PENGUKURAN RISIKO ASET TEKNOLOGI INFORMASI BERBASIS PBI PADA SEKTOR PERBANKAN DI INDONESIA

Rudy M. Harahap[1]; Marisa Caroline Subita[2]; Shinta Octavia[3]

[1, 2, 3] **Jurusan Komputerisasi Akuntansi, Fakultas Ilmu Komputer, Universitas Bina Nusantara, Jln. K.H. Syahdan No. 9, Kemanggisan/Palmerah, Jakarta Barat 11480**
rudy.m.harahap@binus.ac.id

ABSTRACT

In the globalization era, information technology (IT) plays an important role in the daily corporate operation. However, there are some risks in the IT implementation. To minimize these risks, a corporate should have an IT risk management. The objective of this research is to measure IT asset risks in Indonesia banking sector. The focus of this research is the IT risks, control, and risk mitigation. The research data is processed by Risk Register Table, based on Bank Indonesia Regulation (PBI). The measurement shows the risks trend rate is not too high. However, there is a need to minimize the risks. To minimize the risks, the measurement results could be used. The minimization of IT risks could improve the bank services to its users.

Keywords: *risk measurement, IT asset risk, Bank Indonesia Regulation (PBI)*

ABSTRAK

Pada era globalisasi saat ini, teknologi informasi berperan penting bagi sebuah perusahaan dalam menjalankan kegiatan operasionalnya sehari-hari. Namun, terdapat juga risiko pada implementasi teknologi informasi tersebut. Oleh karena itu, perusahaan harus memiliki manajemen risiko teknologi informasi. Penelitian ini bertujuan untuk mengukur risiko aset TI pada perusahaan sektor perbankan. Penelitian dikhususkan pada risiko-risiko TI serta pengendalian dan mitigasi risiko. Data penelitian diolah dengan menggunakan tabel Risk Register berdasarkan PBI. Dari hasil pengukuran menunjukkan bahwa tingkat kecenderungan terjadinya risiko tidak terlalu besar. Akan tetapi, masih diperlukan perbaikan untuk meminimalkan risiko tersebut. Hasil pengukuran dapat digunakan untuk memperkecil risiko. Minimalisasi risiko teknologi informasi dapat meningkatkan pelayanan perusahaan kepada nasabahnya.

Kata kunci: *pengukuran risiko, risiko aset TI, PBI (Peraturan Bank Indonesia)*

PENDAHULUAN

Teknologi informasi (TI) mengambil peranan yang penting bagi perusahaan yang bergerak di sektor perbankan. Fungsi TI tidak hanya sebagai fasilitas pendukung utama, tetapi juga dapat menjadi *critical success factor* dalam suatu industri seperti halnya pada PT Bank Sinarmas, yang telah menggunakan dan memanfaatkan TI dalam menjalankan proses bisnisnya selama bertahun-tahun. Penggunaan TI ditujukan untuk meningkatkan pelayanan kepada setiap nasabahnya dan meningkatkan *performance* perusahaan.

Bagian TI perusahaan telah memainkan peranan yang penting dalam menjalankan roda bisnis. Namun, perusahaan belum melakukan identifikasi risiko implementasi TI. Dengan demikian, perlu dilakukan penelitian untuk mengidentifikasi risiko TI dan mengetahui aset mana saja yang perlu dilindungi jika terjadi ancaman sehingga perusahaan dapat memperkecil kerugian yang akan timbul. Untuk mengidentifikasi risiko ini, digunakan Peraturan Bank Indonesia (PBI) sebagai pedoman pengukuran risiko.

Ruang lingkup penelitian ini adalah pengukuran risiko pada aset TI, yang mencakup *hardware* (perangkat keras), *software* (perangkat lunak), jaringan (LAN, WAN), data/ informasi, sarana pendukung, dan sumber daya manusia pada perusahaan dengan menggunakan metode Peraturan Bank Indonesia (PBI). Yang dilakukan pada penelitian ini adalah mengukur risiko aset TI tersebut dan menganalisis risiko Aset TI, yang terlibat dalam proses bisnis antara bank dengan nasabah seperti *teller* dan *customer service* serta pengendalian dan mitigasi risiko yang harus dilakukan terhadap aset TI perusahaan.

Adapun tujuan penelitian ini adalah (1) Menganalisis dan mengukur risiko yang terjadi pada aset TI perusahaan dan (2) Menganalisis pengendalian dan mitigasi risiko yang harus dilakukan oleh Divisi TI perusahaan. Penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus. Teknik pengumpulan data yang digunakan adalah penelitian kepustakaan dan penelitian lapangan. Penelitian kepustakaan dilakukan dengan cara mempelajari buku-buku ilmiah serta literatur yang berkaitan dengan masalah yang dibahas atau diteliti. Penelitian lapangan dilakukan dengan mempelajari dokumen, wawancara, dan observasi.

Peneliti mengumpulkan dokumen-dokumen perusahaan dari beberapa bagian atau divisi yang berhubungan dengan aset TI, di mana dari dokumen-dokumen tersebut bisa didapatkan informasi mengenai aset TI perusahaan, termasuk risiko-risiko yang dapat terjadi. Kemudian, dilakukan wawancara dengan Kepala Divisi TI, Kepala Bagian Kebijakan dan Prosedur TI, staf Administrasi TI, dan staf lainnya di kantor perusahaan. Wawancara dilakukan sebanyak 8 kali, yaitu dari bulan Oktober 2008 sampai dengan Desember 2008. Pada saat yang sama, juga dilakukan observasi langsung ke kantor cabang Thamrin Menara Satu untuk mengetahui proses bisnis yang dilakukan sehari-hari dan gedung Divisi TI di Jalan Lombok, Jakarta. Observasi dilakukan dari bulan Oktober 2008 sampai dengan Desember 2008. Teknik analisis yang digunakan berbasis PBI, yang dipilih dari beberapa pendekatan yang ada. PBI lebih menyajikan secara rinci langkah-langkah

untuk mengukur tingkat risiko yang ada di perusahaan sektor perbankan.

METODE PENELITIAN

Metode yang digunakan adalah metode Peraturan Bank Indonesia (PBI). Yang dilakukan pada penelitian ini adalah mengukur risiko aset TI dan menganalisis risiko aset TI, yang terlibat dalam proses bisnis antara bank dengan nasabah seperti *teller* dan *customer service* serta pengendalian dan mitigasi risiko yang harus dilakukan terhadap aset TI perusahaan. Selain itu, penelitian ini menggunakan pendekatan kualitatif dengan metode studi kasus. Teknik pengumpulan data yang digunakan adalah penelitian kepustakaan dan penelitian lapangan. Penelitian kepustakaan dilakukan dengan cara mempelajari buku-buku ilmiah serta literatur yang berkaitan dengan masalah yang dibahas atau diteliti. Penelitian lapangan dilakukan dengan mempelajari dokumen, wawancara, dan observasi.

