalam daftar hitam (tidak dianggap sebagai nasabah yang baik) maka aplikasi akan diserahkan kepada Unit *Froud Control* untuk di lakukan peninjauan kembali. Sementara itu apabila tidak ada permasalahan, Unit APC-*Merchant* akan mengirim formulir order EDC ke Unit *Technical Support*. Setelah menerima order permintaan EDC, dilakukan penginputan data baru (*new record data*) berdasarkan *serial number* (s/n) mesin EDC ke sistem (*EDC Very Centre*), kemudian melakukan pengintalan pada mesin EDC dan Input *master key* EDC, serta melakukan tes transaksi *online* secara *dual control.* Selanjutnya MRO akan mendatangi pemohon (*merchant*) untuk melakukan pemasangan berdasarkan EDC yang diterima dari *Technical Support–*

EDC *Management*. Selain itu MRO harus memberikan pelatihan (*training*) tentang cara penggunaan EDC pada *merchant*.

4.2 Pengamanan Sistem Informasi Transaksi Elektronik *Merchant* Bank Permata

Alur transaksi elektronik pada Bank Permata dilengkapi dengan beberapa layer sebagai sistem pengamanan. Transaksi yang dimaksud adalah transaksi Kartu Debet, Kartu Maestro, Kartu Kredit baik yang dilakukan secara *online* maupun *offline*. Sedangkan sistem itu sendiri menurut Manajer *Froud Banking* (wawancara, 6 April 2011) terdiri dari: *authorization*, kode persetujuan, terminal limit, proses *settlement*, sales slip (*sales draft*), *Network Access* atau *Network Access Control* (*NAC*), Base24/ON2, dan *Asscend*.

Lebih lanjut dijelaskan oleh Manajer *Froud Banking* (wawancara, 6 April 2011) layer atau sistem pengamanan pada alur transaksi elektronik tersebut berikut ini.

a. *Authorization* adalah proses untuk mendapatkan persetujuan dari bank penerbit kartu atas setiap transaksi yang akan dilakukan oleh cardholder di merchant yang menerima transaksi dengan menggunakan kartu pada saat menggesekan kartu plastik pada *EDC*. Persetujuan dari bank penerbit kartu sering disebut kode persetujuan (*approval code/authorization code*).
b. Kode persetujuan adalah kode yang tercetak pada slip transaksi EDC yang merupakan kode persetujuan (*approval code*) atas setiap pelaksanaan transaksi kartu kredit, kartu debet, kartu maestro dan transaksi *payment point*.
c. *Terminal limit* adalah batas maksimum transaksi per hari dengan menggunakan Kartu Debet/Kredit pada EDC *Fixed Line* dan/atau EDC Wireless yang dilakukan pemegang Kartu Debet/Kredit yang besarnya ditentukan oleh bank.
d. Proses *settlement* adalah proses pengiriman data rekapitulasi oleh *Merchant* atas transaksi kartu kredit dan transaksi kartu maestro yang telah terjadi dari EDC di *merchant* ke sistem bank dan merupakan dasar penagihan transaksi kartu kredit dan transaksi kartu maestro dari

merchant kepada bank.

e. Sales Slip (*sales draft*) adalah formulir yang digunakan sebagai bukti *merchant* atas transaksi kartu kredit yang memuat keterangan mengenai lokasi dan nomor *merchant*, nomor kartu kredit, tanggal transaksi kartu kredit, nama dan tandatangan pemegang kartu kredit, jumlah seluruh transaksi kartu kredit dan kode persetujuan.

f. *Network Access* atau *Network Access Control* (NAC) adalah sebuah pendekatan terhadap jaringan komputer yang mencoba untuk menyatukan teknologi *endpoint*, otentikasi *user* atau sistem dan jaringan. NAC adalah suatu *software* yang merupakan sistem untuk menampung semua transaksi.

g. Base24/ON2 adalah *Switching System* . *System* ini dijalankan paralel /bersamaan untuk memastikan semua aktivitas di ON/2 bisa berjalan di Base24, *Switching System* sendiri adalah sistem yang menyediakan dukungan atau sistem untuk memilah jenis transaksi ATM, *Merchant*, dan *electronic banking* lainnya dan termasuk transaksi *routing* dan otorisasi, *Electronic Data Interchange, reporting* dan kontrol jaringan.

h. *Asscend* adalah *system processing/host* yang memproses transaksi kartu kredit/debit dan merchant yang terkoneksi dengan jaringan Visa International atau Mastercard. *Ascend* juga disebut juga dengan card manajemen sistem yang akan melanjutkan ke visa card atau mastercard international.

4.2.1 *Normal Online Transaction*

Sebagaimana telah disebutkan di bab sebelumnya bahwa *online* transaksi adalah dimana keadaaan EDC pada *merchant* terhubung secara langsung dengan sistem jaringan bank. Untuk lebih jelasnya staf Bank Permata (wawancara, 17 April 2011) menjelaskan bahwa proses transaksi bisa menggunakan transaksi debet dan kredit, digambarkan sebagai berikut.

a. Alur transaksi kartu plastik pada EDC *Merchant*:

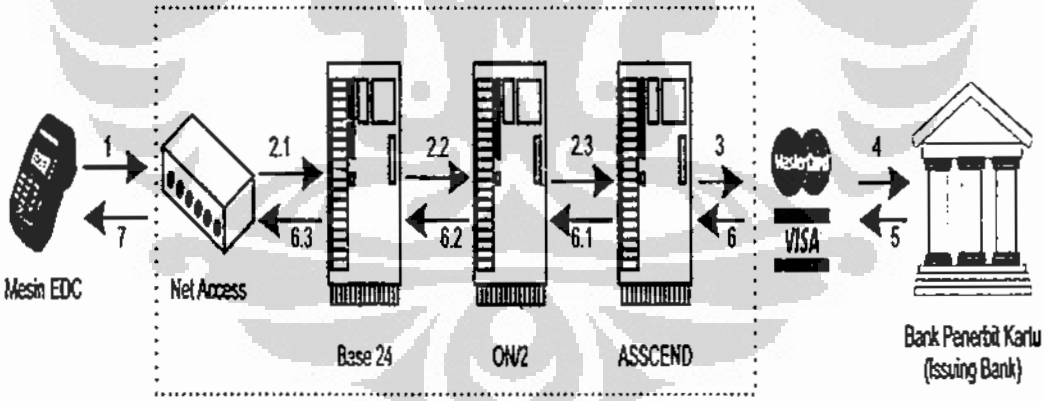
1. Pemengang kartu (*card holder*) datang ke toko, hotel atau tempat penjualan barang dan jasa lainnya (*merchant*). *Card holder* dapat

melakukan transaksi dengan dua cara yaitu dengan melakukan metode transaksi *swipe*[1](*magnegtic stripe*) dan DIP[2] pada ECD Bank Permata.

2. Pada layar EDC akan muncul tampilan sedang dalam pengolahan *(login processing)*. Kemudian pada tampilan jumlah pembayaran (*amount*) masukkan nominal transaksi dan tekan tombol enter.
3. Petugas *merchant* meminta *card holder* untuk memasukkan nomor *personal indetification number* (PIN) untuk proses otorisasi. Jika otorisasi pada *card holder* meggunakan tanda tangan (*signature autorizazion*), maka petugas *merchani* meminta *card holder* mendatangai pada layar EDC pada kolom *signature*.
4. Jika transaksi berhasil (*approval*), maka mesin EDC akan mencetak struk pembayaran.
5. Tekan tombol *enter* jika ingin mencetak struk ke-2 (*copy*), atau tekan tombol *clear* untuk kembali ketampilan awal.
6. Petugas *merchant* dan *card holder* memastikan nilai transaksi sesuai.

GAMBAR 20

NORMAL ONLINE TRANSACTION



Sumber: Wawancara dengan Manajer *Froud Kontrol* 2011

b. Sedangkan proses otorisasi transaksi *online* pada EDC internal Bank Permata dapat dijelaskan sebagai berikut:

[1] Swipe adalah activitas menggesekan kartu stripe kartu pada edc reader pada setiap merchant
[2] DIP adalah aktivitas memasukan kartu debet atau kredit serta karu lainnya pada setiap merchat

1. Pemegang kartu (*card holder*) baik kartu kredit maupun kartu debit mendatangi *merchant* untuk melakukan *swipe* maupun DIP.
2. Proses pada internal sistem Bank Permata
   2.1 Mesin EDC akan mengirim pesan permintaan otorisasi (*request authorization*) ke Base 24 eps melalui *Network access control* sebagai penampung semua transaksi elektronik Bank Permata.
   2.2 Base 24 eps akan memeriksa keamanan *terminal id* dan *Merchant id* apakah masih berlaku. Selanjutnya meneruskan ke ON/2.
   2.3 Jika kartu kredit dan debit akan diteruskan ke *Ascend*.
3. *Ascend* akan mengirim permintaan otorisasi, ke *acquiring bank*. Untuk kartu jenis visa akan dikirim ke visa card international dan jenis mastercard akan mengirimkan ke mastercard international.
4. Bank penerbit kartu memberikan persetujuan (ditolak/diterima) dan memberi jawaban ke visa atau mastercard internasional
5. Visa atau mastercard internasional akan mengirim permintaan otorisasi (*aurthorization request*) ke *Ascend*.
   5.1 *Ascend* meneruskan jawaban ke ON/2
   5.2 ON/2 akan mengirimkan keBase 24 Eps. Akan tetapi sebelumnya melakukan validasi terlebih dahulu, yang terdiri dari nomor kartu, masa berlaku masa berlaku kartu, *card validation value* (CVV) apabila kartu tersebut dikeluarkan oleh visa card atau *card validation code* (CVC) apabila kartu tersebut dikeluarkan oleh mastercard. Apabila sudah dinyatakan valid, maka akan dilakukan pengecekan kembali limit dari *cardholder* (apakah terpenuhi atau tidak).
   5.3 Base 24 eps akan mengirim respon ke NAC.
6. NAC akan meneruskan jawaban transaksi ke mesin EDC.

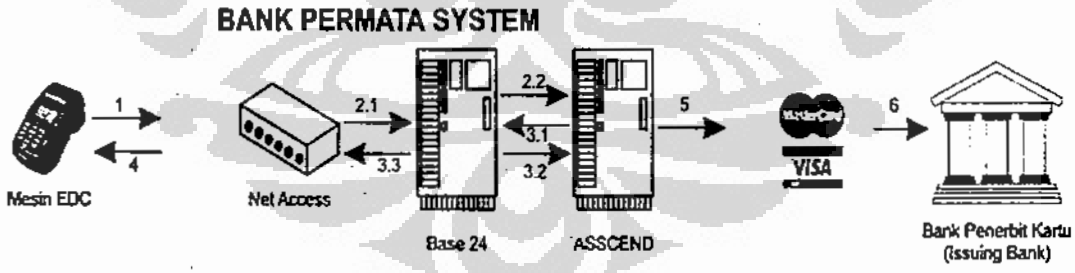
7. Pada layar EDC akan muncul *sales draft* dengan nomor kartu dan *approval code*, artinya sudah ada persetujuan dari bank penerbit dan transaksi *merchant* (Bank penerbit harus merespon paling lama 10 detik) dan EDC akan mencetak struk pembayaran dan data transaksi pembelajaan EDC akan disimpan dalam memori.

c. Penyelesaian (*Settlement*)

Semua transaksi di Merchant akan tersimpan (*save file*) mesin EDC. Setiap *merchant* bisa melakukan penyelesaian atau *settlement* setelah transaksi selesai. Namun menurut *Manajer Relation Merchant* (wawancara 18 April 2009) "pihak bank menyarankan pihak *merchant* untuk melakukan *settlement* satu kali sehari". Sedangkan pelaksanaannya masih banyak yang melakukan *settlement* pada setiap selesai transasaksi. Sedangkan proses *settlement* adalah sebagai berikut:

Gambar 21

ALUR SETTLEMENT



Sumber: Wawancara dengan Manajer Prod Kontrol 2011

Ketika transaksi *settlement* yang dilakukan oleh *merchant* kepada bank penerbit atau *issuing* bank dijelaskan sebagai berikut:

1. Mesin EDC mengirim data *settlement* atas transaksi yang disetujui melalui NAC.
2. Proses pada sistem internal Bank Permata.

2.1 Oleh NAC akan diteruskan ke Base 24eps.

2.2 Base 24 selanjutnya meneruskan ke ON/2

2.3 Jika kartu kredit atau debit bank lain akan diteruskan ke *Ascend*

3. *Ascend* akan menyimpan *file settlement* tersebut dan memberikan jawaban ke mesin EDC.

3.1 jawaban di kirim ke base 24eps

3.2 Base 24eps akan membuat *report settlement* dan *Asscend* akan membuat *report* pembayaran merchant.

3.3 Base 24eps akan meneruskan jawaban data *settlement* ke NAC

4. NAC akan meneruskan jawaban *settlement* dari *Ascend* ke mesin EDC yang kemudian mencetak slip *settlement*.

5. *Ascend* akan meneruskan data *settlement* ke Visa atau Mastercard intenasional.

6. Visa atau mastercard internasional meneruskan data *settlement* ke bank penerbit kartu dan mendebit rekening bank penerbit kartu visa atau mastercard internasional dan mengkredit rekening Bank Permata di visa atau mastercard internasional.

Sementara itu pada saat proses pembayaran oleh *issuing* bank kepada kepada *merchant* (*merchant payment*), sebagai berikut:

1) Pada saat proses yang sama Base 24 eps mengirim *file* penyelesaian mutasi-mutasi transaksi ke *Ascend*, Base 24 eps juga menulis laporan.

2) Laporan transaksi akan dikirim ke *Ascend* dan menyusun laporan

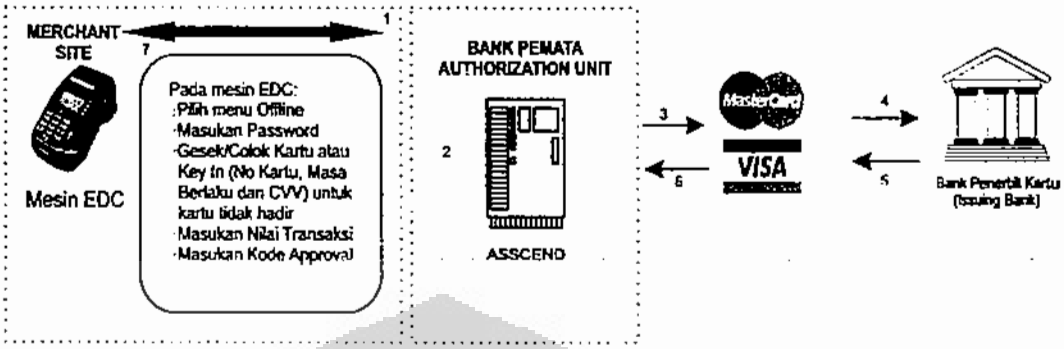
3) Laporan akan digunakan oleh unit pembayaran untuk membayar *merchant* berdasarkan laporan pembayaran *merchant* di *Ascend*.

4.2.2 *Normal Offline Transaction*

Menurut staf Bank Permata transaksi *offline* secara normal dilakukan adalah ketika *card holder* akan menggunakan EDC pada *merchant*, cukup dengan memberikan informasi kepada *merchant* tentang nomor kartu dan masa berlaku, serta *Card Value* tanpa melakukan *Swipe* maupun DIP. Normal transaksi *offline* dapat digambarkan sebagai berikut:

Gambar 22

NORMAL OFFLINE TRANSACTION



Sumber: Bank Permata 2011

1. *Merchant Site* (Toko) akan menelepon *(call autorization unit*) ke *acquiring bank (autrorization bank*),
2. Petugas otorisasi Bank Permata menginput data *card holder* dan data transaksi akan di input melalui *Ascend;*
3. *Ascend* akan mengirim dan meminta persetujan dari visa atau mastecard.
4. Visa atau mastercard international dakan meneruskan ke *issuing bank*, misalnya (toka a menelpon ke *acquiring* bank untuk *aprroval code*) dan sama seperti transaksi *online*.
5. Bank penerbit akan memberikan jawaban.
6. Jawaban akan diteruskan ke *Asscend.*
7. Petugas autorisasi akan berdasarkan data di *Ascend* menginformasikan data transaksi jika transaksi disetujui petugas *merchant* atau pemilik *merchant* melakukan langkah-langkah transaksi *offline* berdasarkan data berdasarkan data *Asscend* yaitu:
   (a) Pilih menu *offline* pada EDC;
   (b) Masukkan *password* pada EDC;
   (c) Gesek kartu magnetik baik secara *swipe* maupun DIP;
   (d) Masukkan nilai transaksi;
   (e) Masukkan kode *approval.*

Kemudian alur transaksi *offline* dan sistem *settlement* serta pembayaran dijelaskan oleh *Manager Business Unit* (wawancara, 13 April 2011), berikut ini.

> Pada saat toko itu mengirim *settlement*, dan bank langsung membayarkan tagihan kepada *merchant*. Padahal visa atau mastercard belum membayar kepada bank penerbit (Bank Permata, artinya dana (*settlement*) ditanggung terbih dahulu oleh bank penerbit, setelah 1 hari atau 2 hari maka bank pengelola (visa atau master card) akan membayar kepada bank penerbit (Bank Permata). Sedangkan proses *settlement* dan pembayarannya sama dengan *settlement* dan pembayaran pada transaksi *online* normal.

Dari beberapa sistem pengamanan pada alur atau proses transaksi yang diuraikan baik secara *online* maupun *offline* di atas, ada juga bagian pengawasan yang mengamankan alur atau proses transaksi, *settlement* dan pembayaran baik secara *online* maupun *offline* yaitu unit *Froud Control*. Menurut *Froud Control Officer* (Wawancara 19 April 2011) Tugas *Froud Control* terdiri dari 1) menganalisa transaksi yang mencurigakan; 2) melakukan konfirmasi kepada *merchant* dan mengklarifikasinya; 3) konfirmasi terhadap bank penerbit untuk mendapat klarifikasi transaksi; 4) mengajukan transaksi pembayaran kepada *merchant* ditunda dan ditutup jika diperlukan apabila terjadi transaksi yang mencurigakan; 5) mengajukan agar membayarakan *settlement* yang dilakukan *merchant* apabila tidak terdapat bukti penundaan pembayaran; dan 6) mempersiapkan laporan bulanan terkait penundaan pembayaran kepada *settlement merchant*.

Pada operasionalnya pengawasan Transaksi yang mencurigakan oleh unit *Froud Control* ini dilengkapi perangkat komputer jenis *personal computer* (PC) yang dilengkapi dengan sistem (*software*) GMONA. Menurut Manajer *Froud Control* (wawancara, 17 April 2011) GMONA adalah " sistem yang dipasang untuk mendeteksi transaksi-transaksi sesuai dengan *rule*". Lebih jelasnya oleh Manajer *Froud Control* (wawancara, 17 April 2011) pada layar PC dapat dilihat nama *merchant*, *merchant* - ID, nilai transaksi, tanggal dan waktu transaksi serta kode otorisasi.

Pengawasan dan analisa transaksi dilakukan setiap hari untuk mengamati transaksi yang mencurigakan. Apabila menemukan transaksi yang mencurigakan, maka unit *froud control* ini akan melakukan konfirmasi terhadap *merchant* yang bersangkutan. Selain melakukan konfirmasi terhadap *merchant*, melakukan konformasi juga kepada bank penerbit (baik kartu debit maupun kredit) untuk

bank lokal konfirmasi mengunakan atau via telephone, sedangkan untuk bank luar negeri konfirmasi menggunakan atau via fax dan email.

Jika ditemukan transaksi yang mencurigakan Unit *Froud Control* dapat memerintahkan Unit Pembayaran untuk membatalkan pembayaran kepada *merchant* atau meng-*hold* melalui emal atau fax dengan format tertulis tegas manajer *Froud Control* (wawancara, 17 April 2011). Untuk menguatkan pembatalan tersebut melakukan pengumpulan data dan *sales draft* dari *merchant*, jika dibutuhkan, maka unit *Froud Investigation* akan melakukan penyelidikan secara fisik atau turun kelapangan dan membuat laporan-laporan terhadap Transaksi mencurigakan yang dituangkan dalam laporan investigasi.

Sementara itu, yang dimaksud Transaksi yang mencurigakan dalam hal ini adalah transaksi tidak wajar. Sebagaimana dijelaksan oleh Manajer *Froud Analisys* (Wawancara 19 April 2011) transaksi tidak wajar tersebut misalnya:

> 1) yang dilakukan pada malam hari tidak sesuai dengan jenis produk yang ada pada *merchant* atau toko tempat bertransaksi; 2) 2 kartu yang berbeda, 1 *approve*, dan satu *pick-up* harus dilakukan konfimasi; 3) *merchant* baru yang mempunyai transaksi dalam jumlah besar per-hari; 4) *merchant* yang bergerak dalam bidang perdagangan kecil namun transaksi hariannya besar; dan 5) transaksi yang sangat berbeda dari kebiasaan transaksi sebelumnya.

Dalam pada itu banyaknya transaksi yang diawasi sekitar 2000 transaksi per-harinya diseluruh Indonesia. Hal ini dilakukan di kantor Bank Permata Bintaro Jakarta.

Hal ini sesuai dengan bidang tugas dari Unit *Froud Control* yang bertugas melakukan pengawasan, deteksi, dan investigasi terhadap jalannya transaksi pada EDC di *Merchant* Bank Permata. Sebagaimana dikuatkan oleh data yang diperoleh dari *profile company* Bank Permata (2011) tentang tugas *Froud Control* sebagai berikut:

a. Meninjau, menganalisis, dan investigasi *merchant* kepada semua pontensi penipuan oleh pedagang.
b. Menahan pembayaran kepada *merchant* untuk mencegah dan menimbulkan *fraud banking* serta kerugian akibat *chargeback* dari bank penerbit.
c. Meninjau dan melacak *chargeback* untuk setiap transaksi di *merchant*.

d. Membuat lapiran transaksi perdagangan di *merchant*.

4.3 Faktor-faktor Yang Mempengaruhi Terjadinya *Fraud Banking* di *Merchant* Bank Permata.

Penyebab terjadinya *fraud banking* melalui transaksi elektronik pada EDC Bank Permata dilihat dari dua aspek, yaitu proses pengajuan *merchant* dan proses transaksi elektronik. Yang dimaksud sistem pengaman transaksi elektronik adalah sistem pengamanan dimulai dari menggunakan kartu palstik (Kartu Kredit atau debit) sampai kepada proses otorisasi atau persetujuan dari pihak bank, dalam hal ini adalah Bank Permata.

4.3.1 Faktor Proses Akuisisi *Merchant* Bank Permata.

Untuk meningkatkan pelayanan kepada nasabah dan meningkatkan keuntungan (*profitable*) Bank Permata, menurut *Manager Fraud Control* (wawancara , 6 April 2011) MRO atau juga bisa disebut *Sales Merchant Unit* melakukan mendatangi langsung (*kanvasing*) untuk mencari pemohon *merchant*. Akan tetapi jumlah karyawan yang bekerja sebagai tenaga sales *merchant* tersebut tidak memenuhi, sehingga mengaharuskan Bank Permata merekrut tenaga sales kontrak (*outsourching*). *Sales Outsourching* ini hanya dikontrak untuk waktu beberapa tahun dan dapat diperpanjang apabila sales tersebut dianggap baik.

Namun menurut *Manager Fraud Control* (wawancara , 6 April 2011) *sales outsourcing* ini tidak mendapatkan pendidikan yang diselenggarakan oleh Bank Permata seperti karyawan tetap (*inhouse*). Sales ini hanya diberikan pelatihan dan pengetahuan tentang *merchant* dan selanjutnya ditugaskan untuk mencari nasabah (pemohon *merchant*) sebanyak-banyaknya. Dalam pada itu tenaga kontrak ini akan dinilai baik atau tidaknya tergantung target untuk memperoleh nasabah bank yang ditetapkan oleh Bank Permata. Sehingga setiap sales berlomba-lomba untuk mencari nasabahnya untuk memenuhi target yag dibebankan kepadanya.

Sebagaimana menurut *sales merchant 1* (wawancara, 10 Februari 2011) dijelaskan:

> Sekitar akhir oktober 2009 pada sore hari ada seseorang yang menelepon bagian *merchant* Bank Permata Cabang Melawai Jakarta Selatan, seseorang tersebut mengaku bernama Tony dan menanyakan bagaimana

> caranya apabila ingin mengajukan pemasangan mesin EDC baru Bank Permata dan apa saja persyaratannya. Kemudian saya jelaskan cara pengajuan mesin EDC harus memiliki SIUP, NPWP, KTP, mengisi formulir atau dokumen *merchant data form* (MDF) dan perjanjian kerjasama (PKS). Kemudian saya diminta datang ke toko Pretty Mom di Mangga Dua Square, untuk mengambil data-data yang akan digunakan sebagai persyarakatan pengajuan EDC di Bank Permata. Data-data tersebut adalah SIUP No. 03203/1.824.51 atas nama perusahaan *Pretty Collection*; NPWP No. 79.858.604.6-026.000 atas nama Tony ; KTP no 09.5203.200475.0124 atas nama Tony; MDF dan PKS yang telah diisi serta ditandatangani.

