MANAJEMEN RISIKO TEKNOLOGI INFORMASI PERUSAHAAN MENGGUNAKAN FRAMEWORK RiskIT (STUDI KASUS: PEMBOBOLAN PT. BANK PERMATA, Tbk)

Iwan Iskandar
Jurusan Teknik Informatika Fakultas Sains dan Teknologi
Universitas Islam Negeri Sultan Syarif Kasim Riau
Email: iwaniskandar01@yahoo.com

ABSTRAK

Kasus pembobolan dana nasabah Bank Permata yang dilakukan oleh sekelompok cyber telah mengakibatkan kerugian hingga milyaran rupiah. Modus kejahatan ini dilakukan dengan cara mengacak TIN (*Telephone Identification Number*) dan mengambil data dari media EDC (*Electronic Delivery Channel*). Analisa terhadapaRisiko TI dilakukan dengan menerpakan Framework RiskIT yang bermanfaat untuk menekan seminimal mungkin risiko yang diakibatkan teknologi informasi. Pihak Bank Permata telah membentuk *Risk Control Owner* (RCO) yang bertanggung jawab dalam menentukan minimum kontrol standar dan menerapkan proses assurance untuk memastikan bahwa tujuan dari kontrol tersebut tercapai. Strategi TI dalam mendukung proses bisnis dapat dilihat dari inisiasi program dan aplikasi IT serta implementasi *Securty Plan* berupa *Security Event Log Management System* dan *Security Configuration Monitoring System* sebagai upaya dalam mencegah risiko pembobolan dana nasabah. Hasil yang diperoleh dari analisa risiko TI menggunakan RiskIT berupa perbaruan terhadap risiko TI melalui proses Identifikasi, Evaluasi dan Respon terhadap risiko yang ada.

Kata Kunci: EDC (*Electronic Delivery Channel*), Framework RiskIT, *Telephone Identification Number (TIN).*

ABSTRACT

Burglary case Permata Bank customer funds committed by a group of cyber has resulted in losses to billions rupiahs. Mode of the crime is done by randomizing TIN (Telephone Identification Number) and retrieve media data from the EDC (Electronic Delivery Channel). Analysis conducted by the IT terhadapaRisiko menerpakan RiskIT Framework is useful to reduce risks to a minimum due to information technology. The Bank has established a Risk Control Permata Owner (RCO) are responsible for determining the minimum standards and implement controls assurance process to ensure that the goals of such control is achieved. IT strategy in support of business processes can be seen from the initiation of programs and IT applications and the implementation of Plan Securty Security Event Log Management System Configuration and Security Monitoring System as an effort to prevent the risk of break-ins in customer funds. The results obtained from analysis of IT risk using the form RiskIT updates on IT risk through a process of identification, evaluation and response to risks.

Keywords*: EDC (Electronic Delivery Channel), RiskIT Framework, Telephone Identification Number (TIN).*

PENDAHULUAN

Dalam mencapai tujuan bisnisnya, setiap perusahaan, organisasi maupun perbankan selalu di dukung oleh teknologi informasi yang berkualitas terutama dalam mengoptimalkan proses bisnisnya. IT sangat penting dalam mempermudah dan mempercepat aktivitas kerja bisnis sehingga menghasilkan bisnis yang optimal dan efisien. Penerapan IT sebagai pendukung proses bisnis harus sesuai dengan tujuan yang ingin dicapai. Jika penerapan IT tersebut tidak sesuai maka akan menimbulkan risiko terutama jika teknologi IT disalahgunakan.

Risiko yang ditimbulkan akibat kesalahan penerapan IT dapat merugikan proses bisnis seperti kerugian finansial, fraud yang dilakukan oleh pihak internal, timbulnya ketidakpercayaan pelanggan, menurunnya reputasi perushaan dan lain sebagianya. Oleh sebab itu, diperlukan manajemen atau pengelolaan dan pengukuran terhadap risiko IT. Pengukuran ini dilakukan untuk mengetahui profil resiko TI, analisa terhadap resiko, kemudian melakukan respon terhadap resiko tersebut sehingga tidak terjadi

dampak-dampak yang dapat ditimbulkan oleh resiko tersebut.

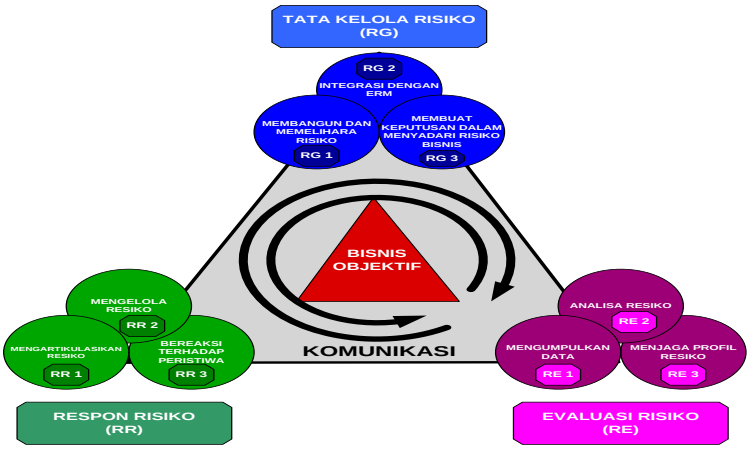
Terdapat beberapa metode atau framework yang bisa dijadikan sebagai best practice dalam penerapan risiko IT. Dalam penelitian ini akan dibahas risiko IT pada Bank Permata menggunakan Framework RiskIT.