HASIL DAN PEMBAHASAN

Perbankan adalah segala sesuatu yang berkaitan dengan bank, mencakup kelembagaan, kegiatan usaha serta cara dan proses dalam melaksanakan kegiatan usahanya. Perbankan Indonesia dalam menjalankan fungsinya berasaskan demokrasi ekonomi dan menggunakan prinsip kehati-hatian (Rully Anthony, 2008). Bank adalah badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak (PBI, 2000).

Tujuan perbankan adalah menjadi penghimpun dan penyalur dana masyarakat serta bertujuan untuk menunjang pelaksanaan pembangunan nasional dalam rangka meningkatkan pemerataan pembangunan dan hasil-hasilnya, pertumbuhan ekonomi dan stabilitas nasional, ke arah peningkatan taraf hidup rakyat banyak. Perbankan memiliki kedudukan yang strategis, yakni sebagai penunjang kelancaran sistem pembayaran, pelaksanaan kebijakan moneter, dan pencapaian stabilitas sistem keuangan sehingga diperlukan perbankan yang sehat, transparan, dan dapat dipertanggungjawabkan (Djojosoedarjo, 2000).

Teknologi Informasi adalah *hardware*, *software*, telekomunikasi, manajemen database, dan teknologi pemrosesan informasi lainnya yang digunakan dalam sistem informasi berbasis komputer (O'Brein, 2005: 704). Teknologi Informasi merupakan suatu alat yang dapat menerima, memproses, menyimpan dan mengeluarkan hasil digital, yakni dari bagian-bagian pembangunan yang digunakan untuk membuat sistem informasi. Teknologi Informasi didefinisikan sebagai suatu teknologi yang berhubungan dengan pengolahan data menjadi informasi dan proses penyaluran data atau informasi tersebut dibatasi oleh ruang dan waktu (Indrajit: 2).

Aset Teknologi Informasi merupakan barang yang dinilai oleh suatu perusahaan atau organisasi yang dapat memberikan manfaat pada kegiatan operasional pada perusahaan, yang berwujud maupun yang tidak berwujud dan dijadikan sebagai modal perusahaan atau organisasi (Rully Anthony, 2008). Aset Teknologi Informasi dilihat dari segi manfaat yang dirasakan terbagi atas (1) *IT Asset Tangible,* yaitu aset pada perusahaan yang bermanfaat bagi perusahaan atau *user* yang secara nyata dapat langsung diaplikasikan untuk keuntungan pribadi maupun bersama seperti *hardware, database, server,* komputer; dan (2) *IT Assets Intangible,* yaitu aset pada perusahaan yang bermanfaat bagi perusahaan maupun bagi *user* yang secara tidak nyata dapat diperoleh manfaatnya seperti *software aplikasi, program aplikasi, security program,* dan *license software*.

Hardware adalah mesin dan media, perlengkapan fisik (kebalikan dari program komputer atau metode penggunaan) serta peralatan mekanis, magnetis, elektrik, elektronik, atau optikal. Artinya, *hardware* adalah peralatan fisik yang membentuk suatu sistem komputer dan segala perlengkapan yang berhubungan dengannya (O'Brein, 2005: 702). *Software* adalah program dan prosedur komputer yang berkaitan dengan operasi sistem informasi. *Software* merupakan sebuah kumpulan rinci intruksi-intruksi yang mengontrol sebuah komputer atau jaringan komunikasi, yang terbagi menjadi 2, yaitu *system software* dan *application software*. *System software* adalah sebuah kumpulan rinci instruksi komputer yang dapat digunakan untuk membentuk tugas terkait serta memproduksi hasil yang terkait. *System software* merupakan program yang mengendalikan dan mendukung berbagai operasi sistem komputer seperti sistem operasi, DBMS, *program* layanan, dan utilitas (O'Brein, 2005: 715). *Application software* adalah suatu program atau kombinasi dari beberapa program yang dibuat untuk kegunaan khusus.

Pengertian sistem adalah (1) Sekelompok elemen yang saling berhubungan dan membentuk kesatuan; (2) Sekelompok komponen yang bekerja bersama menuju tujuan yang bersama dengan menerima *input* serta menghasilkan *output* dalam proses transformasi yang teratur; (3) Perakitan metode, prosedur atau teknik yang disatukan oleh interaksi teregulasi untuk membentuk kesatuan organisasi; dan (4) Sekumpulan orang, mesin, dan metode yang teratur dan yang dibutuhkan untuk menyelesaikan serangkaian fungsi tertentu (O'Brein, 2005: 714). Di sisi lain, informasi adalah data yang ditempatkan dalam konteks yang berarti dan berguna untuk pemakai akhir (*end user*). Adapun menurut PBI (2007: 53), informasi adalah aset yang sangat penting bagi bank, baik informasi yang terkait dengan nasabah, keuangan, laporan, maupun informasi lainnya.

Risiko merupakan kemungkinan terjadinya beberapa ancaman yang mudah menyerang (Peltier, 2001: 21). Jenis-jenis risiko terkait TI adalah risiko operasional, risiko kepatuhan, risiko hukum, risiko reputasi, reputasi strategis, dan risiko likuiditas (PBI, 2007: 15). *Pertama*, risiko operasional melekat di setiap produk dan layanan yang disediakan bank. Penggunaan TI dapat menimbulkan terjadinya risiko operasional yang disebabkan ketidakcukupan/ketidaksesuaian desain, implementasi, pemeliharaan sistem atau komputer dan perlengkapannya, metode pengamanan, testing, dan standar internal audit serta penggunaan jasa pihak lain dalam penyelenggaraan TI. *Kedua*, risiko kepatuhan dapat timbul bila bank tidak memiliki sistem yang dapat memastikan kepatuhan bank terhadap ketentuan yang berlaku bagi bank seperti kerahasiaan data nasabah. Risiko kepatuhan dapat berdampak buruk terhadap reputasi serta citra bank, juga berdampak pada kesempatan berusaha dan kemungkinan ekspansi. *Ketiga*, risiko hukum adalah ketika bank menghadapi risiko hukum yang disebabkan adanya tuntutan hukum, ketiadaan peraturan perundangan yang mendukung atau kelemahan perikatan seperti tidak dipenuhinya syarat sah suatu kontrak. *Keempat*, risiko reputasi adalah opini publik yang negatif yang dapat timbul karena kegagalan sistem yang mendukung produk, kasus yang ada pada produk bank, dan ketidakmampuan bank memberikan dukungan layanan nasabah pada saat terjadi kegagalan sistem (*downtime*). Opini negatif ini dapat menurunkan kemampuan bank memelihara loyalitas nasabah dan keberhasilan produk dan layanan bank. *Kelima*, risiko strategis timbul karena ketidakcocokan TI yang digunakan bank dengan tujuan strategis bank dan rencana strategis yang dibuat untuk mencapai tujuan tersebut. Hal ini karena kualitas implementasi maupun sumber daya yang digunakan TI kurang memadai. Sumber daya tersebut mencakup saluran komunikasi, *operating systems*, *delivery network*, serta kapasitas dan kapabilitas pengelola TI. *Keenam*, risiko likuiditas disebabkan oleh ketidakmampuan atau kegagalan bank memenuhi kewajiban keuangan jangka pendek dan atau kewajiban keuangan lainnya pada saat jatuh waktu.