Data-data tersebut kemudian diajukan kepada *Merchant Relation Manager* sampai kepada *Head of Merchant Acquring* untuk mendapat persetujuan. Selanjutnya data itu dikirim ke Bank Permata Cabang Bintaro bagian *usage dan support* untuk diverifikasi ulang oleh APC, kemudian dikirim ke bagian *Technical Support* untuk penerbitan mesin EDC. Setelah mesin EDC siap, saya antar ke Mangga Dua Square untuk memasang instalasi mesin EDC tersebut. Dan yang terakhir saya melakukan *training* dengan memberikan contoh transaksi satu juta rupiah menggunakan kartu *testing* yang saya bawa dimulai dari: pembatalan transaksi, penyelesaian transaksi, transaksi penggunaan kartu kredit dan debit, serta cara membedakan kartu palsu.

Dalam pada itu *Sales Merchant 1* (wawancara, 10 Februari 2011) mendapat pesanan kembali dari empat toko lainnya untuk mengajukan akuisisi *merchant* melalui *Merchant* Pretty Mom. *Sales Mechant 1* menjelaskan proses pengajuannya adalah berikut ini.

> Pada 5 November pemohon *Merchant* Toko Pretty Mom yang telah di setujui merefercnsikan rekannya untuk mengajukan mesin EDC. Setelah itu saya pergi ke Toko Pretty Mom bersama dengan *Sales Merchant* 2. Setelah tiba pemiklik Toko tersebut telah mempersiapkan dokumen aplikasi *merchant* sebanyak 4 dokumen, yaitu toko Hongkong, Padma Collection, San-san dan Vercases. Dokumen tersebut telah dilengkapi dengan KTP, NPWP, SIUP, MDF dan PKS sesuai dengan persyaratan yang ditentukan oleb Bank. Kemudian dokumen tersebut saya proses ke Bank Permata dan akhirnya disetujui. Selanjutnya setelah EDC siap, saya antar ke pemilik Toko Pretty Mom dan *Merchant* Rizki Boutiqe dan bukan ke pemobon langsung sesuai dengan dokumen yang diajukan.

Sementara itu *Sales Merchant* 2 (wawancara, 12 Februari 2011) mengemukakan hal itu dilakukan "untuk mengejar target yang dibebankan Bank Permata kepada saya". Selain tidak dilakukan verifikasi atau investigasi pada pemohon *merchant*, setelah EDC siap, tidak dilakukan *training*, alasannya mereka sudah mengerti melakukan transaksi dengan menggunakan EDC. Namun sehari setelah penyerahan EDC, akan dilakukan pengecekan. Hasil yang diketahui dari monitor komputer ada beberapa jumlah transaksi yang cukup besar, yaitu Rp. 50.000.000,- ; Rp. 40.000.000; Rp. 80.000.000,-; dan Rp. 90.000.000,- . "Selanjutnya transaksi tersebut dilakukan selama 2 minggu sekali oleh mereka, sementara saya hanya membiarkan saja dan tidak melakukan tindakan apapun transaksi yang tidak wajar itu" (*Sales Merchant* 2, 12 Februari 2011).

Proses akuisisi *merchant* yang dilakukan oleh *Sales Merchant* 1 maupun 2 diatas, menurut *Manager Fraud Banking* (wawancara, 6 April 2011) "telah menyalahi prosedur." Seharusnya Dokumen pengajuan tersebut di verifikasi terlebih dahulu dan *Sales Merchant* bertemu langsung dengan calan nasabah (pemohon *Merchant*) walaupun ada referensi dari *customer* sebelumnya. Dan apabila tidak diverifikasi ada celah dokumen yang diserahkan asli tapi palsu. Artinya ada pemalsuan identitas atau data-data yang dimuat dalam data tersebut fiktif. Karena *Acquiring Processing Control* (APC) hanya verifikasi kelengkapan data, akibatnya pengajuan disetujui dan dikeluarkan mesin EDC untuk keempat *Merchant* tersebut.

Kemudian terjadinya *fraud banking* bukan hanya atas kesalahan dari proses akuisisi EDC atau *merchant,* akan tetapi disebabkan juga oleh para nasabah yang memindah tangankan atau meminjamkan EDC kepada orang lain tanpa persetujuan bank. Sebagaimana dijelaskan dalam hasil berita acara pemeriksaan saksi 1 (Dit Krimsus Polda Mentro jaya 2010) menjelaskan:

> Pada pertengahan November 2008 saudara A meminjam EDC dengan alasan untuk melakukan transaksi namun pada saat itu saya tidak menyetujuinya, namun sekitar akhir bulan nopember saudara A datang lagi untuk meminjam mesin EDC, dengan transaksi harian minimal Rp. 50.000.000,- atau lima puluh juta rupiah per-harinya, dan bersedia mengganti Rp 3.500.000,-. Kemudian setelah dipertimbangkan karena toko saya tidak produktif lagi, maka saya meminjamkan kepada saudara A.

Begitu juga yang terjadi pada saksi B dengan dalam berita acara pemeriksaan penyidik (Dit Krimsus Polda Metro Jaya 2011) saya meminjamkan EDC pada saudara A dengan alasan tidak produktif dan mendapat imbalan dari hasil meminjamkan EDC.

Hal itu juga dikuatkan oleh A (Wawancara 28 April 2011) " Memang saya meminjam EDC tersebut dengan tujuan melakukan transaksi fiktif atau *fraud banking*.". EDC yang dipinjam kemudian di proses kloning sehingga apabila melakukan transaksi atau *settlement* seolah- sesuai dengan *rule* yang diterapkan oleh Bank Permata.

Dari beberapa penyebab *fraud banking* di atas memungkinkan atau memberi peluang kepada pelaku untuk melakukan *hacking* terhadap mesin EDC. Sebagaimana dijelaskan oleh *Manajer Froud Control* (wawancara 12 April 2011) "proses akuisisi yang tidak sesuai prosedur, kehilangan EDC atau dipindah tangankan merupakan faktor penyebab terjadinya *fraud banking* yang ada di Bank Permata. " adapun beberapa transaksi fiktif yang menimbulkan kerugian bagi Bank Permata adalah sebagai berikut:

Tabel 1

Data Transaksi Fiktif

NO	Tanggal Transaksi	Jumlah Transaksi
1.	01 Desember 2009	Rp. 46.199.160,-
2.	02 Desember 2009	Rp. 58.663.780,-
3	03 Desember 2009	Rp. 68.398.120,-
4	04 Desember 2009	Rp. 82.584.600,-
5	07 Desember 2009	Rp. 94.619.000,-
6	08 Desember 2009	Rp. 190.972.600,-
7	09 Desember 2009	Rp. 93.114.700,-
8	10 Desember 2009	Rp. 89.915.000,-
9	11 Desember 2009	Rp. 92.889.300,-
10	15 Desember 2009	Rp. 95.394.180,-
11	16 Desember 2009	Rp. 94.810.100,-
12	17 Desember 2009	Rp. 94.952.000,-
13	22 Desember 2009	Rp. 95.760.900,-
14	23 Desember 2009	Rp. 96.427.100
15	24 Desember 2009	Rp. 96.532.450
16	28 Desember 2009	Rp. 96.108.600,-
17	29 Desember 2009	Rp. 94.279.000,-
18	30 Desember 2009	Rp. 94.496.500,-
	JUMLAH	Rp. 1.710.495.500,-

Sumber: Dit Krimsus Polda Metro Jaya 2011

4.3.2 Faktor Proses Transaksi Elektronik

Proses transaksi elektronik pada EDC meliputi: proses transaksi baik *online* maupun *offline*, *settlement* dan pembayaran (*payment*). Pada mesin EDC hanya memiliki sistem pengamanan berupa *password* atau *signature* pemilik kartu (*card holder) (Manajer Froud Control*, 12 April 2011). Sehingga apabila *password* dan *signature* cocok akan diteruskan ke *network access control* (NAC) . Sedangkan NAC yang berfungsi sebagai penampung semua transaksi elektronik pada Bank Permata yang akan mengidentifikasi kesesuaian *Merchant-Id* (M-ID) dan T-ID sehingga akan diteruskan ke Base 24 eps dan On/2. Kemudian sistem *Ascend* yang hanya berfungsi sebagai manajemen *card system* yang akan meneruskan ke visacard dan mastercard international.

Uraian di atas menjelaskan sistem pengamanan pada transaksi elektronik tersebut hanya pada mesin EDC , NAC serta Base-24 eps. Sistem pengamanan tersebut telah dimanfaatkan oleh *hacker* untuk mengkloning mesin EDC, dengan cara merubah sistem EDC dan menyimpan data transaksi yang siap dilakukan penagihan (*settlement*) (*Manager Froud Control*, 12 April 2011). Artinya transaksi pembelian barang atau jasa tidak pernah dilakukan namun *sales draft* atau seluruh transaksi terekam dan tersimpan pada mesin EDC. Sehingga pada saat *settlement* melalui mesin EDC oleh pelaku kejahatan, langsung dapat di proses oleh sistem NAC maupun EDC, karena yang dilakukan hanya mengidentifikasi M-ID atau T-ID Mesin EDC dan batas minimum atau limit transaksi yang ditagihkan oleh *merchant* kepada Bank Permata.

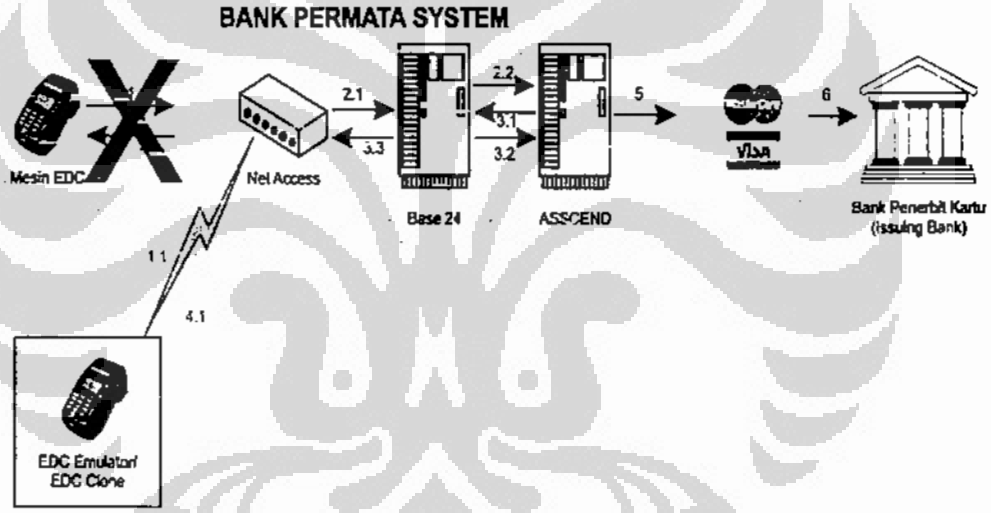
Sebagaimana dikuatkan oleh keterangan pelaku kejahatan *fraud Banking* dalam berita acara pemeriksaan tersangka (Dit Krimsus Polda Metrojaya 2010):

> EDC tersebut di Kloning, artinya saya meminta seorang ahli komputer untuk merubah sistem proses transaksi tanpa melakukan proses transaksi, hanya tinggal memasukan angka atau nominal yang diinginkan untuk melakukan proses *settlement* secara *offline* kepada Bank Permata. Hal ini diketahui setelah saya mempelajari mulai dari proses akuisisi *merchant* dan transaksi elektronik pada EDC dari teman saya. Ternyata pada mesin EDC tidak ada sistem pengamanan yang baik, melainkan pengamanan hanya *password* atau tandatangan ketika pemilik kartu akan menggunakan kartu tersebut.

Sementara itu, *Manager Froud Control* (wawancara, 12 April 2011) menjelaskan "memang tidak ada pengamanan lain, selain *password*, *signature* dan identifikasi M-id dan T-ida pada NAC serta Base 24 eps." Sehingga memungkinkan terjadi fraud banking dengan menggunakan transasksi fiktif dan *settlement* secara *offline* pada EDC (*offline fraud settlement transaction*) tanpa melalui tahapan- tahapan yang sesuai dengan *rule* yang dtetapkan pel Bank Permata baik secara *online* maupun *offline*. *offline fraud settlement transaction* tersebut dapat digambarkan sebagai berikut:

GAMBAR 23

OFFLINE FRAUD SETTLEMENT TRANSACTION



Sumber: hasil wawancara dengan Manajer *Froud Control* di kembangkan oleh peneliti 2011

Transaksi maupun *settlement* seharusnya dilakukan seperti pada angka 1 berwarna hitam, akan tetapi Transaksi maupun *settelement* dilakukan pada angka 1 berwarna merah. Pada angka 1 berwarna merah EDC yang sebenarnya tidak pernah mengirim *settlement* (sebagian EDC hilang atau dipindahtangankan dan sebagian EDC tidak melalui proses akuisisi yang ditetapkan Bank Permata). *Settlement* dilakukan pada EDC hasil *clone*, dalam hal ini disebut dengan EDC *emulator* yang dirancang oleh pelaku *fraud banking* (*fraudster*).

Selanjutnya *settlement* dari EDC *Emulator* yang dilakukan oleh *fraudster* diterima oleh NAC pada angka 2 (manajer *fraud Analis*, 20 April 2011). Kemudian akan diteruskan ke base 24 eps untuk melakukan pengecekan identitas *merchant* (M-ID) dan Nomer EDC (*terminal Identitiy*- T-ID) karena dianggap syah atau valid maka diteruskan ke *ascend* pada angka 2 untuk menerima data *settlement* dari Base 24. Kemudian *ascend* mengirim jawaban *settlement* sukses ke Base24, Saat bersamaan Base24 membuat *report settlement* dan dikirim ke *ascend* dan *ascend* membuat *report* pembayaran *merchant*. Saat yang sama juga Base24 menerukan jawaban sukses dari *Ascend* ke NAC. NAC tidak pernah mengirim jawaban *settlement* sukses ke EDC melainkan Jawaban *settlement* sukses terkirim ke EDC *emulator/clone*, sehingga *asscend* mengirim data *settlement* ke Visa International (angka 5). Dan visa internasional melakukan penagihan kepada bank penerbit pengkreditan ke rekening Bank Permata dan mendebet atau menarik rekening bank penerbit kartu di Visa International.

Ketika Pembayaran ke *merchant* atas *offline fraud settlement* dilakukan setelah *Ascend* menerima data *settlement* dari Base 24. *Ascend* mengirim jawaban *settlement* sukses ke Base24 dan Base24 membuat *report settlement*. *Report settlement* di kirim ke *ascend* dan *ascend* membuat *report* pembayaran *merchant*. Berdasarkan *report* pembayaran *merchant* (angka 4 berwarna merah), Unit *payment* melakukan pembayaran ke rekening *merchant* satu hari setelah proses *settlement*.

BAB 5
ANALISA DAN PEMBAHASAN

5.1 Analisis Manjemen Pengamananan Sistem Informasi Merchant Bank Permata.

Informasi telah mengambil bagian penting pada setiap aspek kehidupan. Sebuah dalil menyebutkan siapa yang menguasai informasi, maka dialah yang menguasai dunia (Hadiman 2010). Sehubungan dengan hal tersebut mengandung sebuah makna, betapa penting dan tingginya nilai suatu informasi mendukung kelancaran pada setiap aktivitas kehidupan. seseorang yang memiliki informasi lebih berada pada posisi yang di untungkan, dan sebaliknya yang memiliki informasi sedikit berada pada posisi yang dirugikan.

Namun informasi yang dimiliki, tidak seharusnya disebarluaskan begitu saja, atau dapat diakses oleh setiap orang. Ada bagian-bagian tertentu dari informasi yang harus di rahasiakan dan dijaga dari sesuatu hal, agar tidak terjadi penyalahgunaan peruntukannya, atau bahkan merusak informasi tersebut. Maka dari itu perlu meningkatkan sistem teknologi informasi untuk menjamin keberlangsungan usaha. Sebagaimana Simanjuntak (2010, hlm. 16) mengemukakan " Penerapan teknologi maju merupakan kebutuhan nyata untuk kemudahan dan percepatan proses produksi."

5.1.1 Analisis Manajemen Sistem Pengamanan Informasi Pada Akuisisi Merchant Bank Permata.

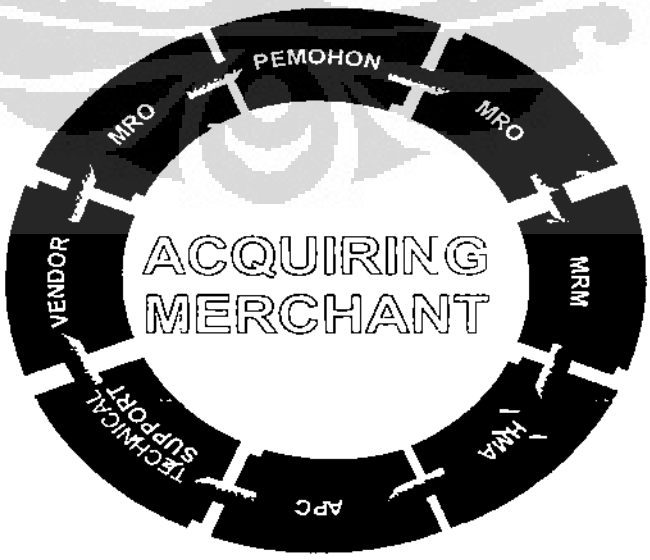
Bank Permata dalam meningkatkan usaha di bidang perbankan untuk mendapatkan *profitable* telah mengembangkan layananan produk berbasis teknologi informasi yaitu transaksi elektronik (*e-commerce*), dalam hal ini sistem *merchant*. Namun sistem *merchant* Bank Permata tersebut harus didukung oleh manajemen pengamanan sistem informasi yang baik. Sehingga dapat mencegah terjadinya kerugian dan mencegah terjadinya kejahatan. Sebagaimana telah terjadi *fraud banking* yang telah dilaporkan di Polda Metro Jaya 2010, dan menyebabkan kerugian sebesar 70 milyar.

Oleh karena itu hasil penelitian sistem pengamanan proses akuisisi *merchant* ini akan dianalisis menggunakan teori triad atau CIA, sebagaimana Ken M. Shaurette (2006) mengemukakan untuk mengelola resiko terhadap pengamanan informasi melihat 3 aspek yaitu integritas, kerahasiaan, dan ketersediaan.

Proses pengajuan atau permohonan *merchant* oleh pemohon (pedagang, toko, dan jasa lainnya) bisa melalui *call center* nomor 63399 atau 0217456888 Bank Permata atau melalui *Marketing Relation Officer* (MRO). Setelah itu MRO akan mendatangi pemohon *merchant* dengan memberikan formulir atau aplikasi yang haris diisi dan dipenuhi. Aplikasi tersebut disebut dengan *merchant data form* (MDF). Tahap pertama Pemohon harus mengisi nama *merchant*, alamat, asal kota, nama bank, rekening penampung *merchant*, nama perusahaan, ukuran hisnis, dan memberikan *fotocopy* persyaratan persyaratan KTP, KITAS bagi warga asing, Nomor Pokok Wajib Pajak (NPWP), Surat Ijin Usaha Perdagangan (SIUP), Akte, dan perjanjian kersama antara pihak pemohon dengan bank penerbit, dalam hal ini Bank Permata. Selain itu juga menandatangani perjanjian kerjasama. Selanjutnya apabila persyaratan yang diajukan pemohon lengkap maka akan diproses oleh Bank Permata. Berdasarkan hasil penelitian alur proses *acquiring merchant* dapat digambarkan sebagai berikut:

Gambar 24

Proses Acquiring Merchant



Sumber: Penulis 2011

Persyaratan yang dilengkapi pemohon merupakan data yang penting bagi Bank Permata dalam proses akuisisi *merchant*. Sehingga Menurut Ken M. Shaurette (2006) data tersebut harus mempunyai integritas, yang dimaksud adalah menjaga keakuratan dan kelengkapan informasi serta cara memproses informasi tersebut. Walaupun proses *acquring merchant* terdiri dari beberapa tahap atau *layer*, namun pada proses awal yaitu mengisi aplikasi dan menyerahkan persyaratan, yang diminta hanya *fotocopy* tanpa diminta atau menunjukan yang aslinya. MRO tidak pernah melakukan verifikasi data yang diterima akurat dan lengkap secara legalitas apakah data itu asli atau tidak, melainkan kelengkapan persyaratan tersebut hanya formalitas sehingga begitu lemah sistem pengamanan pada tahap awal ini, yang akan berpengaruh terhadap tahap selanjutnya.

Setelah dinyatakan lengkap secara formalitas, MRO akan menyerakan atau diteruskan kepada *Manager Relation Merchant* (MRM). Kemudian MRM melakukan verifikasi kembali dan ditanda tangani. Verifikasi yang dilakukan oleh MRM sendiri hanya melihat kelengkapannya saja, apakah KTP, KITAS bagi warga asing, Nomor Pokok Wajib Pajak (NPWP), Surat Ijin Usaha Perdagangan (SIUP), Akte, dan perjanjian kersajama antara pihak pemohon dengan bank penerbit sudah terpenuhi. Sedangkan keakuratan data tersebut diabaikan, sehinga secara legalitas keaslian *fotocopy* persyaratan tidak diperhatikan pada tahap kedua.

Pada tahap ketiga, MRO meneruskan ke *Head of Merchant Aquiring* (HMA). Karena HMA ini merupakan level pimpinan, ketiga data yang diberikan oleh MRM dianggap sudah memenuhi baik keakurannya maupun kelengkapannya sehingga HMA hanya menandatangani untuk diteruskan kebagian atau unit APC. Unit APC ini merupakan tahap keempat dari proscs akuisisi *merchant*.

Unit ini berfungsi melakukan input data ke Base24 eps atau On2 dan *Ascend*, pemeriksaan terhadap kelengkapan dan keakuratan data pemohon *merchant*. APC juga melakukan pemeriksaan (*cheking blacklist*) status nasabah apakah bermasalah atau tidak ke Bank Indonesia (BI). Namun pada pemeriksaan inipun tidak menjamin keamanan dari proses akuisisi *merchant*. Karena BI hanya melakukan pemeriksaan dan pengecekan bagi nasabah yang sudah terdaftar sebelumnya, sehingga apabila pemohon *merchant* baru atau tidak pernah terdaftar

di bank manapun maka BI tidak akan menemukan daftar hitam atau pemohon tersebut bermasalah. Jadi unit ini berfungsi apabila pemohon *merchant* pernah cacat atau bermasalah dengan semua bank, karena setiap orang datanya akan terekam di BI. sehingga data tersebut tidak mempunyai nilai tinggi (*confidentiality*) (Ken M, Shaurette 2006), artinya bisa saja orang yang mengajukan atau pemohon *merchant* bukan orang yang sebenarnya bermasalah atau bukan orang yang berhak.

Tahap kelima APC menandatangi permohonan orde EDC ke unit *Tecnical Support* (TS). TS akan segara memproses permintaan APC tentang order EDC tersebut. Fungsi TS memesan kepada *vendor* EDC dan melakukan penginputan data baru (*new record data*) berdasarkan *serial number* (s/n) mesin EDC ke sistem (EDC *Very Centre*), kemudian melakukan penginstalan pada mesin EDC dan *Input Master Key* EDC, serta melakukan tes transaksi *online* secara *dual control*. Penginputan data baru (*new record data*) berdasarkan *serial number* (s/n) mesin EDC ke sistem EDC *Very Centre* agar pada saat proses transaksi nanti, EDC ini dikenal oleh sistem yang mengatur transaksi baik di Base 24 maupun di *Ascend*. Sedangkan *master key* adalah *password* yang akan diberikan kepada pemohon *merchant*, yang bertujuan untuk proses otentikasi dan mengamankan pada transaksi *settlement* di *merchant* Bank Permata.

Namun *password* tersebut hanya mengamankan EDC supaya tidak jatuh atau tidak digunakan oleh orang yang tidak berhak. Sedangkan bagi pengamanan sistem informasi internal bank sendiri begitu lemah, merujuk teori CIA dari Ken M, Shaurette (2006) sistem pengamanan harus memenuhi aspek ketersediaan (Availability) jika ada seseorang atau *hacker* yang dapat melacak *password* tersebut menajamin ketersedian data atau informasi pihak yang berwenang dapat mengakses data yang akurat pada saat dibutuhkan dengan menggunakan jaringan komputer. sehingga dalam sistem pengembangan keamanan selain otentikasi diperlukan *coding* dan *encryption*, sehingga benar-benar aman *(Lim and Bazavan* 2006). Tahap terakhir akan diberikan kepada vendor dan MRO untuk melakuan penginstalan, namun dalam tahap ini tidak ada fungsi pengawasan yang mengawasi apakah EDC diberikan kepada pemohon langsung atau orang lain.