Konsep Framework RiskIT

Risk IT adalah suatu framework yang didasarkan pada seperangkat prinsip-prinsip penuntun untuk pengelolaan yang efektif dari risk IT. Framework RiskIT merupakan pelengkap COBIT yakni suatu framework komprehensif untuk tata kelola dan pengendalian usaha solusi berbasis IT dan layanan. Sedangkan COBIT menyediakan satu set kontrol untuk mengurangi resiko IT, RiskIT menyediakan suatu framework bagi perusahaan untuk mengidentifikasi, mengatur, dan mengelola resiko IT.

Pada gambar 1 memperlihatkan 3 domain dalam *RiskIT* yakni Tata Kelola Risiko (*Risk Governance-RG*), Evaluasi Risiko (*Risk Evaluation-RE*), dan Respon Risiko (*Risk Response-RS*). Masing-masing domain terdapat tujuan yang harus dicapai, dan dibagi dalam beberapa sasaran proses serta aktivitas yang dilakukan untuk mencapainya. Dalam definisi RiskIT, risiko IT disorot sebagai risiko bisnis.

Risiko lain yang termasuk perusahaan menghadapi risiko strategis, risiko lingkungan, risiko pasar, risiko kredit, risiko operasional dan risiko kepatuhan. Di banyak perusahaan, TI terkait resiko dianggap sebagai komponen risiko operasional, misalnya,dalam industri keuangan dalam kerangka kerja Basel II. Namun, bahkan risiko strategis dapat memiliki komponen TI untuk itu, terutama di mana TI adalah enabler kunci inisiatif bisnis baru. Hal yang sama berlaku untuk risiko kredit, mana yang buruk TI (keamanan) dapat mengakibatkan penurunan peringkat kredit.



Gambar 1. Framework *RiskIT* (Risk IT, 2009)

Tabel 1. Domain RiskIT (Risk IT, 2009)

DOMAIN	TUJUAN	KODE	SASARAN PROSES	KODE	AKTIVITAS
Tata Kelola Resiko / **Risk Governance (RG)**	Pastikan bahwa praktek manajemen risiko TI tertanam dalam perusahaan, memungkinkan perusahaan untuk mengamankan	RG1	**Membangun dan mempertahankan pandangan risiko umum** -Memastikan bahwa kegiatan manajemen risiko menyelaraskan dengan kapasitas tujuan perusahaan untuk TI, terkait kerugian dan	RG1.1	Lakukan penilaian risiko perusahaan IT.
				RG1.2	Mengusulkan TI batas risiko toleransi..
				RG1.3	Menyetujui TI toleransi risiko.
				RG1.4	Menyelaraskan kebijakan risiko TI.
				RG1.5	Promosikan risiko IT-sadar budaya.

	risiko yang optimal untuk disesuaikan kembali.		toleransi subjektif ledership.	RG1.6	Mendorong komunikasi yang efektif dari risiko IT.
		RG2	**Integrasikan dengan ERM** - Mengintegrasikan strategi dan operasi risiko TI dengan keputusan risiko bisnis strategis yang telah dibuat di tingkat perusahaan.	RG2.1	Membangun dan memelihara akuntabilitas untuk IT manajemen risiko.
				RG2.2	Koordinat risiko IT strategi dan strategi bisnis risiko.
				RG2.3	Beradaptasi risiko TI praktek untuk praktek risiko perusahaan.
				RG2.4	Menyediakan sumber daya yang memadai untuk manajemen risiko TI.
				RG2.5	Memberikan jaminan independen terhadap manajemen risiko TI.
		RG3	**Membuat menyadari risiko keputusan bisnis** - Pastikan bahwa keputusan perusahaan mempertimbangkan berbagai peluang dan konsekuensi dari ketergantungan pada TI untuk sukses.	RG3.1	Keuntungan manajemen buy-in untuk pendekatan analisis risiko TI.
				RG3.2	Menyetujui TI analisis risiko.
				RG3.3	Embed risiko TI pertimbangan dalam pengambilan keputusan bisnis strategis.
				RG3.4	Menerima risiko TI.
				RG3.5	Memprioritaskan kegiatan respon IT Risk.
Evaluasi Risiko / **Risk Evaluation (RE)**	Pastikan bahwa TI terkait risiko dan peluang yang diidentifikasi, dianalisis dan disajikan dalam istilah bisnis.	RE1	**Mengumpulkan Data** - Mengidentifikasi data yang relevan untuk memungkinkan efektif terkait TI identifikasi risiko, analisis dan pelaporan.	RE1.1	Membangun dan mempertahankan model untuk pengumpulan data.
				RE1.2	Mengumpulkan data pada lingkungan operasi.
				RE1.3	Kumpulkan data tentang peristiwa risiko.
				RE1.4	Mengidentifikasi faktor risiko.
		RE2	**Menganalisa Risiko** - Mengembangkan informasi yang berguna untuk mendukung keputusan risiko yang memperhitungkan relevansi bisnis faktor risiko.	RE2.1	Tentukan lingkup TI analisis risiko.
				RE2.2	Perkiraan risiko TI.
				RE2.3	Mengidentifikasi opsi-opsi risiko respon.
				RE2.4	Melakukan peer review TI analisis risiko.
		RE3	**Menjaga Profil Risiko** - Menjaga up-to-date dan persediaan lengkap risiko yang dikenal dan atribut (misalnya, requency diharapkan, dampak potensial, disposisi), sumber daya TI, kemampuan dan kontrol seperti yang dipahami dalam konteks produk bisnis, layanan	RE3.1	Pemetaan sumber daya TI untuk proses bisnis.
				RE3.2	Tentukan kekritisan bisnis sumber daya TI.
				RE3.3	Memahami kemampuan IT.
				RE3.4	Perbarui risiko IT komponen skenario.
				RE3.5	Menjaga risiko TI mendaftar dan peta risiko TI.
				RE3.6	Mengembangkan indikator risiko TI.