Analisis risiko adalah proses mengidentifikasi aset dan ancaman, serta memprioritaskan serangan ancaman dan

mengidentifikasi pengamanan yang sesuai (Peltier, 2001: 21). Di sisi lain, pengukuran risiko adalah rangkaian proses yang dilakukan dengan tujuan untuk memahami signifikansi dari akibat yang akan ditimbulkan suatu risiko, baik secara individual maupun portofolio, terhadap tingkat kesehatan dan kelangsungan usaha. Pemahaman yang akurat tentang signifikansi tersebut akan menjadi dasar bagi pengelolaan risiko yang terarah dan berhasil guna (Dilan S. Batuparan, 2001).

Manajemen risiko adalah proses mengidentifikasi risiko dan mengukur untuk mengurangi risiko (Peltier, 2001: 224). Manajemen risiko adalah proses logik yang digunakan oleh perusahaan bisnis dan individual; sedangkan menurut Djojosoedarso (2005: 2), manajemen risiko adalah pengelolaan berbagai cara penganggulangan risiko.

Operasional kegiatan usaha bank (termasuk pemrosesan transaksi dan pembukuan) sangat tergantung pada keandalan TI. Informasi yang dihasilkan sangat dibutuhkan dalam pengambilan keputusan, baik oleh pihak *intern* bank maupun pihak *ekstern*. Untuk itu, TI bank harus dikelola secara efisien guna memaksimalkan efektivitas penggunaannya dan agar risiko terkait dari teknologi yang diimplementasikan dapat dimitigasi. Mengingat bahwa TI merupakan aset penting dalam operasional yang dapat meningkatkan nilai tambah dan daya saing bank sementara dalam penyelenggaraannya mengandung berbagai risiko, maka bank perlu menerapkan *IT Governance*. Penerapan *IT Governance* dilakukan melalui penyelarasan Rencana Strategis Teknologi Informasi dengan strategi bisnis bank, optimalisasi pengelolaan sumber daya, pemanfaatan TI (*IT value delivery*), pengukuran kinerja, dan penerapan manajemen risiko yang efektif. Keberhasilan penerapan *IT Governance* sangat tergantung pada komitmen dewan komisaris dan direksi serta seluruh satuan kerja di bank, baik penyelenggara maupun pengguna TI. Karena itu, diperlukan kebijakan yang memuat peran dan tanggung jawab dewan komisaris, direksi dan pejabat tertinggi TI dalam memastikan diterapkannya manajemen risiko TI secara efektif.

Manajemen risiko TI bank adalah kemampuan bank memitigasi (mengurangi) risiko-risiko TI tergantung dari hasil identifikasi, pengukuran, pengendalian, dan pemantauan risiko-risiko terkait TI yang berpotensi mengancam keamanan dan operasional bank (PBI, 2007: 14). Mengingat pentingnya TI dalam mendukung tercapainya rencana strategis bisnis bank, maka bank harus mengelola seluruh sumber daya TI sebagai "aset" bank. Sumber daya TI meliputi aplikasi, informasi, infrastruktur dan sumber daya manusia. Untuk itu, pada proses penilai risiko, bank harus melakukan evaluasi atas segala hal yang mengancam sumber daya TI melalui proses identifikasi, pengukuran, dan pemantauan risiko potensial, baik kecenderungan atau probabilitas terjadinya maupun besarnya dampak.

Terdapat berbagai pendekatan yang dapat dilakukan bank dalam proses identifikasi seperti pendekatan proses, aset, produk, dan kejadian. Pada pendekatan berdasarkan aset, identifikasi risiko pengamanan informasi dilakukan dengan melakukan klasifikasi terhadap "aset" terkait teknologi informasi berdasarkan risiko. Selanjutnya, bank melakukan pengukuran kecenderungan atau probabilitas terjadinya risiko atas setiap aset dan besarnya dampak kerugian yang akan dialami untuk dapat mengetahui besarnya risiko potensial yang harus dihadapi atau Nilai Risiko Dasar (NRD).

Penilaian ini dilakukan oleh setiap satuan kerja yang memiliki sumber daya TI dan atau dapat dikoordinasikan oleh satuan kerja yang membidangi TI atau manajemen risiko. Dalam menentukan aset yang kritikal maupun mengukur risiko, setiap satuan kerja harus dapat menentukan kemungkinan adanya ancaman (*threat*), serangan (*attack*), dan kerawanan (*vulnerability*) dari setiap sumber daya TI yang digunakan masing-masing satuan kerja serta kemungkinan dampaknya pada integritas (*integrity*), kerahasiaan (*confidentiality*), dan ketersediaan (*availability*) dari data/informasi yang dimiliki. Proses ini harus dilakukan bank karena identifikasi dan pengukuran risiko dapat menunjukkan potensial kegagalan atau kelemahan proses pengamanan informasi yang dapat berpengaruh pada kesuksesan bisnis bank sehingga bank dapat melakukan penanganan yang tepat terhadap setiap risiko potensial.

Proses manajemen risiko terkait TI yang harus dilakukan setiap bank mencakup 2 hal penting, yaitu tahap penilaian risiko dan tahap pengendalian dan mitigasi risiko (PBI, 2007: 61). Proses penilaian risiko mencakup identifikasi risiko, pengukuran risiko, identifikasi pengendalian yang diimplementasikan, penentuan nilai risiko yang diharapkan, dan analisis nilai risiko.

Pada proses identifikasi risiko, proses yang dilakukan adalah identifikasi (penentuan klasifikasi) risiko aset, identifikasi risiko dan evaluasi risiko yang terkait dengan aset, dan analisis kerawanan. Pada proses identifikasi (penentuan klasifikasi) risiko aset, penilaian risiko pengamanan informasi menggunakan pendekatan aset diisikan pada form *Risk Register* (Tabel 1).