5.1.2 Analisis Manajemen Pengamanan Sistem Informasi Transaksi Elektronik *Merchant* Bank Permata.

Transaksi elektronik pada EDC di *merchant* Bank Permata dilakukan dengan dua cara yaitu *on-line* dan *off-line* transaksi. Sebagaimana telah dijelaskan pada bab 4 proses transaksi elektronik teridiri dari : proses transaksi pembelian, penagihan (*settlement*), dan pembayaran (*payment*). Dari alur atau proses transaksi ini melibatkan pihak dalam perusahaan, dalam hal ini Bank Permata sendiri dan pihak luar dalam hal ini orang-orang yang mempunyai kepentingan (toko, nasabah, dan stakeholder lainnya). Sebagaimana Kadir (2003) informasi tidak hanya digunakan untuk kepentingan internal organisasi, melainkan digunakan juga untuk kepentingan diluar organisasi (eksternal).

Pemakai internal meliputi manajemen paling bawah sampai kepada manajemen tingkat atas, sedangkan eksternal dapat berupa pelanggan, pemegang saham, pemasok, mitra kerja, pegawai pajak, dan *stakeholder* lainnya yang terkait dengan *merchant* Bank Permata (Simanjutak 2009, Kadir 2009). Sistem transaksi ini merupakan sistem dihubungkan dengan lingkungan melalui arus sumber daya disebut dengan sistem terbuka (*open system*) dan sistem tertutup yang dihubungkan dengan sistem internal (*closed system*) (Raymond Mcleod 1998).

Karena sistem transaksi elektornik EDC di *merchant* Bank Permata ini merupakan sistem terbuka dan tertutup, pihak Bank Permata mempunyai pengamanan transaksi dengan menggunakan teknologi informasi berbasis komputer. Mendasari hasil penelitian pengamanan dilakukan dimulai dari transaksi pembelian barang atau jasa dan *settelment* dengan menggunakan aplikasi komputer dimulai dari mesin EDC, *Network Ascess Control* (NAC), Base24 dan On2, dan *ascend* yang merupakan suatu sistem yang bekerja saling terkait satu sama lainnya, sehingga proses transaksi ini begitu cepat kurang lebih sepuluh detik (Catatan lapangan, 13 April 2010).

Pada saat proses transaksi pembelian, c*ustomer* akan melakukan swipe atau DIP di mesin EDC. Petugas *merchant* akan memilih menu *amount* dan memasukan nilai transaksi, nilai transaksi akan ditunjukan kepada *customer* dan jika cocok dengan jumlah transaksi yang dibeli, maka *customer* memasukan *pin*

dan menekan *enter*. Kemudian EDC akan mengirimkan atau meneruskan transaksi tersebut ke sistem bank untuk proses otorisasi transaksi.

NAC akan menangkap sinyal atau menampung transaksi yang dikirimkan oleh EDC di *merchant* Bank Permata. Sistem NAC tidak memiliki sistem keamanan sama sekali. Sehingga informasi yang diproses tidak mempunyai integritas dan nilai yang tinggi (Ken Shaurette 2006), sehingga bisa saja EDC tersebut telah dirusak dalam arti sudah dirubah sistemnya, sehingga seolah-olah EDC itu adalah milik Bank Permata.

Sedangkan Base24eps hanya berfungsi sebagai *switching* yang memisahkan jenis transaksi. Jenis transaksi yang telah dipisahkan yaitu visa card dan mastercard internasional, dan diterusakan ke *Ascend*. *Ascend* akan menerima data transaksi dan meneruskan data transaksi, dan bagian ini berfungsi sebagai manajemen sistem, yang akan memisahkan jenis transaksi. Jika kartu jenis Visa Card Internasional akan diteruskan ke Visa International, dan jika jenis kartu tersebut mastercard internasional akan diteruskan ke master card internasional. Selanjutnya Master dan Visa International akan meneruskan ke bank penerbit untuk mendapatkan jawaban (disetujui atau ditolak). Bank penerbit ini hanya melakukan pemeriksaan apakah masih memenuhi *floor limit* atau tidak. Sehingga kelemahan sistem pengamanan ini apabila pelaku meng-*upgrades* jenis kartu tetap akan memproses transaksi ini.

Selanjutnya, bank penerbit kartu akan memberikan respons berupa jawaban ke Visa atau Master International. Visa dan Master International akan meneruskan jawaban ke Bank Permata yang diterima oleh *ascend*. *Ascend* akan meneruskan jawaban bank penerbit ke Base24 dan diteruskan ke NAC, kemudian diteruskan EDC dan keluar struk pembayaran. Pada proses balik ini juga tidak ada pengamanan.

Sedangkan pada proses *settlement* oleh *merchant*, pemilik *merchant* pengamanan dilakukan pada mesin EDC dan NAC serta oleh bagian *froud control*. Pada mesin EDC pengamanan yang diberikan dengan menggunakan *Password* atau *key master* yang diberikan pada saat diproses oleh bagian *technical support*. Ketikan *password* itu cocok maka EDC akan meneruskan ke sistem NAC.

Sehingga apabila ada *hacker* atau pembajakan *password* EDC tetap akan memproses *settlement* tersebut. Sedangkan NAC hanya menampung semua jenis transaksi, dan akan meneruskan ke Base 24 sampai kepada bank penerbit dan dilakukan pembayaran. Antara NAC dan Base24eps seharusnya ada suatu sistem yang berfungsi untuk memverifikasi apakah *settlement* benar benar dilakukan oleh orang yang berhak atau tidak. Sementara itu pengawasan yang dilakukan oleh unit *froud control* begitu lemah, bagian ini hanya mengecek transaksi yang mencurigakan atau diluar kewajaran. Jiak pelaku *fraud banking* melakukan transaksi yang normal, misal EDC A tiap hari melakukan *settlement* Rp. 50.000.000,-, maka *froud control* tidak akan mengetahui apakah transaksi itu mencurigakan atau tidak, dan yang terpenting dalam pengamanan transaksi ini adalah memasang *sofware* yang berfungsi mengecek atau memeriksa bahwa yang melakukan *settlement* adalah orang yang berhak.

5.2 Analisis Faktor-faktor Yang Mempengaruhi Terjadinya *Fraud Banking* di Merchant Bank Permata.

Melihat analisis di atas tentang pada proses *acquiring* dan transaksi di *merchant* tidak memiliki pengamanan yang optimal maka hal itu menyebabkan terjadinya *fraud banking*. Untuk lebih jelasnya penyebab terjadinya *fraud banking* terdiri dari beberapa faktor berikut ini.

5.2.1 Fakor Proses Akuisisi *Merchant*

Manusia mempunyai peran strategis dalam mengerakan roda suatu perusahaan. Oleh karena itu MRO Bank Permata merupakan ujung tombak dalam hal pemasaran produk *merchant*. Maka dari itu kebijakan manajemen Bank Permata merekrut karyawan *Outsourching* untuk ditempatkan di MRO. Karyawan tersebut apabila mempunyai dedikasi yang tinggi selama bekerja maka kemungkinan akan diangkat menjadi karyawan tetap dan sebaliknya apabila selama kontrak tidak menunjukan dedikasi yang tinggi maka langsung dilakukan pemutusan kerja terhadap karyawan tersebut. Menurut Simanjuntak (2010) pertimbangan merekrut karyawan tersebut dengan alasan investasi dan tingkat upah. Hal ini senada dengan *Manager Froud Control* (wawancara, 12 April 2011) "karena kekurangan untuk memasarkan produk *merchant*, maka perlu merekrut

karyawan *outsourcing* dan apabila tidak bisa bekerja pihak bank tidak repot mengeluarkannya."

Pemasaran dilakukan oleh MRO baik melalui layanan telepon (*Call Center*) maupun kanvasing (mendatangi calon pemohon *merchant*). Tujuan Bank Permata mengembangkan layanan *merchant* adalah benefit bagi *customer* dan benefit bagi *merchant*. Benefit bagi *customer* adalah aman karena *customer* tidak perlu membawa uang *cash* untuk membayar tagihan atau melakukan transaksi, nyaman karena *customer* hanya perlu membawa kartu, tidak perlu menghitung dalam pemhayaran suatu transaksi, ada bukti pembayaran dari struk yang dikeluarkan oleh EDC. Sedangkan benefit bagi *merchant* adalah tidak ada resiko uang palsu, tidak perlu menghitung uang tunai yang diterima atau kembalian (bisa menghemat waktu), tagihan kepada bank penerbit bisa langsung diterima melalui rekening yang terdaftar.

Bagi pengusaha yang bergerak dibidang jasa dan perdagangan yang tertarik mengajukan permohonan *merchant* harus melengkapi persyaratan KTP, KITAS bagi warga asing, Nomor Pokok Wajib Pajak (NPWP), Surat Ijin Usaha Perdagangan (SIUP), Akte, dan perjanjian kersama antara pihak pemohon dengan bank penerbit, dalam hal ini Bank Permata. Persyaratan tersebut harus tetap mempunyai nilai yang tinggi, karena merupakan sumber daya organisasi yang penting bagi keberlangsungan usaha Bank Permata. Agar tetap mempunyai nilai yang tinggi, maka MRO harus menjaga integritas informasi tersebut.

Integritas yang dimaksud dalam toeri ICA yang dikemukakan Ken M. Shaurette (2006) adalah menjaga keakuratan dan kelengkapan informasi serta cara memproses informasi tersehut. Sehingga tidak jatuh kepada orang yang tidak berhak yang dapat mendatangkan kerugian bagi Bank Permata dan dijadikan celah oleh pelaku kejahatan. Hal ini juga dikuatkan oleh Suryadi (2010) sistem pengamanan informasi dipengaruhi oleh faktor manusia, proses dan teknologi. Berdasarkan hasil penelitian, faktor manusia menjadi faktor penyebab terjadinya *fraud banking*, MRO telah menyalahi prosedur yang ditetapkan Bank Permata sehingga tidak dapat menjaga integritas proses *acquring merchant*.

Berdasarkan hasil penelitian atas studi kasus *fraud banking* yang dilaporkan di Polda Metro Jaya, pemohon *merchant* Padma Collection, Hongkong

Fashion, kharisma Collection, dan Rizky Boutiqe ini mengajukan permohonan melalui Toko Pretty Mom. Sehingga integritas dalam hal ini adalah kelengkapan dan keakuratan bersifat semu, artinya kelengkapan data yang diberikan terbukti palsu dan dimanfaatkan oleh pelaku kejahatan untuk melakukan transaksi fiktif. Merujuk Surat Keputusan Kapolri No. Pol: Skep/507/VII/1998 modus operandi yang dilakukan pelaku kejahatan adalah pedagang mengajukan permohonan *merchant* di bank pengelola dengan data palsu (*fictitious merchant*).

Selain dari faktor manusia terjadinya *fraud banking* disebabkan oleh proses akusisi *merchant*. Memang sepintas proses akuisisi *merchant* Bank Permata terkesan berbelit-belit dan mempunyai beberapa layer pengamanan. Namun setelah kita cermati pengamanan yang dilakukan dalam proses akuisisi ini hanya dilakukan oleh unit APC. Namun sistem pengamanannya juga lemah, unit ini hanya memverifikasi data di BI, bagi customer yang sudah pernah berurusan dengan pihak bank, dan tidak dilakukan validitas baik melalui telepon maupun pengecekan secara fisik untuk memastikan pemohon *merchant* adalah pihak yang benar atau syah. Sehingga kesalahan yang terdahulu dari MRO tidak bisa teridentifikasi, karena data yang dimasukan sejak pertama adalah data yang salah, sehingga keluarannya atau *output* akan salah juga. Hal ini dimanfaatkan oleh pelaku kejahatan untuk memasukan data palsu (*fictitious merchant*).

Selanjutnya kesalahan atau kelalaian juga dilakukan berulang kali oleh bagian MRO. Ketika Unit *Technical Support* selesai menginput data, memasukan *key master* kepada EDC, dan mengadakan uji coba, diserahkan kepada MRO, kewajiban MRO bersama *vendor* melakukan instalasi atau pemasangan langsung terhadap pemohon *merchant*. Artinya MRO harus bertemu langsung dengan pemohon dan melakukan *training* cara menggunakan *merchant* dimulai dari proses transaksi hingga *settlement*. Merujuk pada teori CIA dari Ken M. Shaurette (2006) informasi sudah tidak memiliki integritas, kerahasiaan, dan ketersedian, karena jatuh kepada orang yang salah. Sehingga memungkinkan oknum pedagang merusak atau mengubah program alat otorisasi EDC milik pengelola yang dititipkan atau dipinjamkan kepada *merchant*, alat ini direkayasa (*clone*) agar dapat dilakukan otorisasi atau dioperasikan tanpa ada kartu kredit secara fisik.

Kemudian penyebab lain dari *fraud banking* adalah lemahnya kontrol dari *Unit Froud Banking* terhadap keberadaan EDC, padahal dari perjanjian kerjasama (PKS) (Bank Permata 2011), akan dilakukan pengecekan atau kontrol terhadap EDC di setiap *merchant*, apabila sudah tidak beroperasi maka akan ditarik oleh pihak Bank Permata. Namun faktanya berdasarkan hasil penelitian masih banyak EDC yang sudah berpindah tangan atau dipinjamkan. Akibat lemahnya kontrol dari unit ini menyebabkan adanya peluang bagi oknum pedagang atau pelaku kejahatan memodifikasi dan merubah sistem EDC, atau disebut dengan EDC emulator (*Clone*).

5.2.2 Faktor Proses Transaski Elektronik Pada *Merchant* Bank Permata.

Teknologi pengamanan sistem informasi yang dimiliki Bank Permata terdiri dari 5 sistem didalam satu rangkaian sistem (*Password* EDC, NAC, Base24 eps, ON2, *Ascend*) dan satu sistem lain yang terpisah dari alur transaksi yaitu sebuah komputer yang dilengkapi dengan *software* yang bisa mengidentifikasi transaksi mencurigakan. Merujuk teori SDLC yang dikemukakan Lim dan Bazavan (2006) sistem pengamanan informasi pada alur transaksi baik pembayaran maupun *settlement* sudah memalui tahap persyaratan, tahap analisasi, dan tahap *design*. Namun tahap selanjutnya yaitu tahap ujicoba pengamanan dan tahap penyebaran belum pernah dilakukan. Hal tersebut dikuatkan oleh hasil wawancara Manajer Froud Control (12 April 2011)

> memang sejak awal sudah melalui tahap persyaratan, tahap analisa, dan tahap *design*, tapi untuk ujicoba dan penyebaran yang dimaksud belum pernah dilakukan. Dan saya menganggap bahwa dengan sistem password yang ada di EDC dan *Software* yang ada pada unit saya, yaitu untuk melakukan pengecekan terhadap transaki yang mencurigakan sudah cukup untuk untuk mengamankan transaksi.

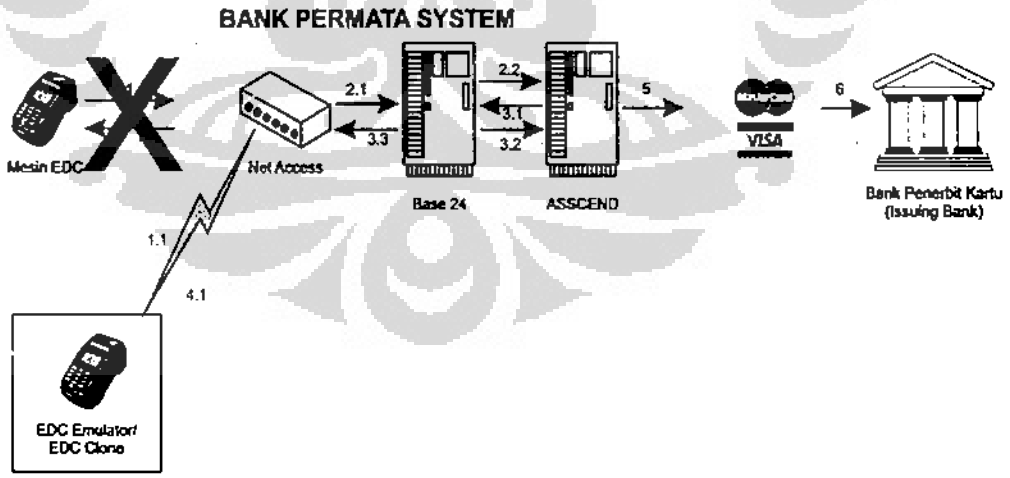
Namun faktanya beberapa sistem pengamanan dalam transaksi elektronik pada EDC di merchant Bank Permata belum mampu menjamin keamanan. Karena Fungsi NAC hanya menampung seluruh transaksi elektronik menggunakan *merchant* Bank Permata. Sedangkan Base24 eps dan ON2 hanya berfungsi sebagai *switching* atau memisahkan jenis transaksi apakah termasuk debit, kredit atau transaksi lainnya. Selanjutnya fungsi dari *ascend* hanya sebagai manajemen sistem, alat ini hanya membagi dan meneruskan apakah transaksi menggunakan

visacard atau master card internasional. Sementara *password* EDC sendiri keamanannya sudah diluar jangkauan bank, artinya pengamanannya tergantung dari pemilik toko itu sendiri. Dalam pada itu *software* yang dipunyai oleh Unit *froud control* hanya melakukan pengecekan atau pemeriksaan terhadap transaksi yang mencurigakan. Sehingga apabila transaksi itu masih diambang wajar, unit ini tidak bisa membedakan apakah ini merupakan *fraud banking* atau bukan.

Penyebab terjadinya *fraud banking* dalam transaksi elekrtonik ini disebabkan faktor sebelumnya yaitu proses akuisisi *merchant*. Sehingga menghasilkan data yang tidak akurat, proses akuisisi *merchant* yang tidak mempuyai sistem pengamanan yang baik, dan penyerahan EDC tidak langsung kepada pemohon serta banyaknya kehilangan mesin EDC atau sudah dipindah tangankan kepada orang yang tidak berhak. Sehingga memungkinkan pelaku kejahatan dapat merusak dan mengubah sistem EDC dengan leluasa. Pelaku telah memasukan data atau *sales draft* palsu dengan mengunakan komputer, dan melakukan *settlement* dan Bank Permata melakukan pembayaran atas *settlement* tersebut. Penyebab *fraud banking* itu apabila digambarkan sebagai berikut:

Gambar 25

Offline Fraud Settlement Transaction



Sumber: Hasil wawancara dan pengembangan penulis 2011

Dari gambar Offline Fraud Settlement tersebut dapat dijelaskan berikut ini.

1. EDC yang sebenarnya tidak pernah mengirim *settlement* (sebagian EDC hilang dan sebagian EDC masih di *merchant*)
   1.1. *Settlement* datang dari EDC *emulator*/EDC *clone* dari TKP yang dilakukan oleh *Fraudster.*
2. *Settlement* dari EDC *clone*/EDC *emulator* yang dilakukan oleh *Fraudster* selanjutnya diterima oleh *net access*
   2.1. Net Access mengirim data settlement ke Base24
   2.2. Base24 melakukan pengecekan apakah data identitas *merchant* atau *merchant identity* (M-ID) dan nomer EDC ,*Terminal Identity* (T-ID) adalah M-ID dan T-ID yang sah dan selanjutnya mengirim data *settlement* ke *Ascend.*
3. *Ascend* menerima data *settlement* dari Base24
   3.1. *Ascend* mengirim jawaban *settlement* sukses ke Base24,
   3.2. Saat bersamaan Base24 membuat *report settlement* dan dikirim ke *ascend* dan *ascend* membuat *report* pembayaran *merchant.*
   3.3. Saat yang sama juga Base24 meneruskan jawaban sukses dari *ascend* ke *net access.*
4. *Net access* tidak pernah mengirim jawaban *settlement* sukses ke EDC
   4.1. Jawaban *settlement* sukses terkirim ke EDC *emulator/clone.*
5. *Ascend* mengirim data *settlement* ke Visa International
6. Visa International meneruskan ke bank penerbit kartu dan melakukan pengkreditan ke rekening Bank Permata di Visa International dan men- debet rekening bank penebit kartu di Visa International

Sedangkan ketika pembayaran ke *merchant* atas *offline fraud settlement* dilakukan:

3. *Ascend* menerima data *settlement* dari Base24
   3.1. *Ascend* mengirim jawaban *settlement* sukses ke Base24 dan Base24 membuat *report settlement.*
   3.2. *Report settlement* di kirim ke *ascend* dan *ascend* membuat *report* pembayaran *merchant.*

Berdasarkan *report* pembayaran *merchant*, *unit payment* melakukan pembayaran ke rekening *merchant* sehari sesudah proses *settlement* dilakukan oleh pelaku *atau fraudster*.

Fraud banking tersebut terjadi karena pada proses transaksi pengamanan hanya berada pada mesin EDC. Sedangkan diantara NAC sampai ke *ascend* tidak ada pengamanan sama sekali. Seharusnya di antara terminal atau sistem NAC dan EDC ada sistem pengamanan. Menurut Lan dan Bazavan (2006) dalam tahap pengembangan sistem pengamanan setelah prosedur *coding* atau *password* harus ada sistem enkripsi dan memuat nomor secara acak, yaitu sebagai berikut:

1. Kriteria cukup acak untuk menghidari pola dan kedekatan.
2. Harus memiliki periode yang besar.
3. Tidak membuat *strings* yang di sukai, seperti 010101.
4. Merupakan algoritma yang sederhana dan performa yang baik.
5. Tidak akan memberitahu beberapa *output* yang bisa memprediksi *output* masa lalu dan masa akan datang.
6. Memiliki persyaratan internal yang cukup bsar dan tidak bisa di prediksi untuk mencegah hasil pencarian.

5.3 Analisis Upaya Untuk Memperbaiki Manjemen Pengamanan Sistem Informasi *Merchant* Bank Permata

Upaya yang harus dilakukan berdasarkan hasil penelitian adalah memperbaiki manajemen pengamanan sistem informasi Bank Permata. Upaya tersebut terdiri dari memperbaiki sistem akusisi merchant dan proses transaksi merchant Bank Permata. Untuk lebih jelasnya penulis akan menguraikan berikut ini.

5.3.1 Upaya Memperbaiki Manajemen Pengamanan Sistem Informasi Akusisi *Merchant* Bank Permata

Merujuk teori Cobit yang dikemukakan Brand dan Boonen (2007), bahwa Cobit dapat mendukung pengendalian dan pengamanan TI. Cobit ini juga terkait dengan sumberdaya TI, yang terdiri dari manusia, aplikasi, informasi dan infrastuktur. Sumberdaya manusia perlu direncanakan, diorganisasikan dan disediakan, didukung, diawasi dan dievaluasi dalam TI ini. Apabila dikaitkan

dengan hasil penelitian perlu perbaikan sistem akuisisi *merchant* dari faktor manusia maupun prosesnya.

Caranya merestrukturasi karyawan MRO dari karyawan yang statusnya *out sourching* menjadi pegawai tetap. Karena beban yang diterima oleh MRO *outsourcing*, target untuk mendapatkan pemohon *merchant* berat sehingga mendorong untuk melakukan penyimpangan, dan loyalitas pegawai *outsorcing* terhadap Bank Permata lemah jika dibandingkan dengan karyawan tetap. Selain itu perlu dibentuk badan pengawas atau auditor terhadap hasil kerja dari MRO

Gambar 26

New Acquiring Merchant

Keterangan:

A= unit untuk melakukan verifikasi terhadap kelengakapan data pemohon

B= unit untuk melakukan verifikasi terhadap kelayakan pemohon

C= unit untuk melakukan analisis resiko pemohon *merchant* dnegan melakukan pengecekan secara fisik

Sedangkan terhadap prosesnya agar ditambah bagian atau unit untuk memeriksa kelengkapan permohonan *merchant* dan unit untuk mengecek kelayakan pemohonan *merchant*. Kemudian setelah proses dilakukan *Application Proccesing Control (*APC) ditambah dengan bagian atau unit yang menganalisa atas resiko terhadap setiap calon merchant dengan melakukan secara fisik atau mendatangi lansung pemohon merchant dan tempat-tempat yang berkaitan dengan persyaratan yang dilengkapi, memberikan hasil analisa resiko, dan memberikan masukan atau perkiraan kelayakan toko.

Hal itu sesuai dengan teori Cobit agar memenuhi kriteria kualitas, terhadap kerahasian, integritas, dan ketersediaan informasi atau data pemohon pada proses akuisisi *merchant*. Sehingga data pemohon benar-benar memenuhi validiatas dan reabilitas, dan mempersempit ruang gerak para pelaku *fraud banking*, karena dengan sistem kriteria ini, kebocoran-kebocoran data atau informasi dapat segera diketahui dan dievaluasi. Selain itu manajemen sistem pengamanan informasi memenuhi kriteria opersaional yang efektif dan efisien.