			dan proses.		
Respon Risiko / **Risk Response (RR)**	Pastikan bahwa isu-isu risiko terkait TI, kesempatan dan peristiwa ditangani dengan biaya-efektif dan sejalan dengan prioritas bisnis	RR1	**Mengartikulasikan Risiko** - Pastikan bahwa informasi tentang keadaan sebenarnya dari eksposur yang berkaitan dengan IT dan kesempatan yang tersedia pada waktu yang tepat dan kepada orang yang tepat untuk respon yang tepat.	RR1.1	Komunikasikan hasil analisis risiko TI.
				RR1.2	Laporan kegiatan manajemen risiko TI dan negara kepatuhan.
				RR1.3	Menafsirkan temuan penilaian independen TI.
				RR1.4	Mengidentifikasi peluang yang berkaitan dengan IT.
		RR2	**Mengelola Risiko** - Memastikan bahwa langkah-langkah untuk menangkap peluang strategis dan mengurangi risiko ke tingkat yang dapat diterima dikelola sebagai portofolio.	RR2.1	Persediaan kontrol.
				RR2.2	Memantau keselarasan operasional dengan batas toleransi risiko.
				RR2.3	Menanggapi eksposur risiko ditemukan dan kesempatan.
				RR2.4	Melaksanakan kontrol.
				RR2.5	Laporan risiko IT kemajuan rencana aksi.
		RR3	**Bereaksi Terhadap Peristiwa** - Memastikan bahwa langkah-langkah untuk menangkap peluang segera atau membatasi besarnya kerugian dari peristiwa yang berkaitan dengan IT diaktifkan secara tepat waktu dan efektif.	RR3.1	Menjaga rencana respon insiden.
				RR3.2	Memonitor risiko TI.
				RR3.3	Memulai respon insiden.
				RR3.4	Berkomunikasi pelajaran dari risiko kejadian.

Manajemen Risiko pada Bank Permata, Tbk

Profil Bank Permata

PT Bank Permata Tbk (Bank Permata) merupakan hasil merger 5 (lima) bank pada tahun 2002. Bank-bank tersebut yakni PT. Bank Bali Tbk, PT. Bank Universal Tbk, PT. Bank Artamedia, PT. Bank Patriot dan PT. Bank Prima Ekspress. Di tahun 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 saham utama ini meningkat menjadi 89,01% pada tahun 2006. Saat ini Bank Permata telah berkembang menjadi bank swasta utama yang menawarkan produk dan jasa inovatif serta komprehensif terutama disisi *delivery channel*-nya termasuk *Internet Banking* dan *Mobile Banking*. Bank Permata kini telah melayani sekitar 1,9 juta nasabah di 55 kota di Indonesia dengan 278 cabang (termaksuk 10 cabang Syariah) dan 631 ATM serta akses tambahan di lebih dari 40.000 ATM (VisaPlus, Visa Electron, MC, Alto, ATM Bersama dan ATM Prima)

Visi dan Brand Promise Bank Permata

Berikut visi dan *brand promise* bank Permata:

Visi:

Pelopor dalam memberikan solusi finansial yang inovatif.

Brand Promise:

Menjadikan hidup lebih bernilai (Mewujudkan *brand promise* di kehidupan

sehari-hari dengan menjalankan nilai-nilai perusahaan dalam bekerja, bersikap, serta berperilaku terhadap *customer*, rekan kerja, komunitas, investor, dan regulator).

Layanan

Bank Permata memiliki beberapa layanan yang menggunakan teknologi informasi seperti E-Banking yang memiliki beberapa fasilitas yang ditawarkan kepada nasabah seperti:

1. PermataNet
   PermataNet merupakan layanan Internet Banking untuk melayani nasabah dalam memenuhi kebutuhan perbankan secara aman, mudah, real time dan leluasa, bisa diakses tanpa dibatasi tempat dan waktu. Untuk dapat menggunakan layanan PermataNet dibutuhkan Mobile Token yang digunakan sebagai alat otentikasi.
2. PermataMobile
   Dengan permata mobile nasabah dapat melakukan transaksi mobile banking berbasis sms untuk berbagai transaksi secara online.
3. PermataTel
   Fasilitas ini diberikan untuk transaksi melalui media telepon. Nasabah wajib memiliki ***TIN (Telephone Identification Number)*** sebagai nomor identifikasi bagi setiap transaksi yang akan dilakukan.
4. PermataATM
   Fasilitas Mobile Cash yang merupakan layanan penarikan uang melalui mesin ATM tanpa kartu. Prosesnya adalah dengan mengirimkan sms yang kemudian nasabah akan mendapatkan passcode berupa 10 angka kode rahasia yang digunakan pada mesin ATM.

Proses Bisnis PT. Bank Permata

Bank Permata memiliki proses bisnis yang unggul dalam mencapai tujuan dan kompetisi terhadap perbankan pada saat ini.

Strategi Bisnis

Bank Permata memelihara komitmennya untuk menjadi penyedia jasa keuangan terkemuka di Indonesia. Oleh karena itu upaya menyeluruh dilakukan untuk memastikan terciptanya layanan berkualitas prima bagi para nasabah melalui jaringan distribusi yang luas, kemampuan perbankan elektronik yang kuat dan sumber daya manusia yang berkualitas. Mulai tahun 2010 Bank Permata meluncurkan program beragam produk dan layanan. Program ini sangat sukses terutama dalam menghimpun tabungan dan giro. Sementara itu inisiatif untuk meningkatkan kemampuan di bidang manajemen risiko, tata kelola perusahaan yang baik, sumber daya manusia, layanan dan operational excellence juga dilakukan untuk menciptakan bisnis yang berkelanjutan bagi Bank Permata.