Tabel 1 Dokumen Hasil Identifikasi dan Pengukuran Risiko (*Risk Register*)

				Inheren				Residual			
No	Aset	Deskripsi Kerawanan	Analisis Kerawanan	Kecenderungan	Dampak	Nilai Risiko Dasar	Pengendalian yang Ada	Kecenderungan	Dampak	Nilai Risiko Dasar	Nilai Risiko yang Diharapkan
0	1	2	3	4	5	6	7	8	9	10	11

Pada kolom nomor 1 di *Risk Register*, yaitu tentang aset, diisi dengan nama atau jenis aset yang dihasilkan dalam menjalankan proses bisnis bank dan aset yang mendukung terlaksananya proses bisnis tersebut. Aset yang dimaksud bukan aset secara akuntansi, namun segala sesuatu yang mempunyai nilai bagi organisasi dan harus diamankan termasuk data, perangkat lunak, perangkat keras, jaringan komunikasi dan data, sarana pendukung, dan sumber daya manusia. Di sini, ditentukan pemilik aset tersebut dan identifikasi tingkatan penting tidaknya (kritikal) aset tersebut bagi unit kerja pengguna dan unit kerja penyelenggara TI.

Pada kolom 2 di *Risk Register* diisi dengan hasil identifikasi, evaluasi pengguna, dan penyelenggara TI terhadap potensial kegagalan atau kelemahan proses pengamanan yang ada/diterapkan bank atas aset yang telah didefinisikan sehingga berpengaruh secara signifikan terhadap kinerja bank. Satu aset dapat memiliki beberapa risiko.

Pada kolom 3 di *Risk Register* diisi dengan faktor rawan yang dapat menyebabkan terjadinya kegagalan atau kelemahan pengamanan TI (risiko), yang telah diidentifikasi pada kolom 2. Tiap risiko dapat memiliki beberapa kerawanan. Contoh pencantuman di kolom 3 adalah pengamanan terhadap lemari penyimpanan arsip kurang memadai dan informasi nasabah tidak disimpan dengan baik pada tempat yang seharusnya.

Selanjutnya, setelah proses identifikasi risiko dilalui, dilakukan proses pengukuran risiko, di mana besarnya pengaruh risiko diketahui dengan menilai kecenderungan risiko dan dampak yang dapat ditimbulkan oleh risiko tersebut terhadap proses bisnis. Kriteria pengukuran yang digunakan mengacu kepada metode *risk assessment* yang berlaku di bank. Proses ini dilakukan oleh personil yang mengetahui proses bisnis dan pengamanan atas informasi di proses tersebut. Kolom 4, 5, dan 6 pada *Risk Register* diisi dengan hasil pengukuran bank atas kecenderungan dan dampak dari risiko sebelum pengendalian dilakukan terhadap aset berisiko tersebut, sedangkan kolom 8, 9, dan 10 diisi dengan hasil pengukuran bank atas kecenderungan dan

dampak dari risiko setelah pengendalian dilakukan terhadap aset berisiko tersebut. Proses pengukuran risiko ini terdiri dari proses pengukuran kecenderungan, pengukuran dampak, dan pengukuran kemungkinan.

Pada proses pengukuran kecenderungan (*probability*), kolom 4 *Risk Register* diisi dengan Kecenderungan Inheren yang merupakan kemungkinan terjadinya risiko sebelum adanya pengendalian. Kolom 8 diisi dengan Kecenderungan Residual yang merupakan kemungkinan terjadinya risiko setelah adanya pengendalian. Kecenderungan dapat diukur dengan suatu kriteria pengukuran, yaitu nilai kuantitatif dari kecenderungan terjadinya risiko yang disebutkan pada deskripsi risiko. Kuantifikasi kecenderungan dapat berupa ukuran terjadinya risiko dalam satuan waktu seperti frekuensi kejadian setiap hari, setiap minggu, setiap bulan, atau setiap tahun. Contoh kriteria pengukuran kecenderungan tampak pada Tabel 2.

Tabel 2 Tingkatan Pengukuran

Level	Frekuensi Kejadian	Potensi Terjadi
5	Sangat sering terjadi	Potensi terjadi tinggi dalam jangka pendek
4	Lebih sering terjadi	Potensi terjadi dalam jangka panjang
3	Cukup sering terjadi	Potensi terjadi sedang
2	Jarang terjadi	Potensi terjadi kecil
1	Hampir tidak pernah terjadi	Kemungkinan terjadi sangat kecil

Pada proses pengukuran dampak (*impact*/*severity*), kolom 5 *Risk Register* diisi dengan Dampak Inheren yang menggambarkan tingkatan kerusakan yang disebabkan oleh terjadinya risiko relatif terhadap aset sebelum ada/diterapkannya pengendalian. Kolom 9 diisi dengan Dampak Residual yang menggambarkan tingkatan kerusakan yang disebabkan oleh terjadinya risiko relatif terhadap aset setelah ada/diterapkannya pengendalian. Contoh klasifikasi dampak tampak pada Tabel 3.

Tabel 3 Klasifikasi Dampak

Nilai	Potensi Gangguan terhadap Proses Bisnis
5	Proses Bisnis mengalami kegagalan total sehingga keseluruhan bisnis bank tidak tercapai.
4	Proses Bisnis mengalami gangguan yang menyebabkan aktivitas bisnis bank mengalami penundaan sampai Aset Pemrosesan Informasi yang terkait pulih.
3	Proses Bisnis mengalami gangguan yang menyebabkan sebagian bisnis bank mengalami penundaan sampai Aset Pemrosesan Informasi yang terkait pulih.
2	Proses Bisnis mengalami gangguan namun aktivitas tugas pokok Tim dapat dikerjakan secara normal karena aset pemrosesan informasi yang terkait dapat digantikan oleh Aset Pemrosesan Informasi lainnya.
1	Tidak menyebabkan gangguan terhadap operasional proses bisnis.

Pada proses penentuan nilai risiko, kolom *Risk Register* diisi dengan Nilai Risiko Dasar (NRD), yaitu tingkatan risiko aset sebelum ada/diterapkannya pengendalian. Kolom 10 *Risk Register* diisi dengan Nilai Risiko Akhir (NRA), yaitu tingkatan risiko aset setelah ada/diterapkannya pengendalian. Penilaian risiko pada contoh ini diukur menggunakan 3 tingkatan yang meliputi *Low*, *Medium*, dan *High* seperti tampak pada Tabel 4.

Tabel 4 Tingkatan Risiko

Kecenderungan					
5	Medium	Medium	High	High	High
4	Low	Medium	High	High	High
3	Low	Low	Medium	High	High
2	Low	Low	Medium	Medium	High
1	Low	Low	Medium	Medium	High
	1	2	3	4	5

Dampak

Setelah proses pengukuran risiko, kemudian dilakukan proses identifikasi pengendalian yang diimplementasikan. Pada proses ini, kolom 7 *Risk Register* diisi dengan langkah-langkah pengendalian yang telah diimplementasikan oleh bank untuk mengurangi risiko atas aset yang diidentifikasi seperti kebijakan dan prosedur bank terkait aset; penggunaan teknologi tertentu untuk mengendalikan risiko secara otomatis, atau tersistem seperti *audit log*, *on line approval*, *parameter value* di sistem. Contoh pencantuman kontrol di kolom 7 untuk aset yang berupa informasi nasabah dalam bentuk *hardcopy*, ketentuan mengenai pengelolaan arsip, akses ruang arsip harus menggunakan PIN, dan penggunaan CCTV. Setelah itu, dilakukan proses penentuan nilai risiko yang diharapkan, di mana atas semua aset yang teridentifikasi, bank menentukan nilai risiko yang diharapkan (limit risiko). Sebagai contoh, apabila diharapkan risiko kebocoran informasi rahasia nasabah harus pada level rendah, pada kolom 11 diisi *Low*.