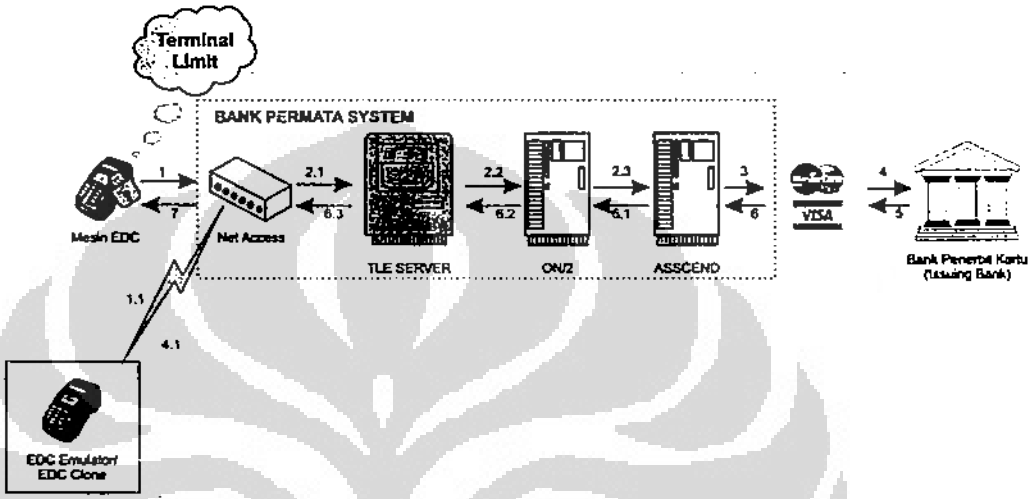
5.3.2 Upaya Memperbaiki Manajemen Pengamanan Sistem Informasi Proses Transaksi Elektornik Merchant Bank Permata

Merujuk teori SDLC, pada sistem informasi internal bank seharusnya antara sistem *NAC* sampai kepada *Ascend* mempunyai sistem pengamanan. Pengamanan yang dimaksud adalah sistem atau *software* enkripsi atau *terminal line encryptions* (TLE). Sementara yang memungkinkan adalah diantara NAC dan Base24 eps, karena NAC berfungsi untuk menampung semua jenis transaksi, dan Base24 eps berfungsi sebagai pemisah. Jadi semu Transaksi yang dikirim kan ke NAC terlebih dahulu diterima TLE untuk proses otorisasi ke mesin EDC kembali, sehingga dapat diketahui yang melakukan Transaksi adalah bukan orang yang berhak, dan apabila fraudster bisa menklonig pasword dan M-Id serta T-Id, masih ada satu tahap pegnaman yang harus dipecahkan yaitu enkripsi dengan nomor acak. Hal tersebut dilakukan baik pada dual alur baik *online* maupun *offline* atau

pembayaran maupun *settelment*. Apabila digambarkan maka sistem pengamanan yang harus dilakukan adalah sebagai berikut:

Gambar 27

New Online dan offline Transaction



Ketika transaksi atau otorisasi dilakukan:

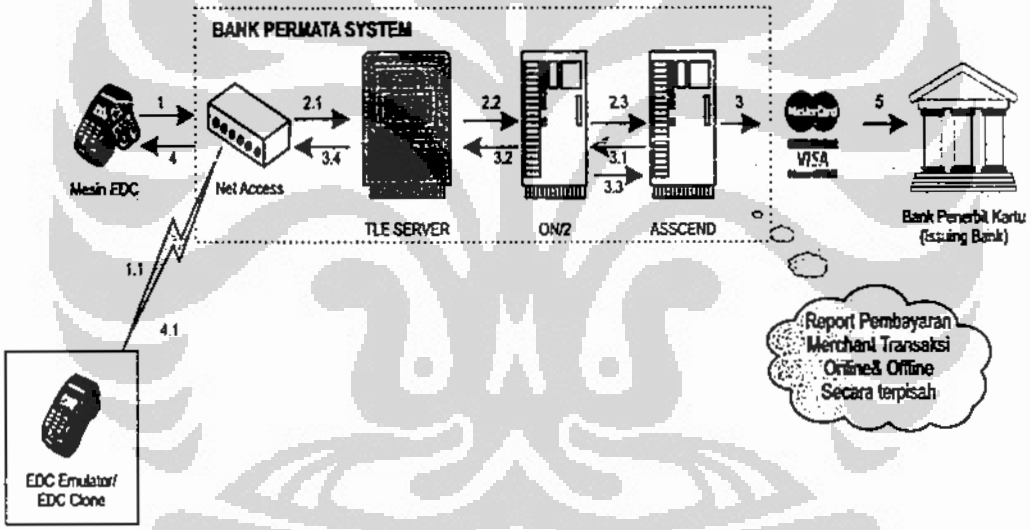
1. Setiap EDC memiliki *limit* maksimum transaksi dan memiliki "*Key*". Saat proses *authorisasi* EDC akan mengirim data transaksi ke Net Acces
2. Net Acces menerima data transaksi dari mesin EDC.
   2.1. NAC akan menerukan data transaksi ke TLE Server untuk melakukan validasi "*Key*" untuk memastikan data transaksi berasal dari EDC Bank Permata.
   2.2. Jika data transaksi berasal dari EDC Bank Permata maka data transaksi akan di teruskan ke Base24, Jika data transaksi berasal dari EDC selain EDC Bank Permata (EDC Emulator atau EDC Clone) seperti proses 1.1 maka data transaksi akan di tolak oleh TLE Server.
   2.3. Base24 menerima data transaksi yang valid and diteruskan ke Asscend
3. Ascend akan menerima data transaksi dan meneruskan data transaksi ke Visa Inetrnational
4. Visa International akan meneruskan ke Bank Penerbit untuk mendapatkan jawaban (disetujui/ditolak)

5. Bank Penerbit kartu akan memberikan respons berupa jawaban ke Visa International
6. Visa International akan meneruskan jawaban ke Bank Permata yang diterima oleh Ascend
   6.1. Ascend akan meneruskan jawaban Bank Penerbit ke Base24
   6.2. Base24 akan menerukan jawaban Bank Penerbit ke TLE Server
   6.3. Server TLE akan menerukan jawaban Bank Penerbit ke Net Access
7. Net Access akan menerukan jawaban ke mesin EDC di Merchant, untuk transaksi yang disetujui maka mesin EDC akan mencetak Sales Draft

Sedangkan pada proses *settlement*:

Gambar 28

New Settlement Transaction



Ketika transaksi di settlement oleh Merchant:

1. Mesin EDC mengirim data *settlement* atas transaksi yang disetujui melalui NAC (Net Access).
2. Net Acces akan menerima data settlement dari EDC
   2.1. Data *settlement* diteruskan oleh Net Access ke TLE Server dan TLE Server untuk melakukan validasi "*Key*" untuk memastikan data transaksi berasal dari EDC Bank Permata.
   2.2. Jika transaksi berasal dari EDC Bank Permata maka data *settlement* akan diteruskan ke Base24, jika data *settlement* berasal dari EDC

selain EDC Bank Permata (EDC *emulator* atau EDC *clone*) seperti proses 1.1 maka data transaksi akan di tolak oleh TLE Server.

2.3. Base24 menerima data transaksi yang valid and diteruskan ke Ascend

3. Ascend akan menerima data settlement dan meneruskan data transaksi ke Visa Inetrnational.

3.1. Ascend akan mengirim jawaban data *settlement* sukses Base24

3.2. Base24 merima jawaban sukses dari Ascend dan meneruskan ke TLE Server dan membuat *report settlement*.

3.3. *Report settlement* di kerim ke Ascend dan Ascend kan membuat laporan pembayaran *merchant* yang memisahkan transaksi *online* dan transaksi *offline*.

3.4. TLE *server* menerima jawaban settlement sukses dari Base24

4. NAC akan menerukan jawaban *settlement* sukses ke Mesin EDC, lalu mesin EDC mencetak *sales settlement*.
5. Visa International akan meneruskan data *settlement* ke Bank Penerbit dan saat bersamaan Visa International melakukan pendebitan rekening Bank Penerbit di Visa International dan mengkredit rekening Bank Permata di Visa international.

Ketika Pembayaran ke Merchant:

1. Unit *payment* mengambil menerima *report* pembayaran *merchant* dari Ascend
2. Pembayaran di pisahkan berdasarkan cara transaksi yaitu *online* dan *offline* setelah melalui proses verifikasi.
3. Transaksi atau *settlement online* bisa langsung di bayarkan ke *merchant*.
4. Transaksi/*settlement offline* harus di *review* oleh *Fraud Control Unit*

BAB 6
PENUTUP

Bab ini, adalah merupakan rangkaian terakhir dari hasil penelitian tentang manajemen pengamanan sistem informasi di *merchant* Bank Permata. Mendasari hasil penelitian kemudian dianalasis dengan menggunakan teori CIA, SDLC, dan Cobit, maka penulis dapat menyimpulkan dan merekomendasikan hasil penelitian, berikut ini.

6.1 Kesimpulan

Manajemen pengamanan sistem informasi *merchant* Bank Permata tidak memiliki pengamanan yang optimal, baik dalam proses akuisisi maupun proses transaksi elektronik pada *merchant* Bank Permata tersebut. Pada proses akuisisi *merchant* informasi dan data pemohon merchant sudah tidak memiliki integritas, kerahasian dan ketersedian. Semua data dan informasi dimulai dari penerimaan permohonan *merchant*, kemudian diproses sampai dikeluarkannya EDC pada *merchant* Bank Permata tidak terintegrasi antara unit satu dengan yang lainnya dan tidak memiliki pencegahan terhadap risiko. Selain itu unit *application proccesing control* tidak melakukan pengecekan atau indetifikasi baik melaui telepon maupun secara fisik, melainkan hanya mengidentifikasi kepada BI, itupun orang-orang yang pernah bermasalah, sedangkan orang yang sama sekali tidak pernah berurusan dengan dunia perbankan, akan dinyatakan bersih oleh pihak BI.

Sedangkan sistem pengamanan pada transaksi elektornik, sistem pengamanan yang ada hanya diberikan pada mesin EDC dengan menggunakan pasword. Sedangkan pada sistem lain hanya berfungsi sebagai penampung transaksi (NAC), *switching* (Base24eps dan ON2), dan manajemen sistem (Asccend). selain itu juga software yang digunakan fungsi *froud control* untuk melacak transaksi yang mencurigakan bukan melacak apakah yang melakukan transaksi itu orang yang berhak atau tidak. Sehingga fungsi *froud control* tidak menjamin sistem keamanan transaski elektotonik pada *merchant* Bank Permata.

Sementara itu faktor yang mempengaruhi terjadinya *fraud banking* pada *merchant* Bank Permata disebabkan oleh faktor manusia, proses, dan

teknologinya. Pertama, Faktor manusia diakibatkan kelalaian MRO dalam melakukan proses akuisisi *merchant*, sejak awal sumber data atau informasi yang diterima sudah menyalahi prosedur yang ditetapkan oleh Bank Permata, sehingga ketika di proses *output*-nya akan salah. Data yang tidak diperoleh tidak memenuhi aspek integritas, walaupun lengkap namun tidak akurat. Sehingga pelaku kejahatan dapat memalsukan data pada proses ini (*fictitious merchant*). sehingga dapat dimanfaakan oleh *fraudster* untuk merusak dan merekayasa sistem EDC.

Kedua, faktor proses. Pada proses akusisi *merchant* juga unit *application proscesing control* hanya melakukan pengecekan atau verifikasi kepada pihak BI terkait apakah pemohon *merchant* ini bermasalah atau masuk dalam daftar hitam, apabila seseorang yang tidak pernah berurusan dengan pihak bank maka hasilnya akan *clean* atau bersih. Seharusnya verifikasi dilakukan terhadap persyaratan yang diajukan pemohon merchant apakah layak atau tidak. Kemudian pada proses terakhir yang dilakukan oleh MRO harus menyerahkan EDC langsung kepada pemohon dan melakukan *training*, akan tetapi hal itupun tidak dilakukan dan diserahkan kepada orang lain yang bukan haknya.

Ketiga, faktor teknologi. Faktor ini terkait dengan alur transaksi *payment* dan *settlement*. Pada alur transaksi ini Bank Permata tidak mempunyai layer pengamanan berlapis, sistem pengamanan hanya pada mesin EDC. Sehingga ketika mesin EDC dapat dirusak atau dirubah sistemnya, pelaku dapat melakukan transaski (*settlement*) dan sistem yang lainnya akan menyetujuinya, akibatnya terjadi *fraud banking* yang merugikan Bank Permata 70 milyar rupiah.

Oleh karena itu, upaya yang dilakukan untuk memperbaiki manajcmen pengamanan sistem informasi *merchant* Bank Permata adalah memperbaiki sistem akuisisi merchant dan pengamanan sistem internal bank pada transaksi elektronik *merchant* Bank Permata. Caranya merekstukturisasi dan mengembangkan sumberdaya teknologi informasi, dimulai dari manusia, aplikasi, insfratruktur, dan teknologinya, sehingga memenuhi kriteria kulitas pengamanan yang efektif dan efisien serta menjamin kerahasiaan, integritas dan ketersediaan.

6.2 Rekomendasi

Dari beberapa kesimpulan yang telah penulis sampaikan di atas. Maka rekomendasi yang dapat disampaikan sebagai berikut:

Sebagai masukan kepada manajer Bank Permata, harus ada komitmen untuk memperbaiki manajemen pengamanan sistem informasi *merchant* Bank Permata. Tidak sekedar berorientasi terhadap *profitable* saja, melainkan keamanan dan kenyamanan baik nasabah maupun Bank permata sendiri. seperti mengalokasikan dana operasional untuk memperbanyak karyawan tetap, membentuk auditor, untuk mengawasi dan mengaudit kinerja karyawan dilapangan khususnya unit MRO, Froud Control, dan APC.

Sementara itu rekomendasi terhadap teknologi, solusinya pengamanan sistem informasi menggunakan *terminal encryptions line* agar dilakukan uji validitas. Apakah mampu mengamankan seluruh transaksi elektronik atau tidak, sehingga hasil penelitian ini dapat bermanfaat bagi Bank Permata. Kemudian dievaluasi kembali sehingga akan menjadi masukan untuk memperbaiki manajemen pengamanan sistem informasi merchant Bank Permata

Untuk yang terakhir penulis sebagai peneliti merekomendasikan penelitian selanjutnya difokuskan kepada manajemen pengamanan sistem informasi terhadap proses transaksi yang menggunakan terminal enkripsi. Hal ini untuk membuktikan apakah terminal tersebut dapat mencegah kejahatan dan kerugian bagi bank. Dengan catatan, apabila rekomendasi penulis diterima dan dioperasionalkan oleh Bank Permata.

DAFTAR ACUAN

Bran, K. And Boonen, H. (2007). IT *govenance based on Cobit 4.1*. Netherlands: IT Govenance Institute

Creswell, J. W. (2002). *Research design qualitative & quantitative*. (Edisi revesi). (Angkatan III & IV KIK UI dan N. Khabibah, Penerjemah). Jakarta: KIKpress.

Djamin, A. (2007). *Tantangan dan kendala menuju polri yang profesional dan mandiri*. Jakarta: PTIK Pres

DitKrimsus Polda Mero Jaya. (2010). Berkas Perkara: Fraud banking Bank Permata. Jakarta : Polda Metrojaya.

Golose, P.R.(2008). *Seputar kejahatan hacking teori dan studi kasus*. Jakarta: YPKIK

Green, G. dan Fischer, R. J. (1998). *Introduction security* (Edisi ke-6). USA: Butterworth Heinemann.)

Haidar, A. (2010). *Makalah: Sistem pengamanan Swakarsa*. Jakarta: tidak terbit.

Hacker, A. (2000). Information sustems security ia an oximorom. Dalam Donald L. Pinkin (Ed*). Information security protecting the global enterprise*. New Jersey: Prentice Hall PTR.

Ian, L. and Bazavan,I. (2006). System development security methodology. In tipton, Harold F and Krause, Micki (ed). *Information security manajemen handbook*. (P.309-324)

Kadir, A. (2003). *Pengenalan sistem informasi*. Yogyakarta: Penerbit Andi Yogyakarta.

Ken M. Shaurette. (2006). Technology convergence and security: a simplified risk management model. In tipton, Harold F and Krause, Micki (ed). *Information security manajemen handbook*. (P. 233-240).

Mcbride. (2006). Enterprise security management program. In tipton, Harold F and Krause, Micki (ed). *Information security manajemen handbook*. (P.223-231).

Mcleoad. R. Jr. (1998). *Sistem informasi manajemen*.(Hendra Teguh, alih bahasa). Jakarta: PT Prenhallindo.

Muhammad, F dan Djaali. (2005). *Metodologi penelitian sosial* (Revisi). Jakarta: PTIK Pres dan Restu Agung.

Murdick, R.G., Ross, J.E., dan Clagget. J.R (1984). Sistem informasi untuk manajemen modern. (J. Djamil, Aliha bahasa). Jakarta: Penerbit Erlangga.

Bank Permata. (2011). *Profile company*. Jakarta: Bank Permata

Pike, M. (2006). Organized crime and malware. In tipton, Harold F and Krause, Micki (ed). *Information security manajemen handbook.* (P.339-350)

Price, S. M. (2006). Developing and controlingsecurity test and evalluation. In tipton, Harold F and Krause, Micki (ed). *Information security manajemen handbook.* (P.213-240)

Santoso, P.B (2010). *Tesis*: penerapan manajemen kemanan infprmasi pada traffic management center direktorat lalu lintas polda metro jadas dengan pengendalian iso 27001:2005. Jakarta: Universitas Indonesia

Simanjuntak, P.J (2010). Diktat: Kepemimpinan dan motivasi. Jakarta: tidak terbit

Snare, J. And Kuper, E. (2005). Text for ISO/IEC final DIS 27001 information tecnology—sekurity techniques. *Information security management system—requirements*. Germany: Din Deutshc Institute for Normung

Sipior, Janice C ett all.(2003). *Information Security Management Handbook : Information Law*. Fifth editon. Editor Harold F. Tipton dan Micki Krause. Diunduh dari www.auerbach-publications.com

Sugiyono. (2008). *Metode penelitian kuantitatif kualitatif dan r&d.* (Edisi ke 5). Bandung: Alfabeta.

Suparlan, P. (1997). *Metode penelitian kualitatif*, Jakarta: Program Kajian Wilayah Amerika Program Pascasarjana Universitas Indonesia.

_____. (2004). Polisi dan fungsinya dalam masyarakat. Dalam P. Suparlan (Ed). *Bunga rampai ilmu kepolisian Indonesia* (hlm 67-71). Jakarta:Yayasan Pengembangan Kajian Ilmu Kepolisian

Suryadi (2010). *Penentuan nilai parimeter indikator analisa resiko*. Jakarta: tidak terbit.

Suyanto, M. (2005). *Teknlogi informasi untuk bisnis*. Yogyakarta: C.V AND OFFSET.

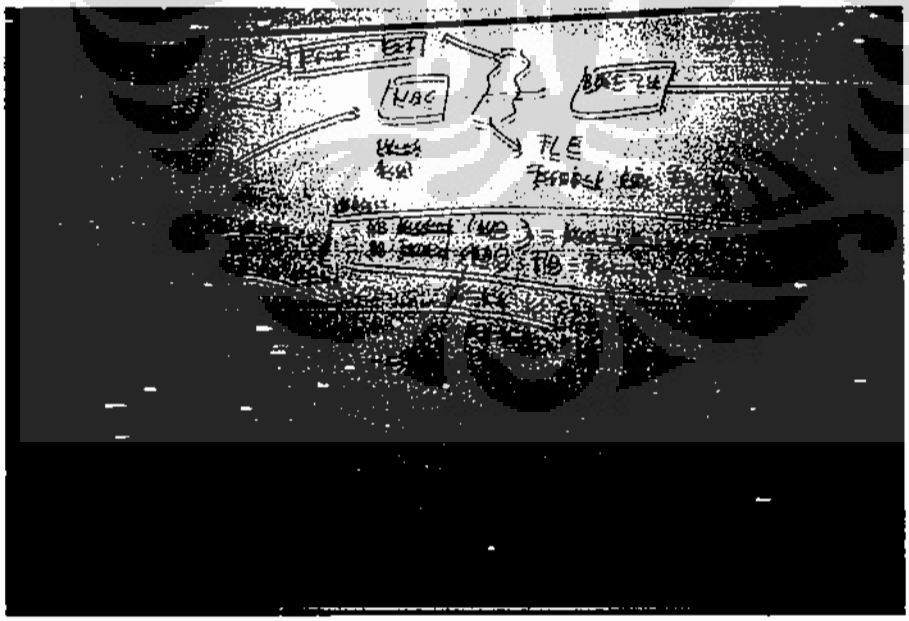
Terry, G.R. (1986). *Prinsiples of management*. (Edisi ke-6). (Winardi, Alih bahasa). Bandung: Alumni/1986/Bandung.

Winarsih, A. S., dan Ratmino. (2008). *Manajemen pelayanan: pengembangan model konseptual, penerapan citizen charter dan standar pelayanan minimal*. Yogyakarta: Pustaka Pelajar

FOTO 1

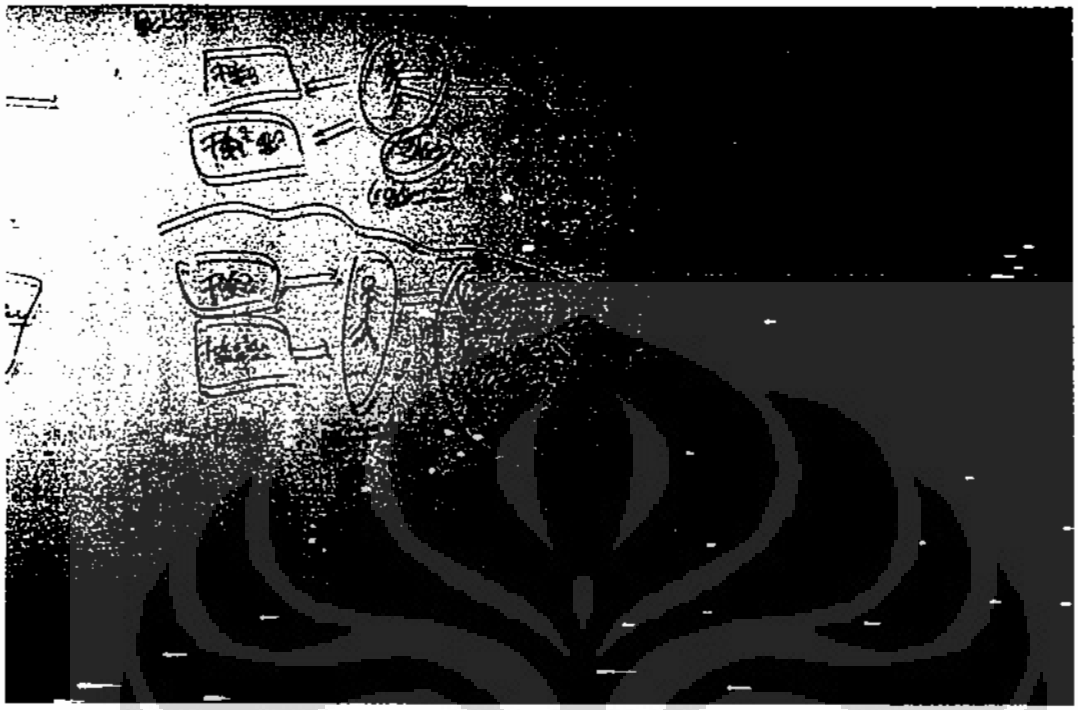
Wawancara dengan Manajer Froud Control PermataBank 12 April 2011

FOTO 1



Paparan Manajemen Control tentang sistem keamanan informasi merchant, 12 April 2011.