Dalam mengembangkan bisnisnya di tahun 2011, Bank Permata secara konsisten memfokuskan target pasarnya pada segmen consumer dan commercial. Untuk sektor consumer, Bank Permata akan fokus kepada *segmen mass* dan *mass affluent* dengan pendekatan terpadu (*customer-centric*) dengan penekanan pada adanya penjualan silang (*cross selling*) guna meningkatkan loyalitas nasabah terhadap Bank Permata. Untuk sektor commercial, Bank Permata akan fokus kepada industri yang unggul, melalui implementasi *value chain* dan pendekatan total relationship guna melayani kebutuhan nasabah secara terpadu [4]. Hal ini akan memberikan dampak pada pertumbuhan kredit maupun *fee based income* kepada segmen consumer dan commercial.

Strategi IT dalam mendukung Proses Bisnis Perusahaan

Peran TI dalam proses bisnis merupakan tools utama bagi perusahaan untuk menaikkan daya saing sekaligus meningkatkan layanan bagi nasabah maupun non nasabah Bank Permata dalam proses transaksi. Manajemen Bank Permata telah mengembangkan TI secara bertahap. Dimulai dengan *Retail Banking* (1993), manajemen secara berturut-turut lalu memutuskan untuk mengimplementasikan di divisi *Finance* (1992), *Wholesale Banking* (1993), *Human Resource* (2002) dan *Risk Management* (2005).

Inisiasi Program dan Aplikasi

Setelah mengimplementasikan TI kemudian Bank Permata melakukan inisiasi

beberapa program dan aplikasi, diantaranya adalah

1. *Global Customer Network* (GCG)
   GCG bermanfaat untuk mengonsolidasikan informasi tentang nasabah melalui *data warehouse*. GCG mampu menghasilkan *uniform clazsification report* atau kesamaan laporan untuk kebutuhan Laporan Bank Umum (LBU) dan Sistem Informasi Debitur (SID). Aplikasi ini digunakan untuk analisis profitabilitas yang dibutuhkan unit-unit bisnis perusahaan dalam menganalisis per nasabah, per produk, per unit yang kemudian menjadi dasar dalam pengambilan keputusan bisnis.
2. *Electronic Delivery Channel* (EDC)
   Fitur yang diberikan yang lengkap diantaranya PermataMobile, PermataNet, PermataMini ATM, dan Permata Tel. Respon nasabah tehadap fasilitas EDC relatif baik. Rata-rata peningkatan transaksi melalui EDC meningkat sekitar 50%. Pengembangan fitur *Internet Banking* dan *Bulk Transfer Online* ke rekening bank lain menjadi salah satu bukti komitmen manajemen memberikan layanan prima kepada nasabah non Bank Permata.

Implementasi dan Pembaharuan TI

Selama tahun 2010, beberapa proyek IT yang signifikan telah diimplementasikan untuk mendukung perkembangan bisnis dan peningkatan pelayanan, berkaitan dengan perbaikan sistem dan peningkatan infrastruktur IT. Berikut sistem TI yang telah diimplementasikan tersebut:

1. **Pembaharuan PC dan Server**
   Melakukan penggantian kurang lebih 5.000 PC berumur di atas 5 tahun dengan PC baru yang memiki spesifikasi lebih baik.
2. **Implementasi *Electronic Trading System (ET)***
   Tujuannya adalah untuk meningkatkan efisensi proses, dimana distribusi nilai tukar valuta asing dan pemrosesan antara cabang dan bagian *Treasury* dilakukan secara otomasi.
3. **Implementasi *Joint Financing System***
   Sistem JF yang baru ini menggunakan platform AS/400 yang dapat menggantikan beberapa proses manual dan meningkatkan secara signifikan kapasitas untuk pemrosesan, rekonsiliasi dan pelaporan.
4. **Implementasi *Fund Accounting and Custody System***
   Melakukan pembaharuan terhadap sistem bisnis Kustodian dan Fund Administration untuk mengurangi proses manual, mampu menyediakan laporan manajemen informasi yang lebih baik dan penyempurnaan proses rekonsiliasi.
5. **Implementasi *Consumer Lending Risk Assessment***
   Untuk mendukung pertumbuhan *Consumer Lending* maka diimplementasikan sistem otomasi meningkatkan proses penilaian risiko pada aplikasi tersebut. Otomatisasi ini mempercepat pemeriksaan permohonan kredit tanpa menghilangkan akurasi pemeriksaan.
6. **Peluncuran Program e-Learning iSafe untuk Keamanan Informasi (*Information Security*)**
   Merupakan program belajar bagi karyawan untuk meningkatkan budaya manajemen risiko berkelas dunia.
7. **User-Id Review**
   Tujuan dari peninjauan User ID adalah untuk memastikan bahwa kewenangan akses ke sistem hanya diberikan kepada karyawan sesuai dengan tugas dan tanggung jawab mereka tanpa benturan kepentingan dalam pelaksanaannya.
8. **Implementasi Otomasi LHBU (Laporan Harian Bank Umum)**
   Untuk mempercepat proses pelaporan ke Bank Indonesia dan memenuhi peraturan, telah diimplementasikan program Otomasi LHBU (Laporan Harian Bank Umum) di unit Global Market Operations (GMO).