Proses akhir tahap penilaian risiko, adalah analisis nilai risiko. Analisis ini dilakukan terhadap isian form *Risk Register*. Contoh pengisian form *Risk Register* (*IT Asset*: Informasi Nasabah dalam bentuk *hardcopy*) penilaian risiko pengamanan informasi yang menggunakan pendekatan aset yang telah melalui tahap penilaian risiko tampak pada Tabel 5.

Berdasarkan isian form *Risk Register*, bank melakukan analisis nilai risiko atas masing-masing aset yang teridentifikasi. Bank harus menganalisis apakah terdapat risiko yang belum dikendalikan, tetapi dapat diterapkan bentuk pengendalian tertentu. Perbandingan antara Nilai Risiko Akhir (NRA) dengan Nilai Risiko yang Diharapkan (NRD) dari berbagai aset yang teridentifikasi merupakan parameter dasar untuk langkah-langkah yang diperlukan dalam memitigasi risiko. Sebagai contoh, apabila diharapkan risiko kebocoran informasi rahasia nasabah harus pada level *Low*, maka perlu dilakukan pengendalian tambahan apabila NRA masih *Medium*. Bank selanjutnya menetapkan Rencana Penanganan Risiko atas aset tersebut. Misalnya, bank perlu memperbaiki *risk control system* untuk pengamanan informasi atau mengkinikan kebijakan dan prosedur pengamanan.

Setelah tahap penilaian risiko, kemudian dilakukan tahap pengendalian dan mitigasi risiko. Pada tahap ini, bank harus menetapkan bentuk penanganan risiko yang akan diterapkan untuk menimalisasi risiko yang dihadapi bank. Dari bentuk-bentuk penanganan risiko (*accept*, *control/mitigate*, *avoid*, *transfer*), pengendalian atau mitigasi risiko memegang peranan penting karena tanpa sistem informasi yang handal dan aktivitas pengendalian TI yang efektif, bank tidak mampu menghasilkan laporan keuangan yang akurat, terkini, utuh, dan lengkap.

Secara umum, bentuk pengendalian adalah kebijakan, ketentuan, dan prosedur yang ada di bank; sistem pengendalian risiko yang dilakukan dengan menggunakan teknologi sehingga secara otomatis dapat memitigasi risiko yang ada seperti *audit log*, *on line approval*, *parameter value* di sistem yang digunakan serta *training* dan *security awareness program*.

Tinjauan atas pengendalian dilakukan 2 kali, yaitu

Tabel 5 Hasil Identifikasi dan Pengukuran Risiko pada *Risk Register*

No	Aset	Deskripsi Risiko	Analisis Kerawanan	Inheren			Kontrol yang Ada	Residual			Nilai Risiko Diharapkan (NRD)
				Kecenderungan (min=1, max=5)	Dampak (min=1, max=5)	Nilai Risiko Akhir		Kecenderungan (min=1, max=5)	Dampak (min=1,max=5)	Nilai Risiko Akhir (NRA)	
0	1	2	3	4	5	6	7	8	9	10	11
1.	Informasi nasabah dalam bentuk hardcopy	Informasi bocor pada pihak yang tidak berwenang	Pengamanan terhadap lemari penyimpanan arsip kurang memadai Informasi nasabah diletakkan terbuka/tercecer	Level 4	Level 5	HIGH	1.Ketentuan melalui pengelolaan arsip 2.Akses arsip dengan PIN 3.CCTV	Level 3	Level 2	MEDIUM	LOW

pertama pada proses penilaian risiko (*risk assessment*) di mana bank mengidentifikasi pengendalian yang telah ada sebelumnya dan kedua setelah mendapatkan NRA. Dengan membandingkan NRD dengan NRA, bank dapat menganalisis kelemahan pengendalian yang telah diterapkan dan bentuk pengendalian pengamanan yang dapat direkomendasikan untuk diterapkan kemudian. Bentuk pengendalian dapat beragam dan tidak terbatas pada pengendalian umum (*general controls*) seperti pengendalian yang harus ada di operasional *Data Center,* tetapi juga pengendalian aplikasi (*application controls*) seperti rekonsiliasi dalam *balancing control activities*. Dengan demikian, atas seluruh aset bank, baik pada level bank, satuan kerja, maupun masing-masing petugas atau pengguna TI, dapat terhindar dari setiap risiko potensial.

PT Bank Sinarmas sebagai salah satu perusahaan yang bergerak di sektor perbankan di Indonesia, saat ini telah menerapkan manajemen risiko sesuai dengan Lampiran 1 Surat Edaran Bank Indonesia No.5/21/DPNP tanggal 29 September 2003 tentang "Pedoman Standar Penerapan Manajemen Risiko bagi Bank Umum". Perusahaan telah membentuk Komite Manajemen Risiko (KMR), Komite Pemantau Risiko (KPR), dan Satuan Kerja Manajemen Risiko (SKMR). Semua anggota Direksi dan Dewan Komisaris yang terlibat dalam KMR, KPR, dan SKPR telah memperoleh sertifikasi manajemen risiko yang diberikan oleh Badan Sertifikasi Manajemen Risiko dan Bank Indonesia. Namun, perusahaan belum memiliki divisi atau staf khusus untuk menangani risiko-risiko TI dan tidak memiliki Direktur TI yang khusus menangani rencana strategis TI, kebijakan dan prosedur serta masalah-masalah yang ada pada Divisi TI. Semua hal yang berhubungan dengan aspek TI dikelola oleh Direktur Operasional. Selain itu, Divisi TI juga tidak pernah mendokumentasikan risiko-risiko yang telah terjadi. Inilah yang menjadi kelemahan perusahaan dalam mengelola risiko TI. Untuk mengatasi risiko TI, manajemen perlu melakukan beberapa proses.

Risiko yang dapat terjadi pada perusahaan pada aspek Risiko Operasional adalah kesalahan posting/pembukuan; kekeliruan pengisian denominasi uang ke kotak uang/salah *setting*; gangguan sistem atau jaringan sehingga ATM tidak dapat beroperasi; kegagalan/penyangkalan transaksi yang dilakukan oleh nasabah (*complaint*); bencana seperti banjir, gempa, kebakaran, dan lainnya; kriminalitas (mesin ATM dibongkar paksa/digondol); dan mesin ATM tidak dapat digunakan untuk melakukan transaksi.