FOTO 3



Wawancara dan paparan dengan Manajer Bussiness Unit

PermataBank
Menjadikan hidup lebih bernilai

MERCHANT DATA FORM
(MDF)

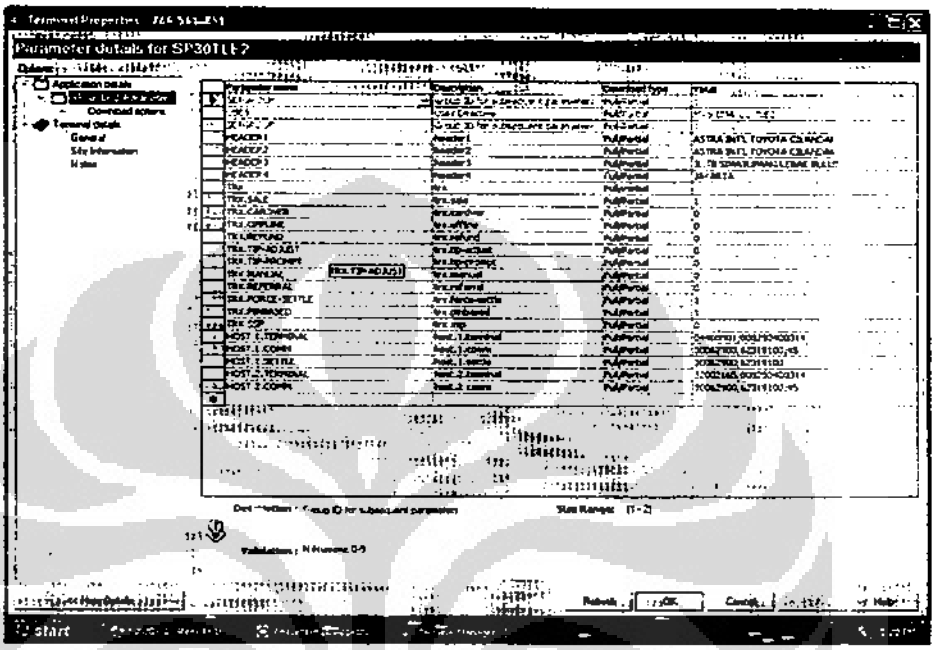
APLIKASI ☐ Baru ☐ Penambahan Outlet ☐ Penambahan EDC	☐ Perubahan Data (ganti data dengan data baru) ☐ Perubahan Merchant Utama	**FASILITAS** ☐ EMA ☐ .....
MID Merchant Utama :		☐ PT ☐ BPR ☐ CV ☐ Koperasi ☐ FA / PD
Nama Merchant :		
Alamat Merchant (Outlet) :		Jenis Industri :
Kota :	Kode pos :	Kode MCC :
Orang yang dapat dihubungi :	Telepon : Hp : Fax :	Lingkungan Merchant : ☐ Kawasan Bisnis / Perkantoran ☐ Kawasan Industri ☐ Perumahan ☐ Pusat Perbelanjaan ☐ Lainnya
Nama Bank :	Nama Cabang :	
Rekening ☐ Rekening Penampungan Merchant No Rekening : Nama Rekening :	Rekening Lain di Bank Permata No Rekening : Nama Rekening : No Rekening : Nama Rekening :	Kondisi Tempat Usaha Merchant ☐ Baik ☐ Renovasi ☐ Kurang Baik / Buruk
Nama Perusahaan :		Status : ☐ Milik Sendiri ☐ Sewa
Alamat Perusahaan :		Ukuran Bisnis : ☐ Kecil (Omzet Kurang dari Rp 100 Juta) ☐ Sedang (Rp 100 juta < Omzet < Rp 500 juta) ☐ Besar (Rp 500 juta - Rp 1 Milyar) ☐ Sangat Besar (Omzet lebih dari Rp 1 Milyar)
Kota :	Kode Pos :	
Telepon : Hp :	Fax : Alamat Email :	Merchant Discount Rate : MDR Maestro ..... % MDR Visa ..... % MDR Master card ..... %
Nama (Pemilik Merchant) :	Tanggal lahir (dd/mm/yy) :	
Alamat rumah saat ini (Pemilik Merchant) :		Dokumen yang Diperlukan : ☐ No. KTP : _____ ☐ No. KITAS : _____ ☐ No. NPWP : _____ ☐ No. SIUP : _____ ☐ No. AKTE : _____ ☐ No. PKS : _____
Kota :	Kode Pos :	
Telepon yang dapat dihubungi (Pemilik Merchant) 1. Rumah 2. Handphone	Fax : Alamat Email :	

BARU		PENAMBAHAN EDC / OUTLET		DANA JAMINAN EDC
EDC YANG DIPERLUKAN	BIAYA SEWA	EDC YANG DIPERLUKAN	BIAYA SEWA	
☐ Fixed Line ..... Unit	Rp. 100.000 / unit *	☐ Fixed Line ..... Unit	Rp. 100.000 / unit *	Rp .....
☐ Wireless ..... Unit	Rp. 175.000 / unit *	☐ Wireless ..... Unit	Rp. 175.000 / unit *	(.....)
*) Syarat & Ketentuan berlaku		*) Syarat & Ketentuan berlaku		Sebagai Jaminan Atas ..... Unit EDC Bank Permata

Merchant dengan ini memberi kuasa kepada Bank untuk melakukan pendebetan biaya sewa EDC & pembukaan dana pada rekening merchant sebesar nilai yang tersebut pada form ini.

KETERANGAN :

Diajukan oleh	Direkomendasi oleh	Disetujui oleh	Disetujui oleh	Disetujui oleh	Disetujui oleh
				Materai Rp 6.000	
Merchant Manager / PFC	Region Head	Head, EMA Business	Head, e-Channel	Merchant	Loan Approval
Tanggal Kunjungan	Nama :	Nama :	Nama :	Nama :	Nama :
Nama :					



```
   TERMINAL CONFIG
 DATE:051011  153738
 M/No: 06160
 S/No: 766-561-851
 P/No: M26160303AP4
 REV : U
 OS  : 0A0006A3
 APPL:
 PMT EMV Ver 5.0

 HOST: IDR
 TID : 04460001
 MID : 008250400314

 HOST: EMA HOST
 TID : 32002165
 MID : 008250400314
```

Lampiran 6

Job Descriptions

Directorate : RETAIL BANKING Business Unit/Functional Unit : EMA Business	Title : EMA Relationship Region	Date : 01.10.10

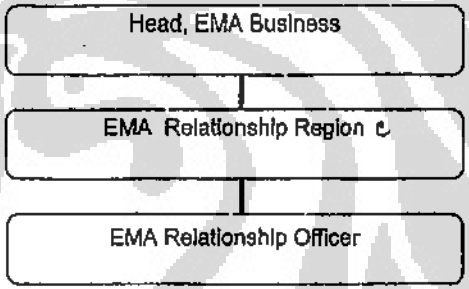
Job Purpose (Why the job exist, what output is expected and how to achieve it)

Job purpose :To manage EMA Business in Regional Area

Output expected : To ensure merchant closing project has been implemented properly

How to achieve : project management, managing administration, complain management & coordination, operation monitoring management

Reporting Relationships (draw an organization chart which cover your position and 1 layer above and under you position)



Report Directly to : Head EMA Business
Report Indirectly to : Head of e-Channel
Reporting : EMA Relationship Officer

Committee Membership (Job Related)

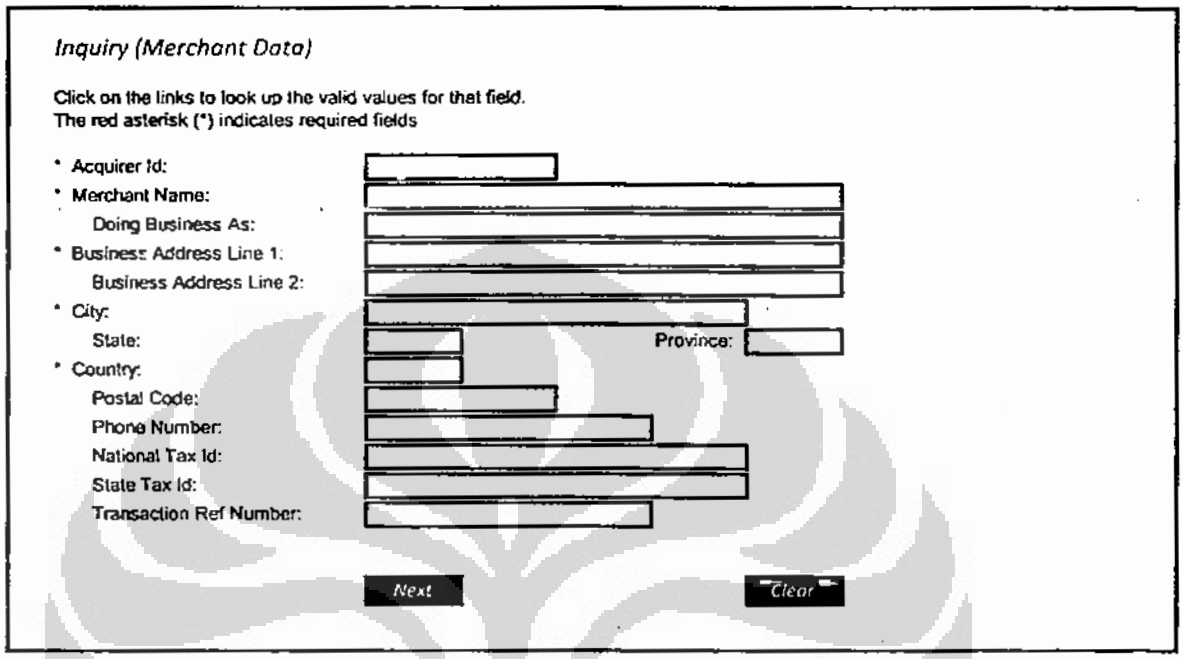
Dimensions

Geographical Span of Influence : X Bank Wide-Regional ..C..... ☐ Own Function ☐ Own Unit ☐ Self
Financial Targets : ☐ Sales _____ ☐ Trading Profit _____ ☐ Expense _____ X None
Approval Authority : O Expense_____ ☐ Credit _____ ☐ Others _____
Product Lines Managed (*) : EDC Mini ATM Debit Card
Customer Segments Managed (*) : Merchant / Customers
Notes : (*) Optional, and can be changed to other dimensions which is more related to the position

Lampiran 7

Key Result Area	Key Accountabilities	Impact			External Relations (Internal&External PB)	Key Performance Indicator (KRI)
		Primary	Shared	Contributory		
Project Management	1. Merchant communication - verbally - formal letter 2. Identify merchant existence	√			Internal - e-Channel - LAP Merchant - Payment Unit - EDCM - FCU - Branches - SME / WB - General Affair - Finance Accounting - Human Resource External - Merchant - Vendor	1. Project management 2. Managing Administration 3. Complain Management & Coordination 4. Operation monitoring management
Managing Administration	1. Letter distribution 2. Process report and status	√				
Complain Management & Coordination between related units	1. Complain management & coordination between related units	√				
Operation monitoring management	1. System closure 2. EDC retrieval 3. EDC rental 4. Hold release	√				

Lampiran 8

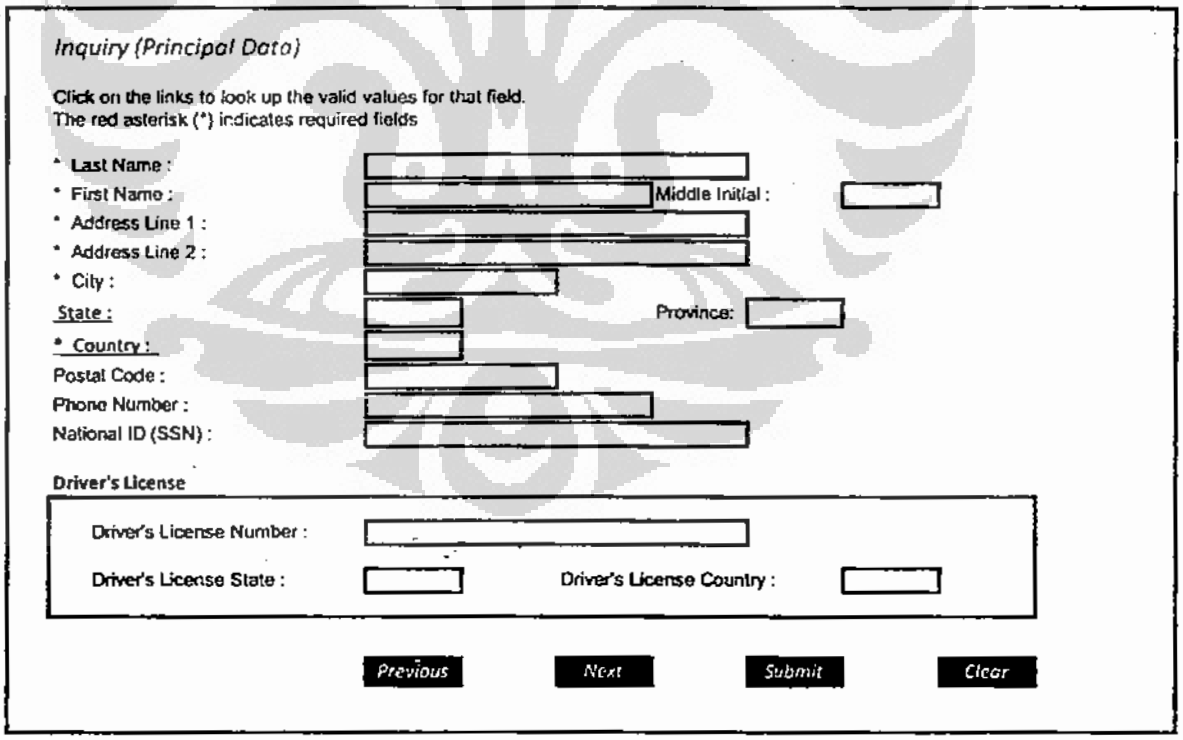


Inquiry (Merchant Data)

Click on the links to look up the valid values for that field.
The red asterisk (*) indicates required fields

* Acquirer Id:
* Merchant Name:
Doing Business As:
* Business Address Line 1:
Business Address Line 2:
* City:
State: Province:
* Country:
Postal Code:
Phone Number:
National Tax Id:
State Tax Id:
Transaction Ref Number:

Next Clear



Inquiry (Principal Data)

Click on the links to look up the valid values for that field.
The red asterisk (*) indicates required fields

* Last Name :
* First Name : Middle Initial :
* Address Line 1 :
* Address Line 2 :
* City :
State : Province:
* Country :
Postal Code :
Phone Number :
National ID (SSN) :

Driver's License

Driver's License Number :
Driver's License State : Driver's License Country :

Previous Next Submit Clear

PERJANJIAN KERJASAMA UNTUK TRANSAKSI DI MERCHANT
No. ..../KD/PP/...../...../....

Pada hari, tanggal, bulan dan tahun sebagaimana tercantum dalam akhir Perjanjian Kerjasama Untuk Transaksi di Merchant ini, telah dibuat dan ditandatangani Perjanjian Kerjasama Untuk Transaksi di Merchant, yaitu untuk :

- ☐ Transaksi Kartu Debet;
- ☐ Transaksi Payment Point;
- ☐ Transaksi Kartu Debet dan Payment Point.

(selanjutnya disebut dengan "**Perjanjian**") oleh dan antara:

1. **PT Bank Permata Tbk**, berkedudukan di Jakarta, dalam hal ini diwakili oleh pihak yang nama dan jabatannya tercantum pada akhir Perjanjian ini dan dengan demikian sah bertindak untuk dan atas nama PT. Bank Permata Tbk, selanjutnya disebut sebagai "**Bank**".

2. _____ (20 spasi) dalam hal ini diwakili oleh pihak yang nama dan jabatannya tercantum pada akhir Perjanjian ini, dengan demikian sah bertindak untuk dan atas nama _____ (20 spasi) selanjutnya disebut "**Merchant**"

Bank dan Merchant secara bersama-sama untuk selanjutnya disebut "Para Pihak".

Para Pihak terlebih dahulu menerangkan hal-hal sebagai berikut:

A. Bahwa Bank adalah suatu perseroan terbatas yang bergerak dibidang jasa perbankan, yang menyediakan dan memiliki berbagai produk dan fasilitas layanan perbankan antara lain produk kartu debet dan payment point.

B. Bahwa Merchant adalah subyek hukum yang merupakan mitra kerja Bank yang menyediakan barang dan/atau jasa yang pembeliannya dapat menggunakan kartu debet dan/atau melaksanakan fungsi sebagai payment point.

C. Bahwa Bank bermaksud bekerjasama dengan Merchant dan Merchant bersedia bekerjasama dengan Bank untuk penggunaan kartu debet untuk pembayaran atas pembelian barang dan/atau jasa yang dijual oleh Merchant dan/atau penyediaan fasilitas dan layanan perbankan sebagai payment point.

Berdasarkan hal-hal tersebut diatas, Para Pihak sepakat dan setuju untuk membuat dan menandatangani Perjanjian dengan syarat-syarat dan ketentuan-ketentuan sebagai berikut:

PASAL 1
DEFINISI

Sepanjang tidak diartikan lain, maka istilah-istilah tersebut di bawah ini mempunyai arti sebagai berikut:

1. **Chargeback** adalah pengajuan klaim oleh Pemegang Kartu Debet kepada Merchant melalui bank penerbit Kartu Debet dan *Acquirer* dengan cara sebagaimana diatur dalam Pasal 6 Perjanjian

2. **Daftar Hitam Merchant** adalah daftar yang memuat keterangan-keterangan tentang Merchant yang memiliki reputasi negatif, yang diterbitkan oleh pihak/badan yang berwenang sesuai dengan peraturan dan ketentuan yang berlaku.

3. **Dokumen** adalah Slip Transaksi EDC, faktur-faktur, pesanan pembelian, pesanan pengiriman, catatan-catatan dan dokumen-dokumen lainnya sehubungan dengan Transaksi Kartu Debet

4. **EDC** (Electronic Data Capture)/**POS** (Point Of Sales Terminal) adalah mesin/terminal milik Bank yang dipinjamkan Bank kepada Merchant yang digunakan untuk melakukan suatu Transaksi Kartu Debet antara lain Pembelian, Pembayaran, Transfer, pemindahbukuan, inquiry maupun transaksi-transaksi lainnya yang dimiliki oleh Bank, dimana semua transaksi tersebut dilakukan dengan menggunakan verifikasi PIN.

5. **EDC Wireless** adalah EDC yang disewakan oleh Bank dan dikenakan biaya sewa kepada Merchant yang berfungsi secara on line, tanpa menggunakan kabel untuk memudahkan Merchant dalam melayani Pemegang Kartu Debet.

6. **EDC Fixed Line** adalah EDC yang disewakan oleh Bank dan dikenakan biaya sewa kepada Merchant yang berfungsi secara on line, dengan menggunakan kabel untuk melayani Pemegang Kartu Debet

7. **Fasilitas Bank** adalah sarana dan/atau prasarana yang dimiliki dan disediakan oleh Bank untuk memperlancar jalannya transaksi perbankan oleh Pemegang Kartu Debet dan/atau Pelanggan Payment Point antara lain layanan PermataTel, PermataNet, Navigator, PermataAtm, PermataShop (EDC) dan layanan counter Bank serta layanan/fasilitas lain yang dikembangkan Bank di kemudian hari.

8. **Hari Kerja** adalah hari dimana Bank dan perbankan lainnya di Indonesia pada umumnya beroperasi dan melakukan transaksi kliring sesuai dengan ketentuan Bank Indonesia.

9. **Jaringan ATM** adalah PermataATM dan/atau semua jaringan ATM lainnya termasuk tapi tidak terbatas pada ALTO, Prima dan ATM Bersama dimana Bank bertindak sebagai acquirer

10. **Kartu Debet** adalah seluruh Kartu Debet Bank, serta Kartu Debet Bank Lain

11. **Kartu Debet Bank** adalah seluruh kartu debet yang diterbitkan oleh Bank termasuk kartu co-branding (dengan logo partner Bank), dan e-wallet yang digunakan oleh Pemegang Kartu Debet untuk melakukan Transaksi Kartu Debet.

12. **Kartu Debet Bank Lain** adalah kartu debet yang diterbitkan oleh bank-bank anggota jaringan ALTO, ATM Bersama, Prima dan jaringan lainnya yang disetujui oleh Bank yang digunakan oleh Pemegang Kartu Debet untuk melakukan Transaksi Kartu Debet.

13. **Limit Transaksi** adalah batas maksimum transaksi per hari dengan menggunakan Kartu Debet pada EDC Fixed Line dan/atau EDC Wireless yang dilakukan Pemegang Kartu Debet sesuai dengan limit transaksi melalui Automated Teller Machine (ATM) yang besarnya ditentukan oleh bank penerbit Kartu Debet.

14. **Merchant Data Form** adalah suatu formulir yang memuat keterangan-keterangan mengenai Merchant dan informasi lain yang diperlukan untuk pelaksanaan kerjasama yang merupakan satu kesatuan dan menjadi bagian yang tidak terpisahkan dari Perjanjian.

15. **Merchant Payment Point** adalah Merchant yang bekerjasama dengan Bank dalam hal pemasangan mesin EDC dan menerima pembayaran tagihan dan pembelian voucher isi ulang pulsa yang dilakukan oleh Pelanggan Payment Point yang memberikan sejumlah uang sebagai biaya administrasi kepada Merchant.

16. **Mitra** adalah pihak lain yang telah bekerjasama dengan Bank untuk memasarkan Voucher Telepon Prabayar dan/atau menerima pembayaran Tagihan melalui Fasilitas Bank.

17. **Nomor ID** adalah kode/nomor unik yang dimiliki oleh setiap Pelanggan Payment Point dan atau Pemegang Kartu Debet yang berfungsi sebagai akses untuk melakukan transaksi Pembayaran.

18. **Kode Persetujuan** adalah kode yang tercetak pada Slip Transaksi EDC yang merupakan kode persetujuan (*approval code*) atas setiap pelaksanaan Transaksi Kartu Debet dan Transaksi Payment Point.

19. **Pelanggan Payment Point** adalah pihak-pihak yang menggunakan layanan Merchant untuk melaksanakan transaksi Pembelian dan Pembayaran.

20. **Pembayaran** adalah transaksi pembayaran yang dilakukan oleh Pelanggan Payment Point di Merchant melalui Fasilitas Bank yang antara lain untuk pembayaran tagihan, cicilan, premi asuransi, pinjaman dan jenis pembayaran-pembayaran lainnya yang dapat dilakukan Pelanggan Payment Point di Merchant sesuai dengan fasilitas yang tersedia pada Fasilitas Bank sebagaimana dicantumkan dalam **Lampiran A Perjanjian**.

21. **Pembelian** adalah transaksi pembelian Voucher Telepon Prabayar yang dilakukan oleh Pelanggan Payment Point dan/atau Pemegang Kartu Debet di Merchant dengan menggunakan Fasilitas Bank yang ada di Merchant.

22. **Pemegang Kartu Debet** adalah setiap nasabah Bank dan atau bank lain yang memiliki Kartu Debet yang nama dan atau tanda tangannya tercantum pada Kartu Debet dan berhak menggunakan Kartu Debet untuk melaksanakan Transaksi Kartu Debet dan Transaksi Payment Point.

23. **Peralatan Bank** adalah EDC Fixed Line dan/atau EDC Wireless dan seluruh peralatan milik Bank lainnya (adaptor, kabel line telepon) yang dipinjamkan dan/atau disewakan oleh Bank kepada Merchant untuk pelaksanaan Transaksi Kartu Debet.

24. **PIN (Personal Indentification Number)** adalah sandi rahasia yang digunakan sebagai alat verifikasi oleh Pemegang Kartu Debet pada saat melakukan Transaksi Kartu Debet dan Transaksi Payment Point.

25. **Rekening Merchant** adalah rekening atas nama Merchant atau pemilik Merchant yang ada pada Bank baik sebagai rekening penampungan Merchant maupun rekening-rekening lainnya yang bukan rekening penampungan Merchant.

26. **Slip Transaksi EDC** adalah tanda terima tertulis yang diterbitkan oleh Bank melalui EDC yang diberikan kepada Pemegang Kartu Debet, setelah Pemegang Kartu Debet melakukan Transaksi Kartu Debet pada Merchant dan merupakan salah satu bukti telah terjadinya Transaksi Kartu Debet yang diantaranya mencantumkan Kode Persetujuan.

27. **Tagihan** adalah tagihan layanan umum, tagihan handphone, tagihan kartu kredit, tagihan asuransi, tagihan cicilan, tagihan *personal loan*, pembayaran tiket pesawat, tagihan internet, dan tagihan biaya pendidikan dan jenis tagihan-tagihan lainnya yang akan dikembangkan dikemudian hari, yang wajib dibayar Pemegang Kartu Debet atau Pelanggan Payment Point dengan menggunakan Fasilitas Bank.

28. **Transaksi Berhasil** adalah transaksi yang dilakukan pada Merchant dimana rekening Pemegang Kartu Debet sudah didebet dan Rekening Merchant sudah dikreditkan dengan jumlah sebesar Transaksi Kartu Debet yang dilakukan oleh Pemegang Kartu Debet dengan ditandai tercetaknya Kode Persetujuan pada Slip Transaksi EDC.

29. **Transaksi Kartu Debet** adalah transaksi pembayaran barang dan/atau jasa yang dilakukan oleh Pemegang Kartu Debet pada Merchant termasuk tapi tidak terbatas pada pembayaran, pemindahbukuan, transfer dan inquiry melalui Peralatan Bank dengan menggunakan Kartu Debet Bank dan Kartu Debet Bank Lain, dimana semua transaksi tersebut dilakukan dengan menggunakan verifikasi PIN.