Fokus Core IT Bank Permata dalam Pencapaian Peningkatan Pendapatan/thn

Untuk periode tahun 2008 – 2009, implementasi TI di Bank Permata berfokus pada *Internet Corporate Banking* dan

beberapa produk dengan karakteristik *High Level Requirement* seperti transfer antar bank. Kontribusi TI pada Bank Permata bisa dilihat dari segmen *middle market* dimana terjadi peningkatan pengelolaan dana pihak ketiga sebesar 181% menjadi 2,8 triliun rupiah pada tahun 2008 (Annual Report, 2008). Sedangkan pada segmen *financial institusion* terjadi peningkatan aset dari 1,8 triliun rupiah pada tahun 2007 menjadi 2,8 triliun rupiah pada tahun 2008 (Annual Report, 2008; Annual Report, 2007). PT. Bank Permata, Tbk., misalnya, per kuartal III/2009 membukukan laba bersih 500 miliar rupiah, melaju 28% dibanding periode yang sama tahun sebelumnya (Annual Report, 2009). Per kuartal III/2009 total pendapatan Bank Permata mencapai 2,8 triliun rupiah naik 19% dibanding periode yang sama tahun sebelumnya yang mencapai 2,3 triliun rupiah. Sedangkan pendapatan bunga bersih sebesar 2,1 triliun rupiah melaju 14 % dibanding periode yang sama tahun sebelumnya. Pendapatan operasional lainnya tumbuh 40% dari 453 miliar rupiah menjadi 634 miliar rupiah. Rasio beban operasi terhadap pendapatan operasi tercatat sebesar 84,8% di tahun 2010 menurun dari 89,2% di tahun 2009.

Manajemen Risiko yang telah ada (*Existing*)

Saat ini Bank Permata telah memiki manajemen risiko yang telah dibuat dan dikelola secara efektif. Hal ini terlihat dari berbagai upaya yang telah dilakukan oleh pihak bank dalam menanggulangi dan meminimalisir tingkat resiko yang dialami.

Kerangka Manajemen Risiko Dalam Penggunaan TI pada Bank Umum yang diterbitkan oleh Bank Indonesia

Penggunaan TI bertujuan meningkatkan kecepatan dan keakuratan transaksi serta pelayanan kepada nasabah. Namun pada implementasinya juga menimbulkan tingkat resiko yang tinggi seperti risiko operasional, reputasi, legal, kepatuhan dan strategis. Oleh karena itu setiap bank harus memiliki manajemen risiko yang terpadu untuk melakukan identifikasi, pengukuran, pemantauan dan pengendalian risiko.

Bank Indonesia sebagai bank pengawas telah membuat aturan manajemen risiko penggunaan TI pada bank umum. Aturan ini wajib diterapkan pada setiap bank yang kemudian dapat disesuaikan parameter-parameter risiko terhadap aktivitas bisnis masing-masing bank. Berikut peraturan yang diterbitkan oleh Bank Indonesia melalui Surat Edaran Bank Indonesia Nomor: 9/30/DPNP Tanggal 12 Desember 2007 (PBI, 2009; BI, 2007), yakni:

A. Laporan Penggunaan Teknologi Informasi

1. Manajemen TI
2. Aplikasi dan Pengembangan
3. Operasional Teknologi Informasi
4. Jaringan Komunikasi
5. Pengamanan Informasi
6. *Business Continuity Plan*
7. *End User Computing*
8. *Electronic Banking*
9. Audit Teknologi Informasi (Audit TI)
10. Penyelenggaraan TI oleh Pihak Lain

B. Rencana Perubahan Mendasar Dalam Penggunaan Teknologi Informasi

1. Rencana Penerbitan *Electronic Banking* Transaksional
2. Rencana Penyelenggaraan *Data Center* dan atau *Disaster Recovery Center* oleh Pihak Lain di Dalam Negeri
3. Rencana Penyelenggaraan *Data Center* dan atau *Disaster Recovery Center* oleh Pihak Lain di Luar Negeri
4. Rencana Penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi oleh Pihak Lain di Dalam Negeri
5. Rencana Penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi oleh Pihak Lain di Luar Negeri

C. Laporan Realisasi Perubahan Mendasar Dalam Penggunaan Teknologi Informasi

1. Realisasi Penerbitan Electronic Banking Transaksional.
2. Realisasi Penyelenggaraan *Data Center* dan atau *Disaster Recovery Center* oleh Pihak Lain di Dalam Negeri
3. Realisasi Penyelenggaraan *Data Center* dan *Disaster Recovery Center* oleh Pihak Lain di Luar Negeri
4. Realisasi Penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi oleh Pihak Lain di Dalam Negeri

5. Realisasi Penyelenggaraan Pemrosesan Transaksi Berbasis Teknologi Informasi oleh Pihak Lain di Luar Negeri

D. Laporan Tahunan Penggunaan Teknologi Informasi

1. Laporan Kejadian Kritis, Penyalahgunaan dan/atau Kejahatan dalam Penyelenggaraan Teknologi Informasi (TI)
2. Permohonan Persetujuan Ulang Penyelenggaraan *Data Center* Dan Atau *Disaster Recovery Center* oleh Pihak Lain di Luar Negeri bagi Kantor Cabang Bank Asing

Kerangka Kerja Manajemen Risiko yang telah diterapkan oleh Bank Permata

Kerangka Kerja Manajemen Risiko/ *Risk Management Framework* (RMF) Bank Permata menetapkan pendekatan terhadap manajemen risiko dan kerangka kontrol dimana risiko dikelola dan diperolehnya keseimbangan antara risiko dan pendapatan. RMF mengidentifikasi berbagai jenis risiko yang berbeda yang dihadapi Bank, masing-masing risiko dikelola oleh seorang *Risk Control Owner* (RCO). Setiap RCO bertanggung jawab dalam menentukan minimum kontrol standar dan menerapkan proses assurance untuk memastikan bahwa tujuan dari kontrol tersebut telah dicapai.

Bank Permata menggunakan berbagai tipe risiko sebagai alat bantu untuk mengidentifikasi risiko secara konsisten dan komprehensif, dimanapun risiko tersebut muncul. Bank telah mengidentifikasi 2 Tipe Risiko, yakni:

1. Non Operasional, seperti Kredit, Pasar, Likuiditas, Negara, Modal, Reputasi, Strategi, Pensiun
2. Operasional, seperti: *People Management, Technology Management, Vendor Management, Property Management, Security Management, Regulatory Compliance, Legal Processes, Accounting and Financial Control, Tax Management and Corporate Authorities and Structure*.