Pada aspek Risiko Reputasi, risikonya adalah keluhan dari nasabah karena adanya kesalahan (*error*) sistem teknologi serta kegagalan transaksi yang dialami nasabah. Risiko Reputasi tersebut juga dapat muncul akibat kesalahan yang dilakukan oleh pihak ketiga sebagai penyedia sarana penunjang sistem teknologi.

Pada aspek Risiko Strategis, risiko yang ada adalah adanya ketidaksesuaian pembelian salah satu *hardware* dengan ketentuan atau rencana yang telah dibuat sehingga *hardware* tersebut tidak dapat memenuhi kebutuhan pengguna untuk jangka waktu panjang karena kapasitas *hardware* yang tidak dapat dipakai untuk waktu yang lama sehingga bank harus membeli *hardware* yang baru.

Pada aspek Risiko Kepatuhan, adalah ketika Divisi TI perusahaan memutuskan untuk mengimplementasikan *Internet Banking*. Implementasinya telah direncanakan untuk berjalan pada tanggal 1 Maret 2008. Pihak Divisi TI telah membuat laporan kepada Bank Indonesia tentang rencana implementasi tersebut 2 bulan sebelum diimplementasikan dan 1 bulan setelah diimplementasikan. Akan tetapi, pada tanggal 3 Maret 2008 rencana tersebut baru dapat diimplementasikan sehingga waktu pengimplementasian tidak sesuai dengan yang direncanakan (1 Maret 2008). Oleh karena keterlambatan implementasi, bank membayar sanksi atas keterlambatan implementasi selama dua hari. Sanksi tersebut yang diartikan sebagai risiko kepatuhan.

Pada aspek Risiko Likuiditas, dengan lingkup ATM, karena bank memiliki jumlah ATM yang banyak, adalah kurangnya jumlah penyediaan dana kas di mesin ATM, jumlah transaksi di mesin ATM yang sangat rendah sehingga uang yang diisikan ke mesin ATM tidak digunakan (*idle money*) dan nasabah tidak dapat melakukan penarikan uang dari mesin ATM karena uang di mesin ATM tidak tersedia atau habis serta tidak dapat/gagal melakukan *settlement* dengan bank lain peserta anggota jaringan ATM lokal atau internasional.

Pada aspek Risiko Hukum, dengan lingkup ATM, risikonya adalah perselisihan antara nasabah dengan bank terkait dengan transaksi nasabah di ATM yang menyebabkan kerugian finansial di pihak nasabah atau bank, perselisihan dengan pihak luar sehubungan dengan penggunaan lisensi perangkat lunak mesin ATM dan mesin *switching*, dan perselisihan dengan bank lain yang menjadi anggota jaringan ATM lokal/internasional.

Sebagaimana bank lainnya, proses pengukuran risiko terhadap aset TI dengan menggunakan pedoman peraturan Bank Indonesia belum pernah dilakukan sebelumnya oleh perusahaan karena pedoman tersebut baru diterbitkan pada awal tahun 2007 (Surat Edaran Bank Indonesia Nomor: 9/30/DPNP tanggal 12 Desember 2007). Oleh karena itu, pada penelitian ini dilakukan identifikasi terhadap aset TI yang penting bagi unit kerja pengguna dan unit kerja penyelenggara TI, dengan menentukan pemilik aset risiko agar risiko yang diidentifikasi dan dinilai atau diukur dapat

dipantau oleh manajemen yang menggunakan *Risk Register* dengan pendekatan aset.

Berdasarkan hasil identifikasi dan pengukuran risiko pada *Risk Register*, atas pengendalian yang telah tersedia di perusahaan, masih terdapat beberapa pengendalian yang harus ditingkatkan oleh perusahaan sehingga perusahaan dapat mengurangi risiko yang dapat terjadi.

Pada aset *hardware,* perusahaan perlu menambahkan pengendalian yang ada pada 11 komponen. Pada *Printer Teller,* yaitu melakukan *maintenance* dari pihak *vendor* atau dari pihak TI bank secara periodik, yakni 1 bulan 1 kali untuk meminimalkan risiko yang dapat terjadi seperti kesalahan konfigurasi sehingga menyebabkan *printer* tidak dapat digunakan dan menghindari risiko operasional dan risiko reputasi pada bank.

Pada *Pinpad Teller* Ingenico (Aktivasi ATM), yaitu melakukan *maintenance* secara periodik, yakni 1 bulan 1 kali untuk meminimalkan risiko yang dapat terjadi, seperti kesalahan instalasi sehingga menyebabkan *user* tidak dapat menggunakan dengan baik (biasanya terjadi pada saat pemasangan pertama kali), dan untuk menghindari dari risiko operasional dan risiko reputasi pada bank.

Pada DMZ 2: *Server* UMG, yaitu melakukan *maintenance* secara periodik, yakni 1 bulan 1 kali untuk meminimalkan risiko yang dapat terjadi seperti *server* yang mati atau *down* sehingga menyebabkan *user* tidak dapat melakukan transaksi yang berhubungan dengan *delivery channel* dan menghindari dari risiko operasional dan risiko reputasi bank.

Pada DMZ 2: SAN *Switch* dan HBA *Cable,* yaitu dengan melakukan *maintenance* secara periodik 1 bulan 1 kali untuk meminimalkan risiko yang dapat terjadi seperti kabel putus karena tidak memakai kabel CAT5 atau CAT6, atau memakai kabel palsu (lebih mudah patah) atau Panel berada di tembok bagian bawah (mudah terinjak atau tertendang oleh staf yang bekerja) sehingga menyebabkan *user* tidak dapat melakukan sebagian transaksi yang ada, dan untuk menghindari dari risiko operasional dan reputasi pada bank.

Pada DMZ 1: *Server Internet Banking,* yaitu dengan melakukan *maintenance* secara periodik 1 bulan 1 kali untuk meminimalkan risiko yang dapat terjadi seperti kesalahan pada pemograman atau rusaknya *hardware* akibat *grounding* sehingga menyebabkan *user* tidak dapat melakukan transaksi *financial* pada aplikasi *Internet Banking*, dan untuk menghindari dari risiko operasional dan risiko reputasi pada bank.

Pada DMZ 1: *Server* DNS+Portal, yaitu dengan melakukan *maintenance* secara periodik 1 bulan 1 kali untuk meminimalkan risiko yang dapat terjadi seperti rusaknya *server* (karena *grounding hardware* atau lainnya) sehingga *user* tidak dapat mencari data/dokumen-dokumen pada portal, dan untuk menghindari dari risiko operasional, risiko reputasi, dan risiko kepatuhan pada bank.

Pada DMZ 1: *Server* Nokia *Management* Portal, yaitu dengan melakukan *maintenance* secara periodik 1 bulan 1 kali untuk meminimalkan risiko yang dapat terjadi seperti rusaknya *server* (karena *grounding hardware* atau lainnya) sehingga *user* tidak dapat mengubah konfigurasi pada *firewall*, dan untuk menghindari risiko operasional pada bank.