30. **Transaksi Payment Point** adalah transaksi Pembayaran, Pembelian dan Transfer, dimana semua transaksi tersebut dilakukan dengan menggunakan verifikasi PIN

31. **Transfer** adalah transaksi pengiriman uang yang dilakukan oleh Pelanggan Payment Point pada Merchant dan ke rekening-rekening yang ditentukan Pelanggan Payment Point yang berada dalam cakupan pelayanan Fasilitas Bank.

32. **Voucher Telepon Prabayar** adalah voucher isi ulang pulsa untuk telepon prabayar yang disediakan oleh Mitra melalui Fasilitas Bank.

PASAL 2
RUANG LINGKUP PERJANJIAN

Para Pihak sepakat bahwa ruang lingkup Perjanjian adalah sebagai berikut:
1. Penempatan Peralatan Bank pada Merchant sebagaimana diatur dalam Pasal 13 Perjanjian.
2. Penerimaan Transaksi Kartu Debet yang dilakukan oleh Pemegang Kartu Debet melalui Peralatan Bank pada Merchant.
3. Penggunaan Fasilitas Bank oleh Merchant untuk melakukan Transaksi Payment Point untuk kepentingan Pelanggan Payment Point.

PASAL 3
TATA CARA PELAKSANAAN TRANSAKSI KARTU DEBET

Para Pihak sepakat bahwa khusus untuk pelaksanaan Transaksi Kartu Debet yang dilakukan Pemegang Kartu Debet pada Merchant tunduk pada ketentuan-ketentuan sebagai berikut:

A. Transaksi Kartu Debet

1. Transaksi Pemegang Kartu Debet pada Merchant yang dianggap sah adalah Transaksi Berhasil. Jika telah terjadi Transaksi Berhasil, maka pada saat yang sama Merchant wajib menyerahkan barang atau jasa yang telah dibeli kepada Pemegang Kartu Debet dengan memberikan bukti Slip Transaksi EDC. Slip Transaksi EDC tersebut tercetak dalam rangkap 2 (dua) yang aslinya disimpan oleh Merchant dan copy diberikan kepada Pemegang Kartu Debet atau Bank apabila diperlukan sebagaimana dinyatakan dalam Pasal 8 Perjanjian.

2. Merchant hanya dapat menerima transaksi Pemegang Kartu Debet sesuai dengan Limit Transaksi yang telah ditetapkan. Apabila Merchant menerima transaksi yang dilakukan Pemegang Kartu Debet yang melebihi Limit Transaksi, maka segala kerugian dan resiko yang timbul sepenuhnya menjadi tanggung jawab bank penerbit Kartu Debet.

3. Bank akan melakukan pembayaran kepada Merchant pada waktu yang sama dengan waktu Transaksi Kartu Debet dengan mengkreditkan ke Rekening Merchant yang ada pada Bank tanpa potongan apapun. Besarnya jumlah Transaksi Kartu Debet yang akan dikreditkan ke Rekening Merchant adalah sesuai dengan jumlah yang ada pada catatan Bank, dan Merchant menyetujui bahwa dalam hal terdapat ketidaksesuaian besarnya jumlah Transaksi Kartu Debet antara catatan Merchant dengan catatan Bank, maka Bank akan melakukan pembayaran kepada Merchant sesuai jumlah Transaksi Kartu Debet yang ada pada catatan Bank.

4. Apabila ternyata Transaksi Kartu Debet dilakukan dengan adanya unsur-unsur kejahatan atau penipuan atau kecurangan (fraud) dan adanya keterlibatan Merchant dan/atau keluarganya dan/atau pegawainya dalam setiap Transaksi Kartu Debet, maka Merchant dengan ini melepaskan Bank dari tuntutan dan/atau gugatan

dan/atau klaim dan/atau ganti rugi yang diderita oleh Merchant dan/atau keluarganya dan/atau pegawainya, dan apabila transaksi tersebut menimbulkan kerugian pada Bank, maka Bank berhak untuk mendebet Rekening Merchant sebesar nilai kerugian yang dialami Bank.

5. Para Pihak sepakat bahwa semua pengkreditan atas Transaksi Kartu Debet dilakukan dalam mata uang Rupiah.

6. Apabila ada perubahan Rekening Merchant, maka Merchant wajib memberitahukan secara tertulis kepada Bank sekurang-kurangnya 15 (lima belas) Hari Kerja sebelum perubahan tersebut berlaku efektif dan Merchant tunduk pada aturan yang ditetapkan oleh Bank.

7. Apabila terdapat selisih pembayaran kepada Merchant, maka dalam hal terjadi selisih lebih, Merchant wajib mengembalikan selisih lebih tersebut kepada Bank melalui Fasilitas Bank dalam waktu selambat-lambatnya 7 (tujuh) Hari Kerja setelah tanggal Transaksi Kartu Debet atau setelah Merchant menerima laporan dari Bank mengenai selisih tersebut (mana yang lebih dulu), dan apabila terjadi selisih kurang, maka Merchant akan melaporkan kepada Bank dalam waktu selambat-lambatnya 20 (dua puluh) hari kalender sejak tanggal Transaksi Kartu Debet dan Bank akan membayarkan selisih kurang tersebut selambat-lambatnya 7 (tujuh) Hari Kerja setelah menerima laporan dari Merchant. Apabila laporan atas selisih pembayaran kepada Merchant dilaporkan oleh Merchant setelah lewatnya jangka waktu yang ditentukan dan/atau menurut catatan Bank transaksi yang dilaporkan Merchant merupakan Transaksi Berhasil, maka Bank berhak untuk menolak laporan atau klaim Merchant dan tidak berkewajiban melakukan pembayaran apapun terkait dengan klaim tersebut.

8. Dalam hal terjadi kesalahan/kekeliruan pembayaran kepada Merchant yang dilakukan oleh Bank yang menyebabkan pembayaran tersebut menjadi lebih atau kurang dari jumlah pembayaran yang seharusnya dibayarkan oleh Bank, maka Bank berhak dengan itikad baik, untuk setiap saat memperbaiki kesalahan/kekeliruan tersebut dengan melakukan pendebetan atau pengkreditan dari/ke Rekening Merchant. Sehubungan dengan hal tersebut, Merchant dengan ini memberikan kuasa kepada Bank untuk setiap saat melakukan pendebetan Rekening Merchant untuk melakukan perbaikan pembayaran tersebut.

9. Transaksi Kartu Debet dengan menggunakan Kartu Debet jaringan lokal (jaringan ATM Bersama, Prima dan ALTO) yang gagal dimana rekening Pemegang Kartu Debet sudah terdebet, maka Merchant tidak diperbolehkan untuk melakukan pengembalian dana Pemegang Kartu Debet dengan cara memberikan uang tunai ataupun barang kepada Pemegang Kartu Debet. Pengembalian uang Pemegang Kartu Debet akan dilakukan dengan proses pengkreditan kembali sejumlah uang tersebut pada rekening Pemegang Kartu Debet melalui masing-masing bank penerbit Kartu Debet.

B. Otorisasi

1. Untuk setiap Transaksi Berhasil, Bank akan mengirimkan Kode Persetujuan yang tercetak pada Slip Transaksi EDC.

2. Apabila pada layar EDC tidak muncul Kode Persetujuan dan/atau tidak ada respon atas transaksi dan/atau EDC tidak mengeluarkan Slip Transaksi EDC, maka transaksi dianggap gagal dan Merchant wajib menolak untuk melanjutkan Transaksi Kartu Debet serta barang/jasa yang dibayar tidak boleh diserahkan kepada Pemegang Kartu Debet. Jika Pemegang Kartu Debet adalah nasabah Bank, maka Merchant wajib menginformasikan Pemegang Kartu Debet untuk menghubungi

layanan PermataTel atau melalui Fasilitas Bank tetapi jika Pemegang Kartu Debet adalah nasabah bank lain, maka Merchant wajib menginformasikan Pemegang Kartu Debet tersebut untuk menghubungi bank penerbit Kartu Debet sebagaimana tercantum dalam Pasal 3 huruf A ayat 8 Perjanjian. Apabila Merchant tetap melakukan pengembalian dengan cara memberikan uang tunai atsupun barang kecada Pemegang Kartu Debet, maka dalam hal terjadi Chargeback kepada Bank. Bank berhak untuk melakukan pendebetan dari Rekening Merchant sejumlah nilai Chargeback tersebut.

PASAL 4
TATA CARA PELAKSANAAN TRANSAKSI PAYMENT POINT

Para Pihak sepakat bahwa khusus untuk pelaksanaan Transaksi Payment Point yang dilakukan oleh Merchant untuk kepentingan Pelanggan Payment Point atau oleh Pemegang Kartu Debet pada Merchant tunduk pada ketentuan-ketentuan sebagai berikut:

A. Umum

1. Merchant wajib mematuhi ketentuan mengenai pelaksanaan Transaksi Payment Point sebagaimana diuraikan dalam Perjanjian ini.

2. Setiap transaksi Pembayaran yang dilakukan oleh Pelanggan Payment Point melalui Merchant dan/atau yang dilakukan oleh Pemegang Kartu Debet akan dianggap sah, apabila Pelanggan Payment Point dan/atau Pemegang Kartu Debet sudah memasukkan Nomor ID dengan benar dan terdapat Kode Persetujuan pada Slip Transaksi EDC serta Rekening Merchant dan/atau Rekening Pemegang Kartu Debet sudah terdebet sebesar jumlah transaksi Pembayaran yang dilakukan oleh Pelanggan Payment Point dan/atau Pemegang Kartu Debet.

3. Setiap transaksi Pembelian yang dilakukan oleh Pelanggan Payment Point dan/atau Pemegang Kartu Debet pada Merchant akan dianggap sah jika Rekening Merchant atau Rekening Pemegang Kartu Debet telah terdebet sebesar nilai Voucher Telepon Prabayar dan terdapat Kode Persetujuan pada Slip Transaksi EDC serta saldo pulsa telepon milik Pelanggan Payment Point dan/atau Pemegang Kartu Debet telah bertambah sebesar nilai Voucher Telepon Prabayar yang dibeli Pelanggan Payment Point dan/atau Pemegang Kartu Debet.

4. Setiap transaksi Transfer yang dilakukan oleh Pelanggan Payment Point dan/atau Pemegang Kartu Debet pada Merchant akan dianggap sah jika Rekening Merchant atau Rekening Pemegang Kartu Debet telah terdebet sebesar nilai yang ditransfer oleh Pelanggan Payment Point dan/atau Pemegang Kartu Debet dan rekening tujuan Transfer telah terkredit sejumlah nilai tersebut serta terdapat Kode Persetujuan pada Slip Transaksi EDC.

B. Pembayaran

1. Para Pihak sepakat bahwa semua Transaksi Payment Point akan dilakukan dalam mata uang Rupiah. Sehubungan dengan pelaksanaan Transaksi Payment Point berdasarkan Perjanjian, maka dengan ini Merchant memberikan kuasa dan wewenang kepada Bank untuk mendebet dana dalam Rekening Merchant sejumlah nilai Transaksi Payment Point yang dilakukan dan mengkreditkan dana yang didebet tersebut ke rekening-rekening pihak yang berkepentingan atas Transaksi Payment Point tersebut.

2. Merchant dengan ini bertanggung jawab dan membebaskan Bank dari tuntutan dan/atau gugatan dan/atau klaim dan/atau permintaan ganti kerugian dari pihak manapun yang mungkin timbul sehubungan dengan terjadinya Transaksi Payment

Point yang disertai dengan unsur-unsur kejahatan atau penipuan atau kecurangan (fraud), dan apabila transaksi tersebut menimbulkan kerugian pada Bank, maka Bank berhak mendebet Rekening Merchant sebesar nilai kerugian yang dialami Bank.

3. Apabila terdapat selisih pendebetan dalam Rekening Merchant, maka selambat-lambatnya 7 (tujuh) Hari Kerja sejak tanggal terjadinya Transaksi Payment Point, Merchant wajib melaporkan selisih tersebut kepada Bank melalui Fasilitas Bank. Apabila laporan atas selisih pendebetan baru dilaporkan oleh Merchant setelah lewatnya jangka waktu yang ditentukan dan/atau menurut catatan Bank Transaksi Payment Point yang dilaporkan Merchant merupakan Transaksi Berhasil, maka Bank berhak untuk menolak dan mengabaikan laporan atau klaim Merchant. Dalam hal terjadi keadaan demikian, maka Para Pihak sepakat bahwa catatan yang dijadikan acuan rekonsiliasi adalah catatan Transaksi Payment Point yang ada pada Bank.

C. Komitmen Kerjasama

Bank berhak dan berwenang untuk sewaktu-waktu mengubah persyaratan dan ketentuan mengenai Transaksi Payment Point dan setiap perubahan akan diberitahukan secara tertulis terlebih dahulu selambat-lambatnya 30 (tigapuluh) Hari Kerja sebelum perubahan tersebut berlaku, dan perubahan tersebut mengikat bagi Merchant dan Merchant berkewajiban untuk mentaati setiap perubahan persyaratan dan ketentuan mengenai pelaksanaan Transaksi Payment Point.

D. Otorisasi Transaksi

1. Untuk setiap Transaksi Payment Point yang berhasil, Bank akan mengirimkan Kode Persetujuan yang akan tercetak pada Slip Transaksi EDC yang digunakan sebagai salah satu alat bukti telah dilakukannya Transaksi Berhasil.

2. Dalam hal terjadi gangguan atas komunikasi dimana Transaksi Payment Point oleh Merchant dibatalkan atau ditolak untuk diteruskan namun terjadi pendebetan Rekening Merchant, maka Merchant wajib melaporkan Transaksi Payment Point tersebut kepada Bank untuk disesuaikan dengan catatan yang ada pada Bank pada hari yang sama saat Transaksi Payment Point dilakukan. Apabila menurut catatan Bank Transaksi Payment Point yang dilaporkan Merchant merupakan Transaksi Berhasil, maka yang akan dijadikan acuan adalah catatan Bank, karenanya Merchant bertanggung jawab dan membebaskan Bank dari segala tuntutan dan/atau gugatan dan/atau klaim yang mungkin timbul dan diajukan oleh Pelanggan Payment Point dan/atau pihak lain manapun juga yang diakibatkan oleh hal-hal tersebut.

3. Dalam hal terjadi gangguan atas komunikasi EDC dimana Transaksi Payment Point dibatalkan oleh Pelanggan Payment Point karena Slip Transaksi EDC tidak tercetak, maka segala resiko dan kerugian menjadi tanggung jawab Merchant sepenuhnya dan Merchant wajib membayar setiap dan semua tagihan yang timbul yang diajukan oleh Mitra melalui Bank.

PASAL 5
PEMBATALAN TRANSAKSI

Khusus untuk Transaksi Kartu Debet yang menggunakan jaringan ATM Bersama, Prima dan ALTO, Merchant memahami bahwa Pemegang Kartu Debet tidak dapat melakukan pembatalan Transaksi Kartu Debet dan/atau Transaksi Payment Point yang dilakukan pada Merchant, karena dana dari rekening Pemegang Kartu Debet secara langsung terdebet untuk dikreditkan ke Rekening Merchant pada saat yang sama dengan pelaksanaan transaksi, apabila Merchant

melanggar ketentuan pasal ini, maka Merchant bertanggung jawab sepenuhnya atas resiko yang timbul dari pelanggaran tersebut dan dengan ini melepaskan Bank dari segala tuntutan, gugatan dan atau ganti rugi dari pihak manapun.

PASAL 6
CHARGEBACK

Para Pihak sepakat bahwa ketentuan mengenai Chargeback sebagai berikut:

1. Dalam hal Pemegang Kartu Debet tidak mengakui adanya Transaksi Kartu Debet serta Merchant tidak dapat memberikan salinan Slip Transaksi EDC dan bukti-bukti lainnya atas Transaksi Kartu Debet dalam waktu paling lambat 1 (satu) Hari Kerja setelah ada permintaan dari Bank, maka Merchant akan dikenakan Chargeback oleh Bank minimal sebesar nilai Transaksi Kartu Debet.

2. Dalam hal terjadi Chargeback, Bank tetap berhak dan berwenang untuk mendebet Rekening Merchant dalam jumlah yang sama dengan jumlah Chargeback yang harus dibayarkan oleh Merchant.

PASAL 7
PENERIMAAN TRANSAKSI KARTU DEBET

Para Pihak sepakat bahwa khusus untuk penerimaan Transaksi Kartu Debet, berlaku ketentuan-ketentuan sebagai berikut:

1. Merchant berhak tidak memproses dan/atau menolak Transaksi Kartu Debet apabila:
   a. Kartu Debet belum berlaku.
   b. Kartu Debet telah diubah, dirusak atau dicetak ulang dengan cara apapun tanpa persetujuan Bank.
   c. Kartu Debet telah diblokir, karena sebab apapun juga.
   d. Kartu Debet telah habis masa berlakunya (kecuali ada pemberitahuan dari bank penerbit Kartu Debet).
   e. Tidak terdapat pita magnetis pada Kartu Debet atau pita magnetis rusak.
   f. Mesin EDC Fixed Line dan/atau EDC Wireless tidak mengeluarkan Slip Transaksi EDC.
   g. Untuk Transaksi Kartu Debet, pada Slip Transaksi EDC tidak tercantum Kode Persetujuan.
   h. Merchant mencurigai bahwa Kartu Debet yang akan dipergunakan untuk Transaksi Kartu Debet diduga atau terindikasi palsu atau hasil tindak kejahatan.
   i. Terdapat perbedaan nomor kartu yang tercetak di Kartu Debet dengan nomor kartu yang tertera di layar EDC.

2. Bila Kartu Debet yang digunakan ternyata dicurigai sebagai kartu palsu atau curian atau merupakan hasil dari tindak kejahatan, maka Merchant wajib melakukan tindakan-tindakan sebagai berikut:
   a. Tidak meneruskan Transaksi Kartu Debet tersebut.
   b. menahan Kartu Debet tersebut dengan cara yang baik serta sopan dan kemudian memberitahukan kepada bank penerbit Kartu Debet dan kemudian wajib menjalankan instruksi-instruksi selanjutnya dari bank penerbit Kartu Debet.

3. Dalam keadaan apapun, data Pemegang Kartu Debet yang terdapat dalam Slip Transaksi EDC tidak diperkenankan ditulis, diperbaiki atau diganti, direvisi dan/atau diubah secara manual. Apabila Merchant melanggar ketentuan ini, maka seluruh konsekwensi yang timbul merupakan tanggung jawab Merchant sepenuhnya dan Merchant berkewajiban memberikan ganti rugi kepada Bank dan/atau Pemegang Kartu Debet sebesar kerugian yang mungkin diderita oleh Bank dan/atau Pemegang Kartu Debet akibat dari transaksi tersebut.

PASAL 8
PENERIMAAN TRANSAKSI PAYMENT POINT

Para Pihak sepakat bahwa khusus untuk penerimaan Transaksi Payment Point berlaku ketentuan-ketentuan sebagai berikut:

1. Dalam hal terjadi kegagalan Transaksi Payment Point dan/atau gangguan pelaksanaan Transaksi Payment Point yang diakibatkan oleh kesalahan-kelalaian Merchant dalam menyediakan peralatan dan fasilitas penunjang pelaksanaan Transaksi Payment Point, maka seluruh kerugian yang timbul sehubungan dengan hal tersebut menjadi beban dan tanggung jawab Merchant dan Merchant dengan ini membebaskan Bank dari segala tuntutan dan/atau gugatan yang timbul akibat gagal atau terganggunya pelaksanaan Transaksi Payment Point.

2. Dalam keadaan apapun, data Pelanggan Payment Point dan/atau Pemegang Kartu Debet yang terdapat dalam Slip Transaksi EDC tidak diberankan untuk ditulis, diperbaiki, diganti, diremov dan/atau diubah secara manual oleh Merchant. Apabila Merchant melanggar ketentuan ini, maka seluruh risiko yang mungkin timbul karenanya menjadi beban dan tanggung jawab Merchant sepenuhnya dan Merchant berkewajiban untuk memberikan ganti kerugian kepada Bank dan/atau Pelanggan Payment Point dan/atau Pemegang Kartu Debet sebesar jumlah kerugian yang dialami oleh Bank dan/atau Pelanggan Payment Point dan/atau Pemegang Kartu Debet.

3. Atas setiap pelaksanaan Transaksi Payment Point berdasarkan Perjanjian, Bank berhak mengenakan biaya (charge) kepada Pelanggan Payment Point dan/atau Pemegang Kartu Debet yang akan diperlakukan sebagai pendapatan Bank dalam jumlah sebagaimana ditentukan dalam ayat 4 pasal ini. Besarnya biaya yang dibebankan kepada Pelanggan Payment Point dan/atau Pemegang Kartu Debet wajib diberitahukan oleh Merchant kepada Pelanggan Payment Point dan/atau Pemegang Kartu Debet sebelum Pelanggan Payment Point dan/atau Pemegang Kartu Debet melakukan Transaksi Payment Point dan besarnya biaya tersebut akan tercetak pada Slip Transaksi EDC terpisah dengan nilai Transaksi Payment Point. Atas pembebanan biaya kepada Pelanggan Payment Point dan/atau Pemegang Kartu Debet sebagaimana dimaksud dalam ayat ini, Merchant sepenuhnya bertanggung jawab atas setiap tuntutan, klaim dan/atau gugatan dari Pelanggan Payment Point dan/atau Pemegang Kartu Debet dan/atau pihak lain manapun juga yang mungkin timbul sehubungan dengan pembebanan biaya tersebut.

4. Bank berhak untuk menentukan besarnya biaya yang dibebankan kepada Pelanggan Payment Point dan/atau Pemegang Kartu Debet untuk setiap jenis Transaksi Payment Point berdasarkan Perjanjian, sebagaimana tercantum dalam Lampiran A Perjanjian. Atas pertimbangan Bank sendiri, Bank berhak dan berwenang dari waktu ke waktu untuk mengubah besarnya biaya tersebut dengan melakukan pemberitahuan tertulis terlebih dahulu kepada Merchant paling lambat 30 (tiga puluh) Hari Kerja sebelum perubahan tersebut diberlakukan. Merchant wajib memberitahukan perubahan biaya tersebut kepada Pelanggan Payment Point dan/atau Pemegang Kartu Debet.

5. Untuk setiap pelaksanaan Transaksi Payment Point yang dilakukan oleh Merchant untuk kepentingan Pelanggan Payment Point, Bank akan memberikan insentif kepada Merchant sesuai dengan jenis Transaksi Payment Point yang dilakukan oleh Pelanggan Payment Point dengan besaran yang ditetapkan dalam Lampiran A Perjanjian. Para Pihak sepakat bahwa Bank atas pertimbangannya sendiri, berhak dan berwenang untuk mengubah besarnya insentif tersebut dengan ketentuan bahwa Bank akan memberitahukan secara tertulis terlebih dahulu kepada Merchant selambat-lambatnya 30 (tiga puluh) Hari Kerja sebelum perubahan tersebut diberlakukan.

6. Merchant dengan ini menyetujui bahwa jumlah pendapatan yang merupakan hak dari Bank akan diambil langsung oleh Bank dengan cara mendebet Rekening Merchant pada saat atau setelah pelaksanaan setiap jenis Transaksi Payment Point sesuai waktu yang

ditentukan oleh Bank. Merchant dengan ini memberikan kuasa kepada Bank untuk melakukan pendebetan Rekening Merchant sehubungan dengan pembayaran pendapatan Bank.

7. Merchant hanya dapat melaksanakan Transaksi Payment Point sesuai dengan jenis transaksi Pembayaran dan Pembelian sebagaimana tercantum dalam **Lampiran A** Perjanjian dan dalam rentang Limit Transaksi yang telah ditetapkan oleh Bank. Apabila Merchant menjalankan Transaksi Payment Point diluar yang diatur dalam **Lampiran A** Perjanjian, dan menerima transaksi melebihi Limit Transaksi, maka Bank dapat dan berhak untuk menolak Transaksi Payment Point tersebut.

8. Setiap risiko, kerugian, klaim, tuntutan dan/atau gugatan yang mungkin timbul yang diajukan oleh Pelanggan Payment Point dan/atau pihak lain manapun juga kepada Bank sebagai akibat dari kesalahan/kelalaian Merchant dalam melaksanakan penerimaan Transaksi Payment Point dengan menggunakan Fasilitas Bank sepenuhnya menjadi tanggung jawab Merchant.

PASAL 9
BUKTI TRANSAKSI

Para Pihak sepakat bahwa ketentuan Pasal 9 tentang Bukti Transaksi hanya berlaku untuk Transaksi Kartu Debet serta Transaksi Payment Point.