Direksi Bank Permata telah membentuk RMC dan ALCO untuk melaksanaan fungsi manajemen risiko. RMC menetapkan strategi, kebijakan dan prosedur manajemen risiko, memantau implementasinya, mengembangkan budaya pengelolaan risiko dan memastikan sumber daya yang memadai telah dikembangkan untuk memastikan pengelolaan risiko. ALCO bertanggung jawab untuk mengelola modal dan menetapkan kebijakan terkait dengan pengelolaan neraca dan kepatuhan terhadapnya. Termasuk di dalamnya manajemen likuiditas Bank Permata, kecukupan modal dan risiko nilai tukar mata uang asing dan suku bunga. Berikut pengelolaan risiko-risiko yang ada:

1. Risiko Kredit

Fokusnya adalah pada pemisahan fungsi risiko dan fungsi pengembangan bisnis dalam memproses persetujuan kredit untuk setiap segmen usaha. Hal ini menjamin kemandirian fungsi risiko dari fungsi originationdan penjualan.

2. Risiko Pasar

Bank Permata mengukur risiko potensi kerugian yang dapat dihasilkan dari kemungkinan terjadinya pergerakan yang kurang menguntungkan dalam suku bunga, harga dan volatilitas pasar dengan menggunakan metodologi VaR.

3. Risiko Likuiditas

Bank Permata mengelola risiko likuiditasnya baik dalam jangka pendek maupun jangka menengah. Pengelolaan risiko likuiditas berfokus untuk menjaga agar struktur neraca tetap sehat.

4. Risiko Negara (Lintas Batas)

Risiko negara tergantung pada limit risiko negara yang berlaku yang berasal dari pinjaman yang diberikan, simpanan berbunga pada bank lain, trade dan tagihan lainnya, aksep, sertifikat deposito dan surat kredit dan surat berharga lainnya dimana nasabah adalah penduduk di negara selain Indonesia.

5. Risiko Permodalan

Untuk menjaga tingkat kecukupan modal diatas ketentuan Bank Indonesia.

6. Risiko Strategis

Risiko strategis adalah potensi kemungkinan kerugian karena kegagalan untuk mengoptimalkan potensi pendapatan dari Bank Permata.

7. Risiko Pensiun
Bank Permata mempunyai kewajiban untuk membayarkan manfaat pensiun kepada karyawan yang telah mencapai usia pensiun.

8. Risiko Operasional
Pada *Risk Management Framework* (RMF) risiko operasional dikategorikan menjadi 10 Risk Control Area: *People Management, Technology Management, Vendor Management, Property Management, Security Management, Regulatory Management, Regulatory Compliance, Legal Processes, Accounting and Financial Control, Tax Management and Corporate Authorities & Structure.*

9. Risiko Kepatuhan
Risiko Kepatuhan pada Bank Permata dikelola oleh Direktorat Compliance, yang bertanggung jawab untuk menetapkan dan mempertahankan kerangka kerja sesuai kebijakan kepatuhan regulasi dan prosedur.

Risiko-risiko diatas merupakan bentuk manajemen risiko yang ada (*existing*) yang telah dibuat oleh manajemen Bank Permata berdasarkan **Peraturan Bank Indonesia PBI No. 11/19/PBI 2009 Tertanggal 4 Juni 2009 tentang Sertifikasi Manajemen Risiko Bagi Pengurus dan Pejabat Bank Umum** (PBI, 2009; BI, 2007). Untuk risiko teknologi informasi dikategorikan kedalam risiko operasional.

Kerangka Kerja Manajemen Risiko TI Bank Permata

Manajemen risiko TI digolongkan pada Risiko Operasional. Bank Permata telah membentuk Komite Pengarah TI .

Manajemen Risiko TI

Untuk menjalankan manajemen risiko TI, Bank Permata telah membentuk sebuah **Komite Pengarah TI** yang bertugas untuk memberikan rekomendasi kepada Direksi tentang:

1. Penyelarasan Rencana Strategis Teknologi Informasi dengan Rencana strategis Bisnis Bank
2. Relevansi Proyek IT dalam kaitannya dengan Rencana Strategis IT
3. Kepatuhan Implementasi Proyek IT yang sesuai dengan Project Charter
4. Kesesuaian IT untuk memenuhi kebutuhan Manajemen Sistem Informasi Bank dan kebutuhan Operasional
5. Langkah-langkah untuk meminimalkan risiko investasi IT untuk memastikan bahwa investasi ini memenuhi kebutuhan bisnis
6. Kinerja IT dan cara-cara untuk meningkatkannya
7. Mengelola isu-isu terkait IT, yang tidak dapat diselesaikan secara efektif dan efisien, tepat waktu oleh satu bagian
8. Prioritas investasi yang terkait IT

Susunan Anggota Komite Pengarah Teknologi Informasi:

1. Direktur Teknologi dan Operasi (Ketua)
2. Direktur Risiko (Ketua Pengganti)
3. Direktur Wholesale Banking
4. Direktur Retail Banking
5. Direktur Keuangan
6. Head, Operations
7. Head, Network
8. Head, Information Technology (Sekretaris)

Penerapan Sistem TI untuk Meminimalisir Tingkat Risiko

Berikut sistem yang telah diimplementasikan:

1. Switching System

Sistem Switching yang baru (Base 24) ini akan mampu memproses kartu Euro Master Visa (EMV) yang telah diimplementasikan oleh jaringan kartu elektronik untuk meminimalkan risiko penipuan.

2. *Internet Banking* (PermataNet)

Pengguna Internet di Indonesia tumbuh dengan cepat karena penurunan biaya internet. Demikian pula pengguna PermataNet juga berkembang pesat. Sistem baru ini akan dilengkapi dengan dua faktor otentikasi untuk memberikan kenyamanan dan keamanan bagi nasabah.