Pada DMZ 1: *Server* Juniper *Management,* yaitu dengan melakukan *maintenance* secara periodik 1 bulan 1 kali untuk meminimalkan risiko yang dapat terjadi seperti rusaknya *server* (karena *grounding hardware* atau lainnya) sehingga *user* tidak dapat mengubah konfigurasi pada *firewall*, dan untuk menghindari risiko operasional pada bank.

Pada Utility: UPS, yaitu dengan melakukan *maintenance* UPS secara periodik oleh *vendor* secara berkala 1 bulan 1 kali untuk meminimalkan risiko yang dapat terjadi seperti UPS tidak berfungsi akibatnya *server*-pun mati sehingga *user* tidak dapat melakukan transaksi yang dilakukan, dan untuk menghindari dari risiko operasional pada bank.

Pada Utility: *Genset,* yaitu dengan melakukan *maintenance Genset* secara periodik oleh *vendor* secara berkala 1 bulan 1 kali untuk meminimalkan risiko yang dapat terjadi seperti *Genset* tidak berfungsi sehingga pada saat listrik mati, transaksi tidak dapat dilakukan, dan untuk menghindari dari risiko operasional pada bank.

Pada Utility: AC pada ruangan *server,* yaitu dengan melakukan *maintenance* AC secara periodik oleh *vendor* atau pihak TI bank secara berkala 1 bulan 1 kali untuk meminimalkan risiko yang dapat terjadi seperti AC mati karena listrik padam/tidak di-*maintenance* (sehingga *server* menjadi panas) sehingga pada saat listrik padam transaksi tidak dapat dilakukan, dan untuk menghindari dari risiko operasional pada bank.

Pada aset *software,* perusahaan perlu menambahkan pengendalian yang ada pada 12 komponen. Pada Front End S1/Aplikasi (Aplikasi Front End S1), yaitu dengan melakukan *maintenance* oleh pihak *vendor* dan *mainternance update antivirus* secara berkala untuk meminimalkan risiko yang dapat terjadi seperti modifikasi *software, coding error,* tidak *update antivirus,* kesalahan konfigurasi sehingga *software error,* tidak dapat membaca file-file tertentu, terkena virus, akibatnya transaksi tidak dapat dilakukan, dan untuk menghindari dari risiko operasional pada bank.

Pada IBM *software,* yaitu dengan melakukan *maintenance* oleh pihak *vendor* dan *mainternance update antivirus* secara berkala untuk meminimalkan risiko yang dapat terjadi seperti modifikasi *software, coding error, antivirus* tidak *update,* kesalahan konfigurasi sehingga *software error,* tidak dapat membaca file-file tertentu, terkena virus, akibatnya transaksi tidak dapat dilakukan, dan untuk menghindari risiko operasional pada bank.

Pada apikasi *Customer Service* (S1) Phase II, yaitu dengan melakukan *maintenance* oleh pihak *vendor* dan *mainternance update antivirus* secara berkala untuk meminimalkan risiko yang dapat terjadi seperti modifikasi *software, coding error, antivirus* tidak *update,* kesalahan konfigurasi sehingga *software error,* tidak dapat membaca file-file tertentu, terkena virus, akibatnya transaksi tidak dapat dilakukan, dan untuk menghindari dari risiko operasional pada bank.

Pada *software* Microsoft, yaitu dengan melakukan *maintenance* oleh pihak *vendor* dan *maintenance update antivirus* secara berkala untuk meminimalkan risiko yang dapat terjadi seperti modifikasi *software, coding error, antivirus* tidak *update,* kesalahan konfigurasi sehingga *software error,* tidak dapat membaca file-file tertentu, terkena virus, akibatnya transaksi tidak dapat dilakukan, dan untuk menghindari dari risiko operasional pada bank.

Pada *software* SKN IBS, yaitu dengan melakukan *maintenance* oleh pihak *vendor* dan *mainternance update antivirus* secara berkala untuk meminimalkan risiko yang dapat terjadi seperti modifikasi *software, coding error,* tidak *update antivirus,* kesalahan konfigurasi sehingga *software error,* tidak dapat membaca file-file tertentu, terkena virus, akibatnya transaksi tidak dapat dilakukan, dan untuk menghindari dari risiko operasional pada bank.

Pada *software* Linux Red Hat, yaitu dengan melakukan *maintenance* dengan pihak *vendor* dan *mainternance update antivirus* secara berkala untuk meminimalkan risiko yang dapat terjadi seperti modifikasi *software, coding error,* tidak *update antivirus,* kesalahan konfigurasi sehingga *software error,* tidak dapat membaca file-file tertentu, terkena virus, akibatnya transaksi tidak dapat dilakukan, dan untuk menghindari dari risiko operasional pada bank.

Pada Xlink *software,* yaitu dengan melakukan *maintenance* dengan pihak *vendor* dan *mainternance update antivirus* secara berkala untuk meminimalkan risiko yang dapat terjadi, seperti modifikasi *software, coding error,* tidak *update antivirus,* kesalahan konfigurasi sehingga *software error,* tidak dapat membaca file-file tertentu, terkena virus, akibatnya transaksi tidak dapat dilakukan, dan untuk menghindari dari risiko operasional pada bank.

Pada *software Front End* S1, yaitu dengan melakukan

maintenance dengan pihak *vendor* dan *mainternance update antivirus* secara berkala untuk meminimalkan risiko yang dapat terjadi seperti modifikasi *software, coding error,* tidak *update antivirus,* kesalahan konfigurasi sehingga *software error,* tidak dapat membaca file-file tertentu, terkena virus, akibatnya transaksi tidak dapat dilakukan, dan untuk menghindari dari risiko operasional pada bank.

Pada aplikasi S1 Phase I, yaitu dengan melakukan *maintenance* dengan pihak *vendor* dan *mainternance update antivirus* secara berkala untuk meminimalkan risiko yang dapat terjadi seperti modifikasi *software, coding error,* tidak *update antivirus,* kesalahan konfigurasi sehingga *software error,* tidak dapat membaca file-file tertentu, terkena virus, akibatnya transaksi tidak dapat dilakukan, dan untuk menghindari dari risiko operasional pada bank.

Pada *Switching software,* yaitu dengan melakukan *maintenance* dengan pihak *vendor* dan *mainternance update antivirus* secara berkala untuk meminimalkan risiko yang dapat terjadi seperti modifikasi *software, coding error,* tidak *update antivirus,* kesalahan konfigurasi sehingga *software error,* tidak dapat membaca file-file tertentu, terkena virus, akibatnya transaksi tidak dapat dilakukan, dan untuk menghindari dari risiko operasional pada bank.