1. Para Pihak sepakat bahwa pelaksanaan Transaksi Kartu Debet, dan Transaksi Payment Point dapat dibuktikan melalui dokumen-dokumen sebagai berikut:
   a. Slip Transaksi EDC; atau
   b. Info saldo dan mutasi melalui fax on demand PermataTel; atau
   c. Info saldo dan mutasi pada PermataNet; atau
   d. Info saldo dan mutasi pada PermataMobile; atau
   e. Rekening koran Merchant; atau
   f. Mini statement (8 transaksi terakhir) pada PermataATM; atau
   g. Bukti lainnya yang ditemukan kemudian oleh Bank atau bank penerbit Kartu Debet.

2. Khusus untuk Transaksi Kartu Debet berlaku ketentuan-ketentuan sebagai berikut:
   a. Para Pihak sepakat bahwa berhasilnya Transaksi Kartu Debet dapat dibuktikan dengan adanya Kode Persetujuan pada Slip Transaksi EDC. Slip Transaksi EDC terdiri dari 2 (dua) rangkap, yang setiap bagiannya merupakan bukti transaksi yang sah, dengan pembagian sebagai berikut:
      i Slip Asli untuk Merchant
      ii Kop/tembusan pertama untuk Pemegang Kartu Debet, dan dapat di-print kembali untuk Bank atau bank penerbit Kartu Debet apabila diperlukan

   b. Merchant wajib memastikan bahwa penginputan PIN pada mesin EDC oleh Pemegang Kartu Debet pada saat Pemegang Kartu Debet melakukan Transaksi Kartu Debet dilakukan dengan aman dan tidak diketahui oleh Merchant maupun pihak lain.

   c. Merchant dengan ini melepaskan Bank dari segala tuntutan dan/atau gugatan dari Pemegang Kartu Debet dan/atau pihak lain yang disebabkan oleh kelalaian Merchant dalam penyerahan barang dan/atau jasa sehubungan dengan pelaksanaan Transaksi Kartu Debet sebagaimana dinyatakan dalam Pasal 3 huruf B ayat 2 Perjanjian.

3. Khusus untuk Transaksi Payment Point, Para Pihak setuju berlakunya ketentuan-ketentuan sebagai berikut:

   a. Khusus pelaksanaan Transaksi Payment Point dengan menggunakan layanan

PermataShop. Para Pihak sepakat bahwa bukti berhasilnya Transaksi Payment Point adalah tercetaknya Slip Transaksi EDC yang mencantumkan Kode Persetujuan. Slip Transaksi EDC akan dicetak dalam rangkap 2 (dua) yaitu 1 (satu) lembar cetakan asli dan 1 (satu) lembar copy. Slip Transaksi EDC yang merupakan cetakan asli wajib diserahkan oleh Merchant kepada Pelanggan Payment Point sedangkan Slip Transaksi EDC yang berbentuk copy wajib disimpan oleh Merchant.

b. Merchant wajib memastikan bahwa Slip Transaksi EDC tercetak dalam rangkap 2 (Dua) dan seluruh data Transaksi Payment Point antara lain yaitu nama Pelanggan Payment Point, keterangan yang berhubungan dengan Transaksi Payment Point, Kode Persetujuan dan Nomor ID Pelanggan Payment Point telah tercetak dengan baik.

c. Apabila Slip Transaksi EDC tidak tercetak dengan baik, maka Merchant wajib memastikan melalui Fasilitas Bank sebagaimana disebutkan pada Pasal 9 ayat 1 huruf b, c, d Perjanjian bahwa Rekening Merchant telah berhasil didebet. Jika ternyata Merchant telah menerima konfirmasi Transaksi Berhasil, maka Merchant wajib untuk mengulang pencetakan Slip Transaksi EDC dan melakukan pelaporan kepada Bank. Merchant dengan ini melepaskan Bank dari segala tuntutan dan atau gugatan dari Pelanggan Payment Point dan atau pihak lain yang disebabkan oleh kelalaian Merchant dalam menyerahkan Slip Transaksi EDC kepada Pelanggan Payment Point sehubungan dengan pelaksanaan Transaksi Payment Point sebagaimana dimyatakan dalam ayat ini.

PASAL 10
KLAIM PEMEGANG KARTU DAN/ATAU PELANGGAN

1. Para Pihak sepakat bahwa Merchant wajib untuk menangani secara langsung klaim/keluhan Pemegang Kartu Debet dan/atau Pelanggan Payment Point sehubungan dengan pembelian barang dan atau jasa yang pembayarannya dilakukan melalui Peralatan Bank atau pelaksanaan Transaksi Payment Point selambat-lambatnya 1 (satu) bulan setelah tanggal transaksi tersebut dilaksanakan.

2. Merchant akan bertanggung jawab dan dengan ini membebaskan Bank dari tuntutan apapun yang dilakukan oleh Pemegang Kartu Debet dan/atau Pelanggan Payment Point, jika terjadi perselisihan antara Pemegang Kartu Debet dan/atau Pelanggan Payment Point dengan Merchant sehubungan dengan pembelian barang dan/atau jasa dan pelaksanaan Transaksi Payment Point.

3. Para Pihak sepakat bahwa Bank wajib menangani setiap klaim Pemegang Kartu Debet yang berhubungan dengan proses pembayaran kepada Merchant, selambat-lambatnya 1 (satu) bulan dari tanggal Transaksi Kartu Debet apabila seluruh dokumen dan persyaratan yang ditentukan oleh Bank telah terpenuhi.

4. Apabila Bank memerlukan bukti/dokumen pendukung dari transaksi yang telah dilakukan, maka Merchant setuju dan wajib untuk memberikan bukti/dokumen yang dimaksud dalam jangka waktu 1 (satu) Hari Kerja sejak permintaan tertulis pertama dari Bank. Dalam hal Merchant gagal memenuhi permintaan tersebut dalam jangka waktu yang telah ditentukan, maka Bank berhak untuk langsung mendebet Rekening Merchant minimal sebesar nilai transaksi yang diklaim oleh Pemegang Kartu Debet dan/atau Pelanggan Payment Point.

PASAL 11
TRANSAKSI MENCURIGAKAN

1. Dalam hal terjadi transaksi yang mencurigakan menurut Bank yang dilakukan melalui mesin EDC yang ada pada Merchant, maka Bank berhak untuk menghentikan/menonaktifkan/menarik mesin EDC yang ada pada Merchant dan/atau memblokir dana jaminan penempatan Peralatan Bank sampai dengan adanya pemberitahuan dari Bank.

2. Dalam hal terjadi Transaksi Kartu Debet dan/atau Transaksi Payment Point yang mencurigakan dan atau melebihi batasan jumlah tertentu yang ditetapkan oleh Bank terhadap Merchant karena alasan apapun juga, maka Bank berhak sewaktu-waktu menunda pengkreditan dana ke Rekening Merchant atau melakukan pemblokiran Rekening Merchant sampai proses investigasi selesai dilakukan dalam jangka waktu yang ditentukan oleh Bank.

3. Apabila terbukti bahwa transaksi tersebut pada ayat 1 dan 2 di atas adalah transaksi yang melanggar Perjanjian dan atau peraturan perundang-undangan yang berlaku, maka Merchant dengan ini memberi kuasa kepada Bank untuk mencairkan dana jaminan penempatan Peralatan Bank tersebut untuk menggantikan kerugian Bank tanpa mengurangi hak Bank untuk melakukan tuntutan ganti rugi atas seluruh kerugian yang timbul akibat transaksi tersebut dan Bank tidak wajib melakukan pengembalian atas dana yang ditunda pengkreditannya oleh Bank atau dana yang diblokir sebagaimana dimaksud pada ayat 2 Pasal ini.

4. Merchant harus menyediakan dana atau mengembalikan dana sejumlah nilai transaksi yang diindikasikan sebagai transaksi mencurigakan oleh Bank, dalam hal dana pada Rekening Merchant belum berhasil terblokir atau dana tidak mencukupi dalam waktu selambat-lambatnya 7 (tujuh) Hari Kerja terhitung sejak tanggal Bank menginformasikan adanya indikasi transaksi mencurigakan tersebut kepada Merchant.

PASAL 12
PROMOSI LAYANAN

1. Merchant wajib untuk memasang tanda/logo EDC Fixed Line dan/atau EDC Wireless yang disediakan oleh Bank, di tempat-tempat yang mudah dilihat agar Pemegang Kartu Debet mengetahui bahwa Merchant menerima transaksi pembayaran melalui EDC Fixed Line dan/atau EDC Wireless.

2. Merchant wajib menginformasikan mengenai Peralatan Bank kepada seluruh karyawannya, terutama kepada karyawan yang bekerja di lokasi penjualan barang/produk/jasa.

3. Bank akan menginformasikan mengenai fasilitas EDC Fixed Line dan/atau EDC Wireless untuk pembelian barang/produk pada Merchant kepada setiap Pemegang Kartu Debet melalui media yang ditentukan oleh Bank.

4. Merchant memberi hak dan wewenang kepada Bank untuk mencantumkan nama Merchant dalam buku petunjuk atau sarana promosi apapun yang telah ditentukan oleh Bank.

5. Biaya yang timbul dari promosi atas EDC Fixed Line dan/atau EDC Wireless sebagaimana diatur dalam pasal ini akan ditanggung oleh masing-masing pihak.

PASAL 13
PENEMPATAN PERALATAN BANK

1. Sehubungan dengan pelaksanaan Perjanjian Bank akan meminjamkan dan/atau menyewakan Peralatan Bank kepada Merchant dan Peralatan Bank tersebut merupakan milik Bank sepenuhnya yang wajib dipelihara dengan baik oleh Merchant.

2. Dalam hal Merchant menggunakan EDC, maka Merchant wajib membayar biaya sewa atas mesin EDC tersebut kepada Bank dalam jumlah sebagaimana tercantum dalam Merchant Data Form.
   Besarnya biaya sewa yang tercantum dalam Merchant Data Form dapat diubah sewaktu-waktu oleh Bank dengan melakukan pemberitahuan tertulis kepada Merchant dalam waktu paling lambat 30 (tigapuluh) Hari Kerja sebelum perubahan biaya sewa tersebut berlaku efektif.

3. Pembayaran uang sewa oleh Merchant untuk penggunaan EDC, akan dilakukan dengan cara Bank akan mendebet Rekening Merchant sejumlah uang sewa, dengan ketentuan sebagai berikut
   a. Apabila Rekening Merchant gagal/tidak dapat didebet untuk pembayaran sewa selama 3 (tiga) bulan berturut-turut karena sebab apapun juga, maka Bank berhak untuk melakukan penutupan Merchant tanpa pemberitahuan tertulis terlebih dahulu kepada Merchant dan mencairkan jaminan penggunaan Peralatan Bank, untuk membayar tunggakan uang sewa yang belum dibayarkan oleh Merchant. Apabila masih terdapat sisa dana jaminan Peralatan Bank, maka Bank akan melakukan pembiokiran kembali atas dana tersebut sampai dengan Merchant melakukan klaim atas dana tersebut dan mengembalikan mesin EDC kepada Bank
      Merchant tetap wajib membayar biaya sewa EDC selama mesin EDC belum dikembalikan kepada Bank dan Bank akan mengembalikan sisa dana jaminan Peralatan Bank apabila mesin EDC sudah dikembalikan kepada Bank.

   b. Dalam hal Merchant tidak dapat dihubungi dan Merchant telah menunggak pembayaran biaya sewa selama 3 (tiga) bulan berturut-turut dan mesin EDC tidak dikembalikan kepada Bank, maka Bank berhak untuk melakukan penutupan Merchant dan membuka pemblokiran atas jaminan penggunaan Peralatan Bank untuk langsung didebet sebesar tunggakan pembayaran sewa oleh Merchant. Kelebihan dana setelah didebet akan dilakukan pembiokran kembali atas dana tersebut sampai dengan Merchant melakukan klaim atas dana tersebut dan mengembalikan mesin EDC kepada Bank. Proses pendebetan biaya sewa EDC akan tetap dilakukan selama mesin EDC belum dikembalikan kepada Bank. Apabila mesin EDC sudah dikembalikan kepada Bank, maka sisa dana di Rekening Merchant akan dikembalikan kepada Merchant yang bersangkutan.

4. Para Pihak sepakat bahwa sehubungan dengan penempatan Peralatan Bank pada Merchant selama berlakunya Perjanjian dan atau mesin EDC belum dikembalikan kepada Bank, Merchant harus menyediakan sejumlah dana sebagai jaminan penempatan peralatan Bank.

5. Merchant wajib memastikan bahwa dalam Rekening Merchant harus terdapat saldo minimal dalam jumlah sebagaimana tercantum dalam Merchant Data Form dan besarnya saldo minimal dapat berubah sewaktu-waktu sesuai dengan ketentuan yang berlaku pada Bank dan setiap perubahan tersebut akan diberitahukan dan mengikat kepada Merchant. Ketentuan mengenai saldo minimal tersebut sepenuhnya tunduk pada ketentuan yang berlaku di Bank.

6. Bank akan melakukan pemasangan dan pemeliharaan terhadap Peralatan Bank dan Merchant wajib menempatkan Peralatan Bank pada tempat dan lokasi yang disetujui oleh Bank, serta EDC tidak dapat dipindahkan ke lokasi yang berbeda tanpa ada persetujuan dari Bank.

7. Merchant berkewajiban memelihara dan menjaga keamanan Peralatan Bank dalam kondisi apapun dan Merchant tidak diperkenankan untuk membongkar, memperbaiki, mengubah, menambah, melakukan pengrusakan atau mengurangi komponen-komponen pada Peralatan Bank. Apabila Merchant melanggar ketentuan tersebut, maka Merchant berkewajiban untuk membayar ganti rugi kepada Bank atas kerugian yang mungkin dialami Bank atas pelanggaran tersebut dengan jumlah yang akan ditetapkan oleh Bank. Apabila Merchant tidak memiliki itikad baik dalam melakukan pembayaran ganti rugi atas pelanggaran yang dilakukan oleh Merchant, maka Bank berhak untuk menonaktifkan Merchant dan melakukan pendebetan Rekening Merchant atau dengan cara-cara lainnya untuk penyelesaian masalah ganti rugi tersebut.

8. Bank akan memberikan pelatihan kepada Merchant dan/atau karyawan-karyawannya mengenai cara pengoperasian Peralatan Bank sesuai dengan jadwal yang disepakati oleh Para Pihak, dengan biaya sepenuhnya ditanggung oleh Bank. Merchant berkewajiban untuk memastikan bahwa Peralatan Bank hanya dioperasikan oleh Merchant dan/atau karyawan/pegawai Merchant sesuai dengan petunjuk pemakaian yang berlaku dan Merchant tidak diperkenankan menggunakan Peralatan Bank untuk kepentingan pihak lain atau untuk menerima transaksi dari merchant lain tanpa persetujuan tertulis terlebih dahulu dari Bank, kecuali untuk Transaksi Payment Point dan Transfer. Apabila penggunaan oleh pihak lain tersebut mengakibatkan kerugian bagi Merchant dan atau Pemegang Kartu Debet dan atau Bank dan atau bank penerbit Kartu Debet dan atau pihak lainnya, maka Merchant sepenuhnya bertanggung jawab atas setiap klaim, tuntutan dan atau ganti rugi yang mungkin timbul akibat kelalaian Merchant.

9. Merchant akan mengizinkan Bank setiap waktu untuk memeriksa keadaan dan/atau melakukan perawatan secara berkala terhadap Peralatan Bank yang ada di Merchant. Dalam hal ini, Merchant wajib memeriksa surat tugas dan meminta konfirmasi ke Bank mengenai keabsahan surat tugas tersebut yang dibawa oleh petugas pemeliharaan Bank. Pihak yang berwenang dari Merchant wajib menandatangani surat tugas yang dibawa petugas Bank setelah pemeriksaan/perbaikan selesai dilakukan.

10. Apabila Peralatan Bank tidak beroperasi sebagaimana mestinya, Merchant wajib melaporkan kepada Bank selambat-lambatnya pada tanggal yang sama pada saat peristiwa tersebut terjadi untuk dapat dilakukan pemeriksaan Peralatan Bank oleh petugas yang ditunjuk oleh Bank dan Bank akan segera melakukan perbaikan/penggantian terhadap Peralatan Bank yang tidak berfungsi setelah menerima laporan dari Merchant dan Merchant tidak diperkenankan untuk memperbaikinya sendiri. Segala kerugian yang timbul akibat tidak berfungsinya Peralatan Bank tersebut, baik langsung atau tidak langsung, sepenuhnya menjadi tanggung jawab Merchant.

11. Apabila diminta oleh Bank atau karena sesuatu hal Perjanjian berakhir, Peralatan Bank harus segera diserahkan kembali kepada Bank paling lambat 30 (tiga puluh) Hari Kerja. Dalam hal Merchant tidak bisa mengembalikan Peralatan Bank dalam kondisi baik dengan alasan apapun, maka Merchant berkewajiban membayar biaya penggantian Peralatan Bank dengan jumlah tertentu yang ditentukan oleh Bank. Apabila Merchant tidak memiliki itikad baik dalam melakukan pembayaran ganti rugi atas pelanggaran yang dilakukan oleh Merchant, maka Bank berhak untuk melakukan pendebetan Rekening Merchant atau dengan cara-cara lainnya untuk penyelesaian masalah ganti rugi tersebut termasuk mendebet dana jaminan penempatan Peralatan Bank menjadi pendapatan Bank.

12. Apabila Merchant melanggar salah satu atau beberapa ketentuan dalam pasal ini, maka Merchant berkewajiban untuk membayar ganti rugi kepada Bank setesar nilai kerugian yang mungkin dialami oleh Bank atas pelanggaran tersebut.

13. Merchant wajib mentaati setiap persyaratan dan ketentuan tentang penggunaan dan penempatan Peralatan Bank yang berlaku pada Bank. Bank berhak sewaktu-waktu mengubah persyaratan dan ketentuan mengenai penggunaan Peralatan Bank dengan pemberitahuan terlebih dahulu kepada Merchant dalam jangka waktu selambat-lambatnya 7 (tujuh) Hari Kerja sebelum perubahan tersebut berlaku efektif dan Merchant wajib mentaati setiap perubahan persyaratan dan ketentuan mengenai penggunaan, penempatan Peralatan Bank tersebut. Apabila Merchant keberatan atas perubahan yang ditetapkan oleh Bank, maka Merchant berhak untuk mengakhiri Perjanjian dengan terlebih dahulu memenuhi seluruh kewajibannya yang masih terhutang kepada Bank berdasarkan Perjanjian.

PASAL 14
DOKUMEN

1. Bank berhak untuk melakukan pemeriksaan terhadap Dokumen dan/atau salinan Dokumen yang disimpan oleh Merchant termasuk mengadakan inspeksi ke tempat Merchant.

2. Merchant wajib menyimpan seluruh bukti yang berkaitan dengan Transaksi Kartu Debet dan/atau Transaksi Payment Point sekurang-kurangnya 120 (seratus duapuluh) hari kalender terhitung dari tanggal transaksi.

3. Apabila terjadi Chargeback dari bank penerbit Kartu Debet, maka Merchant harus dapat menyediakan Slip Transaksi EDC yang layak (jelas/terbaca) dalam waktu paling lambat H+1 terhitung sejak Bank menghubungi Merchant dan meminta Merchant untuk memberikan Slip Transaksi EDC.

4. Slip Transaksi EDC akan digunakan sebagai salah satu alat bukti pelaksanaan Transaksi Kartu Debet dan/atau Transaksi Payment Point apabila dikemudian hari timbul permasalahan sehubungan dengan pelaksanaan Transaksi Kartu Debet dan/atau Transaksi Payment Point dan apabila diperlukan dari waktu ke waktu atas permintaan pertama dari Bank, maka Merchant harus memberikan dokumen tersebut untuk diperiksa kecenderannya oleh Bank.

5. Dalam jangka waktu yang disebut dalam pasal ini, atas permintaan pertama dari Bank, Merchant wajib menyerahkan Dokumen dan/atau salinan Dokumen kepada Bank selambat-lambatnya dalam waktu 1 (satu) Hari Kerja sejak tanggal permintaan Bank. Apabila Merchant tidak dapat menyerahkan Dokumen dan/atau salinan Dokumen kepada Bank, maka Merchant wajib bertanggung jawab sepenuhnya terhadap kerugian yang mungkin dialami Bank dan Merchant dengan ini membebaskan Bank dari segala tuntutan, gugatan dan/atau ganti rugi dari Pemegang Kartu Debet atau pihak manapun sehubungan dengan kelalaian Merchant dalam melaksanakan kewajibannya berdasarkan pasal ini.

PASAL 15
AUDIT DAN INSPEKSI

1. Bank berhak melakukan pemeriksaan atau audit baik secara internal maupun melalui pihak ketiga manapun yang ditunjuk oleh Bank terhadap layanan penerimaan Kartu Debet dan seluruh Peralatan Bank di Merchant pada waktu yang ditentukan oleh Bank, dengan ketentuan Bank akan memperlihatkan surat tugas resmi untuk melakukan pemeriksaan atau audit tersebut.

2. Merchant wajib membantu Bank dalam melakukan pemeriksaan atau audit dengan menyediakan data-data dan atau informasi yang diperlukan oleh Bank sehubungan dengan pelaksanaan Perjanjian.

PASAL 16
DAFTAR HITAM MERCHANT

Khusus untuk penerimaan dan pelaksanaan Transaksi Kartu Debet, Para Pihak sepakat untuk memberlakukan ketentuan mengenai Daftar Hitam Merchant, apabila selama pelaksanaan Perjanjian, Merchant tercantum dalam Daftar Hitam Merchant, maka atas permintaan dari Bank Perjanjian ini akan diakhiri dan selain itu juga Merchant wajib mengembalikan mesin EDC kepada Bank.

PASAL 17
PERNYATAAN DAN JAMINAN

1. Masing-masing pihak dengan ini menyatakan dan menjamin pihak lainnya dalam Perjanjian sebagai berikut:
   a. Masing-masing pihak adalah subyek hukum yang tunduk pada hukum negara Republik Indonesia dan pihak yang mewakili mempunyai hak penuh untuk menandatangani dan melaksanakan Perjanjian.
   b. Perjanjian tidak bertentangan dengan Anggaran Dasar masing-masing pihak (jika ada) serta tidak melanggar peraturan pemerintah yang wajib ditaati oleh masing-masing pihak di dalam menjalankan perusahaannya.
   c. Masing-masing pihak telah mengambil semua tindakan yang diperlukan sesuai dengan ketentuan Anggaran Dasar masing-masing pihak (jika ada) diantaranya mengenai kewenangan untuk melaksanakan Perjanjian dan subyek hukum yang menandatangani Perjanjian telah diberi wewenang untuk bertindak demikian untuk dan atas nama masing-masing pihak.

2. Merchant menyatakan dan menjamin akan menerima Transaksi Kartu Debet dan/atau Transaksi Payment Point dengan baik dan penuh tanggung jawab serta tidak melakukan tindakan yang bertentangan dengan hukum, undang-undang serta peraturan yang berlaku di wilayah Republik Indonesia.

3. Merchant menyatakan dan menjamin bahwa Transaksi Kartu Debet yang dilakukan dengan menggunakan Peralatan Bank dan Fasilitas Bank adalah merupakan Transaksi Kartu Debet yang tidak melanggar ketentuan perundang-undangan yang berlaku dan ketentuan mengenai penerimaan pelaksanaan Transaksi Kartu Debet sebagaimana diatur dalam Perjanjian. Dalam hal Bank menemukan indikasi pelaksanaan Transaksi Kartu Debet yang tidak sesuai dengan ketentuan mengenai penerimaan pelaksanaan Transaksi Kartu Debet yang diatur dalam Perjanjian, Bank mempunyai hak penuh untuk menonaktifkan EDC dan atau menarik mesin EDC yang ada pada Merchant, dan Merchant dengan ini membebaskan Bank dari segala klaim dan/atau tuntutan yang timbul sehubungan dengan penonaktifan EDC tersebut oleh Bank.

4. Merchant dengan ini membebaskan Bank dari segala klaim dan/atau tuntutan yang mungkin timbul dari pihak manapun juga sebagai akibat dari kelalaian atau kegagalan Merchant dalam menjalankan Transaksi Kartu Debet.

5. Merchant dengan ini menjamin Bank bahwa Merchant beserta dengan karyawannya dan/atau pihak lain yang bekerja sama dengan Merchant tidak akan memperbanyak dan/atau membuat memberikan, menyewakan, menjual, mengalihkan/gadaikan Peralatan Bank baik sebagian atau keseluruhan kepada pihak lain dengan alasan apapun termasuk menyalahgunakan untuk melakukan transaksi selain dari yang telah ditentukan dalam Perjanjian dengan maksud kejahatan/penipuan/kecurangan. Apabila Merchant melanggar ketentuan tersebut maka Merchant wajib mengganti segala kerugian, tuntutan dan/atau gugatan yang timbul akibat dari pelanggaran tersebut dan membebaskan Bank dari segala klaim dan/atau tuntutan dan/atau gugatan yang timbul dari pihak lain akibat pelanggaran tersebut.