3. *Terminal Line Encryption* (TLE)

PermataBank merupakan salah satu bank pertama di Indonesia yang menggunakan *Terminal Line Encryption* (TLE). TLE menggunakan tanda tangan digital untuk

melindungi informasi yang mengalir di antara mesin EDC (*Electronic Data Capture*) dan komputer di pusat pemrosesan. Fitur ini dibuat untuk meningkatkan keamanan transaksi bagi nasabah dalam penggunaan EDC.

4. DC dan DRC *Infrastructure*

Untuk meningkatkan kinerja dan stabilitas sistem Permatabank, infrastruktur *Data Centre* (DC) dan *Data Recovery Centre* (DRC) yang saat ini berada di Hayam Wuruk dan Bintaro akan ditingkatkan secara signifikan, mencakup perangkat keras komputer dan perluasan fasilitas.

Perencanaan Keamanan TI (*IT Security Plan*)

Keamanan informasi merupakan hal pokok bagi pengamanan data nasabah bank. Peristiwa ataupun kasus pembobolan teknologi informasi tidak lepas dari bagaimana upaya untuk mencegahnya. Bank Permata dalam tiga tahun kedepan sedang mengembangkan IT Security, yaitu:

1. Pembentukan Tim khusus untuk kontrol akses terpusat (centralized access control).
2. Pengkajian terhadap parameter dan platform keamanan.
3. Peningkatan kesadaran akan keamanan informasi.
4. Kebijakan baru mengenai Keamanan Informasi.

IT Security Bank Permata menerapkan beberapa alat bantu untuk mendukung manajemen IT Security, yakni:

1. *Security Event Log Management System*
   Sistem ini memungkinkan Bank Permata untuk mengumpulkan, menyimpan, menganalisis data log serta memantau dan mengambil tindakan atas kejadian yang berhubungan dengan keamanan informasi. Sistem ini mencakup semua aplikasi kritis di Bank Permata.
2. *Security Configuration Monitoring System*
   Alat ini digunakan untuk memonitor konfigurasi sistem keamanan yang dipasang pada server aplikasi yang kritikal.

Permasalahan yang terjadi

Terdapat beberapa kasus yang terjadi di Bank Permata menyangkut permasalahan di bidang teknologi informasi. Adapaun kasus-kasus tersbut adalah:

Kasus 1 : Pembobolan oleh Cyber

Pada bulan Juli 2009 telah terungkap kejahatan cyber yang terjadi pada nasabah Bank Permata Cabang Samarinda Kalimantan Timur. Uang nasabah senilai Rp. 110 juta hilang akibat kejahatan cyber tersebut. Kasus ini telah terjadi lebih kurang 10 orang nasabah Bank Permata. Kejahatan ini dilakukan oleh penjahat cyber yang dilakukan secara berkelompok.

Analisis: Modus Operasional Pembobolan

Pembobolan dana nasabah ini dilakukan dengan modus mengacak 10.000 nomor *Telephone Identification Number* (TIN), yaitu nomor yang digunakan oleh nasabah Bank Permata sebagai akses kode rahasia dalam menggunakan layanan *mobile banking* maupun *internet banking*. Pelaku berhasil menembus 17 nomor TIN dan digunakan untuk mengambil uang tunai sebesar lebih kurang Rp.110 juta yang kemudian uang tersebut ditransfer ke rekening bank lain melalui mesin ATM.

Kasus 2 : Pembobolan melalui media EDC (*Electonic Data Capture*)

Kasus pembobolan Bank Permata di Bandung dengan cara menggunakan Mesin *Electonic Data Capture* (EDC) atau Mesin Gesek Kartu Debit telah merugikan Bank Permata hingga miliaran rupiah. Pembobolan ini dilakukan oleh tersangka yang bernama Riki, warga bandung yang kini buron [6].

Analisis : Modus Operasi

Pembobolan melalui media EDC ini dilakukan dengan modus pemanfaatan mesin EDC yang digunakan sebagai alat gesek kartu kredit. Pemilik mesin EDC ini bekerjasama dengan penjahat cyber dengan mengambil data dari mesin EDC yang sebelumnya telah dikonfigurasi. Pelaku mengabil id dari setiap nasabah Bank Permata yang telah menggunakan kartu kreditnya di mesin EDC tersebut. Dengan diperolehnya data nasabah tersebut, pelaku cyber dengan mudah melakukan pembobolan dana nasabah yang kemudian dimanfaatkan untuk mengambil keuntungan. Hal ini

mengakibatkan kerugian bernilai milyaran rupiah. Pada kasus modus perasi ini, pelaku cyber memperoleh data dari 2 mesin EDC yang masing-masing diperoleh dana sekitar Rp. 1,7 miliyar dan Rp. 676 juta.

HASIL DAN PEMBAHASAN

Menentukan konteks

Pembobolan dana nasabah

Assesment risiko

1. **Identifikasi risiko**

   Identifikasi risiko dilakukan dengan melihat potensi kecendrungan timbulnya risiko yang ada pada penggunaan teknologi TI pada fasilitas transaksi online bank.

   a. Sumber risiko

   Kode identifikasi berupa TIN (Telephone Identification Number) dan media transaksi online berupa EDC

   b. Kejadian

   Pelacakan nomor TIN dan Settingan alat EDC yang dilakukan oleh cyber.

   c. Akibat

   a. Dana nasabah yang dicuri hingga miliaran rupiah.
   b. Menurunnya tingkat kepercayaan nasabah terhadap bank.
   c. Timbulnya rasa takut dalam bertransaksi online oleh nasabah
   d. Dampak negatif terhadap proses bisnis bank.
   e. Dampak negatif terhadap penggunaan TIN dan kartu kredit

   d. Pemicu

   Kode TIN dan alat EDC yang kurang perhatian dari pihak bank.

   e. Pengendalian

   Dengan perbarui teknologi TIN sebagai kode transaksi online dan perhatian khusus terhadap alat EDC yang digunakan secara periodik.