Pada *software Update* ICS Oracle, yaitu dengan melakukan *maintenance* dengan pihak *vendor* dan *mainternance update antivirus* secara berkala untuk meminimalkan risiko yang dapat terjadi seperti modifikasi *software, coding error,* tidak *update antivirus,* kesalahan konfigurasi sehingga *software error,* tidak dapat membaca file-file tertentu, terkena virus, akibatnya transaksi tidak dapat dilakukan, dan untuk menghindari dari risiko operasional pada bank.

Pada *software Tools Management,* yaitu dengan melakukan *maintenance* dengan pihak *vendor* dan *mainternance update antivirus* secara berkala untuk meminimalkan risiko yang dapat terjadi seperti modifikasi *software, coding error,* tidak *update antivirus,* kesalahan konfigurasi sehingga *software error,* tidak dapat membaca file-file tertentu, terkena virus, akibatnya transaksi tidak dapat dilakukan, dan untuk menghindari dari risiko operasional pada bank.

Pada aset Informasi, perusahaan perlu menambahkan pengendalian yang ada pada 4 komponen. Pada Data Identitas Nasabah, yaitu dengan melakukan pengotorisasian dalam memberikan komando untuk data yang tidak boleh dicetak bila tidak diminta oleh pihak yang berwenang, untuk meminimalkan risiko yang dapat terjadi seperti staf yang kurang teliti, data tidak disimpan dengan baik sehingga Data Identitas Nasabah bocor ke pihak lain dan untuk menghindari risiko reputasi pada bank.

Pada Data Nominal Nasabah (saldo harian terakhir), yaitu dengan melakukan pengotorisasian dalam memberikan komando untuk data yang tidak boleh dicetak bila tidak diminta oleh pihak yang berwenang, untuk meminimalkan risiko yang dapat terjadi seperti staf yang kurang teliti, data tidak disimpan dengan baik, dan untuk menghindari dari risiko reputasi pada bank.

Pada *Password* dan *Username Staf,* yaitu dengan melakukan pergantian *password* setiap staf diganti dan setiap 1 bulan 1 kali untuk meminimalkan risiko yang dapat terjadi seperti *password* tidak diubah untuk waktu yang lama sehingga terjadi penyalahgunaan *password* dan *username*, dan untuk menghindari dari risiko operasional pada bank.

Pada Data Transaksional Harian, yaitu dengan melakukan pengotorisasian dalam memberikan komando untuk data yang tidak boleh dicetak bila tidak diminta oleh pihak yang berwenang, untuk meminimalkan risiko yang dapat terjadi seperti data hilang atau dicuri, dan untuk menghindari dari risiko strategis, risiko kepatuhan, dan risiko hukum pada bank.

Pada aset SDM, perusahaan perlu menambahkan pengendalian yang ada pada 3 komponen. Pada *Teller,* yaitu dengan memberikan pengembangan kemampuan bagi staf untuk meminimalkan risiko yang dapat terjadi seperti staf mengundurkan diri dari perusahaan, menyalahgunakan *password* dan *username* untuk mencuri aset perusahaan, sering absen, mogok kerja, tidak masuk kerja sehingga data-data penting bank hilang atau dicuri oleh staf, dan untuk menghindari dari risiko operasional dan risiko hukum pada bank.

Pada *Customer Service* (CS), yaitu dengan memberikan pengembangan kemampuan bagi staf berupa pelatihan untuk meminimalkan risiko yang dapat terjadi seperti memberikan informasi yang salah kepada nasabah baru, staf mengundurkan diri, sering absen, mogok kerja, tidak masuk kerja sehingga data-data penting bank hilang atau dicuri oleh staf, dan untuk menghindari dari risiko operasional dan risiko hukum pada bank.

Pada staf TI (termasuk Kepala Grup TI, Kepala Divisi Sistem *Engineering*, Kepala Divisi *Software Engineering*), yaitu dengan memberikan pengembangan kemampuan bagi staf berupa pelatihan untuk meminimalkan risiko yang dapat terjadi, seperti memberikan informasi yang salah kepada nasabah baru, staf mengundurkan diri, sering absen, mogok kerja, tidak masuk kerja sehingga data-data penting bank hilang atau dicuri oleh staf, dan untuk menghindari risiko operasional dan risiko hukum pada bank.

SIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan, simpulan yang dapat diambil adalah perusahaan belum pernah melakukan pengukuran risiko TI dan setelah dilakukan identifikasi risiko, terdapat beberapa pengendalian yang perlu ditingkatkan sehingga risiko perusahaan dapat diminimalkan. Selain itu, divisi TI perusahaan belum melakukan pencatatan mengenai risiko-risiko yang terjadi setiap tahunnya sehingga tidak diketahui aset-aset apa saja yang risikonya tinggi. Oleh karena itu, disarankan agar (1) divisi TI perlu melakukan pencatatan data mengenai risiko-risiko yang terjadi setiap tahunnya agar dapat digunakan oleh pihak manajemen dalam membuat keputusan dan rencana strategis perusahaan dalam bidang TI; (2) perusahaan melakukan peningkatan pengendalian agar risiko TI dapat diminimalkan; dan (3) karena penelitian ini terbatas pada studi kasus, maka perlu dilakukan penelitian dengan mengambil beberapa sampel tambahan perusahaan yang bergerak di sektor perbankan di Indonesia sehingga gambaran mengenai manajemen risiko TI perbankan di Indonesia dapat diperoleh.

DAFTAR PUSTAKA

Anthony, R. (2008). *Mengenal perbankan Indonesia*. Diakses 25 November 2008, dari http://hukum-perbankan.blogspot.com.

Bank Indonesia. (2007). *Pedoman penerapan manajemen risiko dalam penggunaan teknologi informasi oleh bank umum*. Lampiran Surat Edaran Bank Indonesia Nomor 9/30/DPNP Tanggal 12 Desember 2007.

Batuparan, D.S. (2008). *Kerangka kerja risk management*. Diakses 25 November 2008, dari http://www.bexi.co.id.

Djojosoedarso, S. (2003). *Prinsip-prinsip manajemen risiko dan asuransi*, Jakarta: Salemba Empat.

Indrajit, R.E. (2000). *Manajemen sistem informasi dan teknologi informasi*. Jakarta: Gramedia Pustaka Utama.

Laudon, K.C., dan Laudon, J.P. (2008). *Sistem informasi manajemen #1: Mengelola perusahaan digital*, edisi kesepuluh, Jakarta: Salemba Empat.

O'Brein, J.A. (2005). *Pengantar sistem informasi*, edisi keduabelas, Jakarta: Salemba Empat.

Peltier, T.R. (2001). *Information security risk analysis*, 2nd ed., USA: CRC Press.

Prihanto, H. (2003). *Membangun jaringan komputer: Mengenal hardware dan topologi jaringan*, Jakarta: ilmu komputer.com.