PASAL 18
LARANGAN-LARANGAN

Tanpa mengurangi maksud dari ketentuan mengenai larangan-larangan yang terdapat dalam Perjanjian, maka Merchant dilarang untuk melakukan hal-hal sebagai berikut:

1. Merchant tidak diperbolehkan melakukan tindakan-tindakan yang dapat mengakibatkan kerugian bagi Bank dan atau yang bertentangan dengan Perjanjian ini dan peraturan perundang-undangan yang berlaku.

2. Merchant tidak diperbolehkan mengalihkan semua maupun sebagian haknya yang timbul berdasarkan Perjanjian tanpa persetujuan tertulis terlebih dahulu dari Bank. Setiap penyerahan atau pengalihan dari Perjanjian oleh Merchant tanpa persetujuan tertulis sebelumnya dari Bank, akan dianggap batal dan tidak berlaku.

3. Merchant tidak berhak meminta tambahan biaya/uang kepada Pemegang Kartu Debet atas layanan Transaksi Kartu Debet yang diterima oleh Merchant, kecuali tambahan biaya tersebut merupakan ongkos kirim, komisi dan sejenisnya. Khusus untuk Transaksi Payment Point, Merchant diperkenankan mengenakan sejumlah biaya transaksi tertentu kepada Pemegang Kartu Debet dan/atau Pelanggan Payment Point.

4. Merchant tidak diperkenankan menggunakan mesin EDC untuk transaksi penarikan uang tunai tanpa dilaksanakannya suatu transaksi penjualan barang/produk/jasa secara nyata dengan Pemegang Kartu Debet.

5. Apabila Merchant melanggar salah satu atau beberapa ketentuan dalam pasal ini, maka Merchant bertanggung jawab atas segala resiko yang timbul dan berkewajiban untuk membayar ganti rugi kepada Bank sebesar nilai kerugian yang mungkin dialami oleh Bank atas pelanggaran tersebut.

PASAL 19
KERAHASIAAN

Selama berlakunya Perjanjian dan pada setiap waktu sesudahnya, maka:

1. Setiap informasi dan/atau data yang diberikan oleh Bank kepada Merchant dan/atau karyawan Merchant dan/atau informasi dan/atau data yang diperoleh Merchant dan/atau karyawan Merchant sebagai pelaksanaan dari Perjanjian baik yang diberikan atau disampaikan secara lisan, tertulis, grafik atau yang disampaikan melalui media elektronik atau informasi dan/atau data dalam bentuk lainnya selama berlangsungnya pembicaraan atau selama pekerjaan lain antara Para Pihak adalah bersifat rahasia.

2. Merchant setuju dan sepakat bahwa setiap saat akan merahasiakan informasi dan/atau data yang diperoleh sebagai pelaksanaan dari Perjanjian kepada siapapun atau tidak akan menggunakannya untuk kepentingan Merchant atau kepentingan pihak tertentu, tanpa terlebih dahulu memperoleh persetujuan tertulis dari pejabat yang berwenang dari Bank atau pihak yang berwenang lainnya sesuai dengan ketentuan hukum yang berlaku.

3. Apabila Merchant dan/atau karyawan Merchant melanggar ketentuan sebagaimana dimaksud dalam ayat 1 dan ayat 2 Pasal ini, maka segala kerugian, tuntutan dan/atau gugatan yang dialami Bank merupakan tanggung jawab Merchant sepenuhnya, dan atas permintaan pertama dari Bank, Merchant akan menyelesaikannya sesuai dengan hukum dan perundang-undangan yang berlaku.

4. Kewajiban untuk menyimpan informasi dan/atau data sebagaimana dimaksud dalam ayat 1 dan 2 Pasal ini menjadi tidak berlaku, apabila:
   i. Informasi dan/atau data tersebut menjadi tersedia untuk masyarakat umum.
   ii. Informasi dan/atau data tersebut diperintahkan untuk dibuka untuk memenuhi perintah pengadilan.
   iii. Informasi dan/atau data tersebut diberikan sesuai ketentuan hukum yang berlaku.

PASAL 20
KELALAIAN

1. Bilamana terjadi atau timbul salah satu hal atau peristiwa yang ditetapkan dibawah ini akan merupakan suatu kejadian Kelalaian (Wanprestasi) terhadap Perjanjian:
   a) Kelalaian (Wanprestasi) Dalam Perjanjian.
      Apabila salah satu pihak lalai melaksanakan sesuatu kewajiban atau melanggar suatu ketentuan yang termaktub dalam Perjanjian.
   b) Pernyataan Tidak Benar.
      Bilamana ternyata bahwa suatu pernyataan atau jaminan yang diberikan oleh salah satu pihak kepada pihak lainnya dalam Perjanjian tidak benar atau tidak sesuai dengan kenyataannya
   c) Kepailitan.
      Bilamana Merchant oleh instansi yang berwenang dinyatakan berada dalam keadaan pailit atau diberikan penundaan membayar hutang-hutang (*surseance van betaling*).
   d) Permohonan Kepailitan.
      Bilamana Merchant mengajukan permohonan kepada instansi yang berwenang untuk dinyatakan pailit atau untuk diberikan penundaan membayar hutang-hutang (*surseance van betaling*) atau bilamana orang/pihak lain mengajukan permohonan kepada instansi yang berwenang agar Merchant dinyatakan dalam pailit.
   e) Terkena Sitaan.
      Apabila Merchant dikenakan suatu sitaan, baik sebagian maupun keseluruhan harta benda/kekayaannya.
2. Dalam hal terjadi suatu kejadian Kelalaian berdasarkan Perjanjian oleh salah satu pihak, maka pihak yang tidak lalai dapat memilih apakah tetap meneruskan atau menghentikan Perjanjian. Apabila pihak yang tidak lalai berkehendak untuk menghentikan Perjanjian, maka kehendak tersebut harus diberitahukan secara tertulis kepada pihak yang lalai sekurang-kurangnya 15 (lima belas) hari kalender sebelumnya, kecuali karena sebab dalam ayat 1 c Pasal ini, dimana pihak yang tidak lalai cukup memberitahukan kehendaknya dalam waktu yang wajar menurut pihak yang tidak lalai tersebut.
3. Dalam hal terjadi kejadian kelalaian sebagaimana dimaksud dalam ayat 1 pasal ini, maka Bank berhak dengan seketika menonaktifkan dan menarik Peralatan Bank tanpa harus melakukan pemberitahuan terlebih dahulu kepada Merchant.

PASAL 21
PEMBERITAHUAN DAN KORESPONDENSI

1. Setiap pemberitahuan dan/atau korespondensi yang wajib dan perlu dilakukan oleh masing-masing pihak dalam pelaksanaan Perjanjian harus dibuat secara tertulis dan diserahkan langsung atau dikirimkan melalui pos tercatat, rekening koran Merchant atau melalui faksimile dengan alamat sebagaimana yang tercantum dalam Merchant Data Form, kecuali untuk transaksi yang menurut Bank dimdikasikan sebagai transaksi mencurigakan, maka pemberitahuan ke Merchant akan disampaikan oleh Bank secara langsung atau melalui telepon.

2. Merchant wajib memberitahukan secara tertulis kepada Bank dalam hal terjadi perubahan susunan pengurus, direksi dan/atau komisaris pada Merchant dan/atau perubahan pemilik Merchant atau susunan dan jumlah kepemilikan pemegang saham pada Merchant selambat-lambatnya dalam waktu 14 (empat belas) hari kalender terhitung sejak tanggal efektifnya perubahan tersebut dengan disertai dokumen-dokumen atau akta perubahan pengurus/pemilik yang dibuat oleh/diterbitkan pejabat yang berwenang.

3. Pembatalan/perubahan alamat berlaku jika pembatalan/perubahan secara tertulis telah diterima oleh pihak lainnya dalam waktu 15 (lima belas) hari kerja sejak terjadinya pembatalan/perubahan tersebut sehingga segala akibat keterlambatan pemberitahuan menjadi tanggung jawab pihak yang melakukan perubahan tersebut.

4. Setiap pemberitahuan dan komunikasi ke alamat atau nomor faksimile tersebut di atas, dianggap telah diterima atau disampaikan :
   a. Pada hari yang sama apabila diserahkan langsung dan dibuktikan dengan tandatangan penerimaan pada buku pengantar surat (ekspedisi) atau tanda terima lain yang diterbitkan oleh pengirim.
   b. Pada hari ke-5 (lima), apabila dikirim per pos dan dibuktikan dengan resi pengiriman pos tercatat.
   c. Pada hari yang sama, apabila dikirim melalui faksimile dengan hasil yang baik.

PASAL 22
JANGKA WAKTU DAN PENGAKHIRAN PERJANJIAN

1. Perjanjian berlaku sejak tanggal ditandatangani Perjanjian oleh Para Pihak untuk jangka waktu 2 (dua) tahun, dan diperpanjang secara otomatis untuk jangka waktu yang sama, kecuali terdapat konfirmasi tertulis dari Bank bahwa Perjanjian tidak diperpanjang.

2. Tanpa mengesampingkan ketentuan lain dalam Perjanjian, apabila salah satu pihak menghendaki untuk mengakhiri Perjanjian, maka kehendak tersebut harus diberitahukan secara tertulis dan harus telah diterima oleh pihak lainnya dalam Perjanjian selambat-lambatnya 15 (lima belas) hari kalender sebelum tanggal pengakhiran Perjanjian yang dikehendaki tanpa diwajibkan untuk memberikan alasan-alasannya. Dalam hal pihak yang akan mengakhiri Perjanjian melakukan pengakhiran tanpa pemberitahuan atau dengan pemberitahuan yang waktunya kurang dari jangka waktu yang ditentukan, maka segala kerugian dan/atau tuntutan yang timbul sehubungan dengan pengakhiran Perjanjian menjadi tanggung jawab pihak yang mengakhiri Perjanjian sepenuhnya.

3. Apabila mesin EDC tidak digunakan untuk Transaksi Kartu Debet selama 3 (tiga) bulan berturut-turut, maka Bank berhak untuk mengakhiri Perjanjian dan melakukan penarikan mesin EDC secara seketika tanpa kewajiban untuk memberitahukan pengakhiran Perjanjian tersebut terlebih dahulu kepada Merchant.

4. Bank berhak untuk menonaktifkan Peralatan Bank tanpa pemberitahuan terlebih dahulu dan/atau persetujuan Merchant, semata-mata berdasarkan kebijakan internal Bank atau apabila menurut pertimbangan Bank bahwa Merchant telah melakukan Transaksi Kartu Debet dan/atau Transaksi Payment Point yang tidak sesuai atau melanggar ketentuan-ketentuan dalam Perjanjian dan atau peraturan perundang-undangan yang berlaku.

5. Jika pada saat Perjanjian berakhir/diakhiri masih terdapat kewajiban yang belum diselesaikan oleh masing-masing pihak, maka masing-masing Pihak akan tetap terikat sampai kewajiban tersebut diselesaikan.

6. Dengan berakhirnya Perjanjian tidak menghapuskan hak dan kewajiban masing-masing pihak yang timbul sebelum berakhirnya Perjanjian.

7. Untuk pengakhiran Perjanjian, Para Pihak sepakat untuk mengesampingkan Pasal 1266 Kitab Undang-Undang Hukum Perdata.

8. Dalam hal Perjanjian berakhir atau diakhiri, maka Merchant wajib mengembalikan seluruh Peralatan Bank.

9. Setelah Perjanjian berakhir, Merchant masih bertanggung jawab atas pelaksanaan Transaksi Kartu Debet yang dilakukan sampai dengan 18 (delapan belas) bulan sejak tanggal pelaksanaan Transaksi Kartu Debet terakhir.

10. Pada saat Perjanjian berakhir, Merchant wajib mengirimkan/menyerahkan Slip Transaksi EDC selama 120 (seratus dua puluh) hari kalender sebelum tanggal berakhirnya Perjanjian ke Bank.

PASAL 23
FORCE MAJEURE

1. Yang dimaksud dengan Force Majeure dalam Perjanjian adalah kejadian-kejadian yang terjadi diluar kemampuan dan kekuasaan Para Pihak sehingga mempengaruhi pelaksanaan Perjanjian antara lain:
   a. Gempa bumi, angin topan, banjir, tanah longsor, sambaran petir, kebakaran, dan bencana alam lainnya.
   b. Perang, huru-hara, terorisme, sabotase, embargo, dan pemogokan massal.
   c. Kebijaksanaan ekonomi dan Pemerintah yang mempengaruhi secara langsung terhadap pelaksanaan Perjanjian.

2. Dalam hal terjadi kejadian Force Majeure sebagaimana dimaksud di atas sehingga mempengaruhi pelaksanaan kewajiban salah satu pihak, maka pihak yang mengalami keadaan Force Majeure berkewajiban untuk memberitahukan secara tertulis/lisan kepada pihak lainnya dalam Perjanjian selambat-lambatnya 7 (tujuh) Hari Kerja terhitung sejak terjadinya keadaan Force Majeure tersebut untuk diselesaikan secara musyawarah.

3. Apabila pihak yang mengalami Force Majeure tersebut lalai untuk memberitahukan kepada pihak lainnya dalam kurun waktu sebagaimana dimaksud dalam ayat 2 pasal ini, maka seluruh kerugian, resiko dan konsekuensinya yang mungkin timbul menjadi beban dan tanggung jawab pihak yang mengalami Force Majeure tersebut.

4. Dalam hal Force Majeure terjadi secara terus menerus, maka pihak yang tidak mengalami Force Majeure dapat memilih apakah tetap meneruskan atau menghentikan Perjanjian. Apabila pihak yang tidak mengalami Force Majeure berkehendak untuk menghentikan Perjanjian, maka kehendak tersebut harus diberitahukan secara tertulis kepada pihak yang mengalami Force Majeure dalam waktu yang dianggap baik oleh pihak yang tidak mengalami Force Majeure.

PASAL 24
KUASA

1. Apabila dalam pelaksanaan Perjanjian membutuhkan kuasa khusus dari Merchant, maka kuasa tersebut dianggap telah diberikan oleh Merchant kepada Bank berdasarkan Perjanjian ini.

2. Kuasa-kuasa yang diberikan atau termaktub dalam Perjanjian tidak dapat ditarik kembali dan merupakan satu kesatuan serta menjadi bagian yang tidak terpisahkan dari Perjanjian, yang tidak dapat dicabut, tidak dapat dibatalkan dan tidak akan berakhir karena sebab atau peristiwa apapun juga sepanjang Merchant masih mempunyai kewajiban kepada Bank dan Para Pihak dengan ini melepaskan ketentuan-ketentuan Pasal 1813, 1814 dan 1815 Kitab Undang-Undang Hukum Perdata yang berlaku di Republik Indonesia.

PASAL 25
PENYELESAIAN PERSELISIHAN

1. Para Pihak sepakat untuk menyelesaikan setiap perselisihan yang timbul diantara Para Pihak sehubungan dengan pelaksanaan Perjanjian secara musyawarah untuk mencapai mufakat.

2. Apabila penyelesaian perselisihan secara musyawarah tersebut tdak mencapai mufakat, maka perselisihan tersebut akan diajukan ke pengadilan negeri.

PASAL 26
PILIHAN DAN DOMISILI HUKUM

1. Perjanjian dibuat, ditafsirkan dan diberlakukan berdasarkan hukum negara Republik Indonesia.

2. Segala urusan mengenai Perjanjian dengan segala akibatnya, Para Pihak telah sepakat untuk memilih tempat kediaman hukum yang umum dan tidak berubah pada Kantor Kepaniteraan Pengadilan Negeri di Kotamadya / Kabupaten yang sesuai dengan lokasi bisnis Merchant sesuai yang tercantum di dalam Merchant Data Form.

PASAL 27
PEMBATASAN KEBERLAKUAN

Merchant hanya tunduk dan terikat pada syarat dan ketentuan Perjanjian yang mengatur pelaksanaan transaksi yang dipilih oleh Merchant.

PASAL 28
KETENTUAN-KETENTUAN LAIN

1. Bank akan memberikan pelatihan (*training*) kepada karyawan/petugas yang ditunjuk oleh Merchant mengenai tata cara pelaksanaan Transaksi Kartu Debet dan Transaksi Payment Point dengan menggunakan Peralatan Bank sesuai dengan jadwal yang disepakati oleh Para Pihak.

2. Jika salah satu pihak diwajibkan untuk melaksanakan suatu kewajiban berdasarkan Perjanjian, maka pihak tersebut akan terbukti lalai melaksanakan kewajiban dengan lewatnya jangka waktu yang ditentukan, sehingga mengenai kelalaian itu tidak diperlukan teguran atau bukti berupa apapun dan dari siapapun.

3. Untuk hal-hal yang belum diatur dalam Perjanjian, maka akan berlaku seluruh ketentuan dalam Kitab Undang-Undang Hukum Perdata dan ketentuan Bank Indonesia serta ketentuan-ketentuan peraturan perundang-undangan lainnya yang terkait dengan Perjanjian.

4. Apabila sebagian dari ketentuan-ketentuan dalam Perjanjian bertentangan dengan peraturan perundang-undangan yang berlaku atau tidak dapat dilaksanakan karena ketentuan hukum, maka hal ini tidak mempengaruhi keabsahan dan pelaksanaan dari ketentuan-ketentuan lainnya dalam Perjanjian dan Para Pihak sepakat, dengan upaya terbaik, untuk mengganti ketentuan yang menjadi tidak berlaku, tidak sah atau tidak dapat dilaksanakan tersebut dengan ketentuan baru.

5. Dalam hal Para Pihak tidak dapat lagi melaksanakan Perjanjian, maka para penggantinya atau penerus haknya yang sah terikat pada semua syarat dan ketentuan yang tercantum dalam Perjanjian.

8. Perjanjian merupakan cakupan dari semua persetujuan antara Para Pihak, menggantikan semua penawaran, negosiasi, pengecualian-pengecualian dan kesepakatan-kesepakatan terdahulu baik yang dinyatakan secara lisan maupun tertulis.

7. Seluruh lampiran berikut perubahan dan/atau penggantinya yang ada di kemudian hari menjadi satu kesatuan dengan dan merupakan bagian yang tidak terpisahkan dari Perjanjian.

8. Seluruh pajak dan bea yang timbul sehubungan dengan pelaksanaan Perjanjian menjadi tanggung jawab dan merupakan beban Para Pihak sesuai dengan peraturan perpajakan yang berlaku.

9. Apabila Merchant melakukan tindakan-tindakan diluar ketentuan sebagaimana diatur dalam Perjanjian, maka segala tuntutan dan atau gugatan dan atau klaim yang diajukan pihak lain sehubungan dengan tindakan-tindakan yang dilakukan Merchant tersebut sepenuhnya menjadi tanggung jawab Merchant, dan dengan ini Merchant melepaskan Bank dari segala akibat yang disebabkan oleh kelalaian itu.

10. Para Pihak wajib mematuhi semua syarat-syarat yang dicantumkan di dalam Perjanjian. Kelalaian salah satu Pihak didalam memasti atau melaksanakan isi dari Perjanjian pada satu atau beberapa kali kejadian, tidak akan menghilangkan kewajiban Pihak dimaksud untuk tetap memenuhi segala persyaratan yang terdapat di dalam Perjanjian.

Demikian Perjanjian dibuat dan ditandatangani di _____ (20 scas), dalam rangkap 2 (dua) bermaterai cukup dan mempunyai kekuatan hukum yang sama serta dinyatakan mulai berlaku pada tanggal Perjanjian ini ditandatangani.

.....-.....-20.....

PT Bank Permata Tbk

Nama :_____
Jabatan

Merchant
.....

Meterai 6.000

Nama _____
Jabatan :

DAFTAR RIWAYAT HIDUP

I. DATA PRIBADI .

a. Nama Lengkap : **MUHAMMAD FIRMAN, SIK, MSi**

b. Pangkat / NRP : AKBP / 71040684.

c. Jabatan : Kasat Reskrim Polres Metropolitan Jakarta Pusat.

d. Tmpt/Tgl Lahir : Jakarta, 13 April 1971.

e. Agama : Islam.

f. Suku/Bangsa : Bugis/Indonesia.

g. Tempat TinggaL : Bintaro Puspita V-A / R-6 Bumi Bintaro Permai Jakarta Selatan.

II. KELUARGA.

a. Istri

Nama : Renny Setiawati.

Tmp/Tgl Lahir : Jakarta, 25 Februari 1971.

b. Anak

Nama : i. Muhammad Farhan Firman.

ii. Fara Bunga Firman.

iii. Fairouz Permata Firman.

III. PENDIDIKAN.

a. Umum

i. SDN Lagoa 04 PT. 1979 - 1985 di Jakarta.

ii. SMPN 10 1985 - 1988 di Ujung Pandang.

iii. SMAN 5 1988 - 1991 di Ujung Pandang.

b. Kepolisian

i. AKPOL ANGK.26 1991 - 1994 di Semarang.

ii. PTIK ANGK.37/DD 2000 - 2002 di Jakarta.

iii. SESPIMPOL ANGK.47 - 2008 di Lembang.

c. Kejuruan

i. PA DAS Serse 1995 di Megamendung.

ii. Kursus Resmob 1996 di Megamendung.

iii. PA LAN Serse EK 1999 di Megamendung.

iv. JUR BHS INGGRIS PUSBAHASA HANKAM 2000 di Jakarta.

v. Crime Scene Investigations (CSI) Course Session 2 ILEA - Bangkok 2005 di Bangkok - Thailand.

vi. Advance Management Course (AMC) ILEA - Rosswell 2006 di New Mexico - USA.

d. Penugasan Luar Negeri

i. Utusan Delegasi Polri Intellectual Property Right (IPR) Conference

Torronto - Canada 2007 di Canada.

ii. Utusan Delegasi Polri Intellectual Property Crimes - Law Enforcement Network Conference di Bangkok Thailand, 2009

IV. RIWAYAT KEPANGKATAN

a. Inspektur Dua Polisi Tmt 28 Juli 1994.

b. Inspektur Satu Polisi Tmt 1 Oktober 1997.

c. Ajun Komisaris Polisi Tmt 1 Januari 2001.

d. Komisaris Polisi Tmt 1 Juli 2005.

e. Ajun Komisaris Besar Polisi Tmt 1 JUli 2009.

V. RIWAYAT JABATAN

a. PAMAPTA POLRES METRO JAKARTA SELATAN, 1995 - 1996.

b. KANIT CURANMOR SAT SERSE POLRES METRO JAKARTA SELATAN, 1996 - 1997.

c. KANIT RES/INTEL POLSEK METRO TEBET, 1997 - 1998.

d. KANIT CURI SAT SERSE POLRES METRO JAKARTA SELATAN, 1998 - 1999.

e. WAKASAT SERSE POLRES METRO JAKARTA SELATAN,1999 - 2000.

f. MAHASISWA PTIK, 2000 - 2002.

g. PAMIN RENOPS BIRO OPS POLDA KALTIM, 2002 - 2003.

h. KAPOLSEKTA BALIKPAPAN BARAT POLRESTA BALIKPAPAN, 2003

i. KASAT RESKRIM POLRESTA BALIKPAPAN, 2003 - 2005.

j. KANIT III SAT III/TIPITER DIT RESKRIM POLDA KALTIM, 2005 - 2006.

k. Penyidik Muda Unit I Dit II / Eksus Bareskrim - Mabes Polri, 2006 - 2007.

l. Penyidik Madya Unit I (Indag) Dit II/Eksus Bareskrim - Mabes Polri, 2007 - 2008.

m. Penyidik Satgas BOM Polri, 2007 - sekarang.

n. PASIS SESPIM POL, 2008 - 2009.

o. Kasat II/Fismondev Dit.Krimsus Polda Metro Jaya, 2009 - 2010.

p. Ka Siaga "C" Biro Ops Polda Metro Jaya,2010 - 2011.

q. Kasat Reskrim Polres Metro Jakarta Pusat, 2011 - sekarang.

VI. TANDA JASA (PENGHARGAAN):

1. Piagam Penghargaan Kapolri berdasarkan Surat Keputusan Kapolri No. Pol.: Skep/357/III/2000, tgl.13 Maret 2000 atas prestasi :
" Pengungkapan dan Penangkapan pelaku jual beli senjata api/amunisi illegal dan Pengungkapan kasus pengedar Narkoba dengan 5 tersangka warga negara asing(Nigeria) di Kemayoran".

2. Satya Lencana Kesetiaan 8 tahun.

3. Satya Lencana Kesetiaan 16 tahun.

Jakarta, Juli 2011

Yang membuat

TTD

MUHAMMAD FIRMAN, SIK, MSi
AKBP NRP. 71040684