2. **Evaluasi Risiko**

Evaluasi risiko dilakukan untuk memperoleh sebuah keputusan penting terkait analisis risiko yang telah dibuat. Keputusan tersebut akan dijadikan bahan utama dalam membuat risiko TI untuk melakukan pembaruan dari segi risiko tersebut. Hal ini akan dilakukan secara berulang-ulang dan terus-menerus guna mencapai kesempurnaan dan menutupi/meminimalisir tingkat risiko TI.

a. Mengumpulkan Data

Mengumpulkan data tentang bagaimana proses terjadinya pembobolan TIN

Mengumpulkan data tentang setting EDC

Mengumpulkan data tentang pengamanan dan pemeliharan EDC yang telah dilakukan

Mengumpulkan data nasabah yang merugi

b. Menganalisa Risiko

Dari kejadian yang dialami oleh pihak nasabah dapat dianalisis tentang kekurangan atau celah dari teknogo TI khususnya pada transaksi online menggunakan kode TIN dan alat EDC.

Identifikasi nilai-nilai kemungkinan

Proses identifikasi kemungkinan terjadi berupa:

a. Identifikasi dilakukan dengan mengamati proses pelacakan nomor kode TIN
b. Identifikasi alat EDC yang telah disetting ulang oleh cyber
c. Identifikasi internal jika terbukti adanya pihak internal yang melakukan fraud berupa membocorkan data kode nasabah.

Identifikasi bidang dampak

Identifikasi ini dilakukan berdasarkan dari akibat yang ditimbulkan oleh cyber yang telah membobol dana nasabah. Hal ini merupakan risiko TI yang harus menjadi perhatian penting dalam menutupi celah kekuarangan dari teknologi TI yang digunakan. Dampak yang ditimbulakan bukan hanya dari pihak nasabah namun terpenting adalah terganggunya proses bisnis bank. Tingakat kepercayaan nasabah yang menurun akan menjadi faktor penting dalam perhatian dari manajemen risiko ini.

c. Menjaga Profil Risiko

Melakukan kontrol terhadap data nasabah khususnya kode TIN.

Melakukan update terhadap manajemen risiko TI.

Melakukan kontrol pemeliharana alat EDC.

d.Respon Risiko

a. Mengartikulasikan Risiko
   Memastikan informasi tentang keadaan kejadian pembobolan TIN dan alat EDC
b. Mengelola Risiko
   Memastikan bahwa langkah-langkah untuk menangkap peluang strategis dan mengurangi risiko ke tingkat yang dapat diterima dikelola sebagai portofolio
c. Bereaksi terhadap Peristiwa
   Respon langsung terhadapa kejadian pembobolan dana melului kode TINdan alat EDC yang harus diperhatiakan secara berkala oleh petugas bank.

KESIMPULAN DAN SARAN

Setelah melakukan tahapan analisa hingga evaluasi terhadap risiko TI yang menggunakan framework RiskIT, dapat disimpulkan bahwa:

1. Framework RiskIT merupakan framework yang tepat digunakan dalam melakukan menyelesaikan kasus yang terjadi pada bank permata khususnya untuk risiko TI.
2. Hasil dari Analisa, Evaluasi dan Respon berdasrkan RiskIT yang digunakan telah menghasilkan sebuah keputusan yang bermanfaat dalam pembaharuan Risiko TI pada bank.
3. Transaksi online dan alat EDC yang menjadi sumber risiko harus selalu menjadi perhatian penting guna meminimalisir tingkat risiko yang dialami nasabah.
4. Kejadian pembobolan dana nasabah ini telah menurunkan tingkat kepercayaan masyarakat terutam nasabah bank tersebut.
5. Kerugian yang dialami bukan hanya dari segi finansial namun juga dari segi sosial dan sangat berpengaruh besar terhadap tujuan proses bisnis bank.

Rekomendasi

Dari hasil pembahasan tentang penggunaan framework RiskIT dapat direkomendasikan berupa:

1. Penggunaan framework riskIT dapat diperluas lagi dengan menggunakan skala prioritas terhadap risiko-risiko yang akan ditimbulkan.
2. Manajemen risiko TI harus selalu diperbarui dan dipelihara sehingga ikut menyesuaikan dengan potensi timbulnya risiko akan datang.
3. Peristiwa pembobolan dana nasabah dapat dicegah melalui solusi pendekatan dari pihak bank, nasabah dan pemerintah.

DAFTAR PUSTAKA

Annual Report Bank Permata tahun 2007
Annual Report Bank Permata tahun 2008
Annual Report Bank Permata tahun 2009
Annual Report Bank Permata tahun 2010
Detik.net, “Penjahat Cyber bobol bank Permata Rp.110 juta raib”,13 Juli 2009
TarungNews.com, "Sidang Kasus Pembobolan Bank Permata di PN.Bandung terindikasi Sangat Kental Beraroma Suap", 3 April 2011.
Bataviase.co.id, “Bank Permata dibobol”, 28 September 2010.
www.pikiran rakyat.com, "Bandung Terbanyak Pembobolan Bank Lewat Mesin EDC", 28 September 2010.
Peraturan Bank Indonesia PBI No. 11/19/PBI 2009 Tertanggal 4 Juni 2009 tentang Sertifikasi Manajemen Risiko Bagi Pengurus dan Pejabat Bank Umum.
Lampiran Surat Edaran Bank Indonesia Nomor: 9/30/DPNP, “Pedoman Penerapan Manajemen Risiko dalam penggunaan Teknologi Informasi oleh Bank Umum", 12 Desember 2007
____ (2009): The Risk IT Practitioner Guide, Printed in the United States of America