AUDIT KEAMANAN INFORMASI PADA PT. BANK RAKYAT INDONESIA (PERSERO) Tbk. UNIT SUKOMORO

Onky Prima Wibowo[1)] **Haryanto Tanuwijaya**[2)] **Erwin Sutomo**[3)]
Program Studi/JurusanSistemInformasi
STMIK STIKOM Surabaya
Jl. Raya KedungBaruk 98 Surabaya, 60298
Email : 1)onkyprimawibowo@gmail.com, 2)haryanto@stikom.edu, 3)sutomo@stikom.edu

Abstract: PT. Bank Rakyat Indonesia (persero) Tbk. Unit Sukomoro have applied information technology. When applied information technology occured several problem. There are no specific external audit of information security until now. This research is devoted to information security that include asset security procedurs, physical and environmental security procedures, information technology operational security procedure, and incident handling procedures in information security. This research uses Bank Indonesia regulation that is Surat Edaran Bank Indonesia nomor 9/30/DPNP on 12 December 2007 about Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi oleh Bank Umum. This result from research is recommendation based audit about information security. Recommendation from the research is useful to improve banking services to satisfy bank costumers.

Keywords: Information Security Audit, Information Security, Bank Indonesia Regulation.

PT. Bank Rakyat Indonesia (Persero) Tbk. berada dibawah Bank Indonesia dimana semua Kantor dari PT. Bank Rakyat Indonesia (Persero) Tbk. tersebut wajib memenuhi peraturan dari Bank Indonesia terutama dalam hal keamanan informasi. Keamanan Informasi penting karena menurut Direktorat Penelitian dan Pengaturan Perbankan (2007) kebocoran, kerusakan, ketidakakuratan, ketidaktersediaan atau gangguan lain terhadap informasi tersebut dapat menimbulkan dampak yang merugikan baik secara finansial maupun non-finansial bagi bank. Kantor Unit Sukomoro memenuhi peraturan keamanan informasi dari Bank Indonesia untuk memberikan jaminan keamanan kepada nasabah. Saat ini belum ada audit eksternal yang spesifik mengenai keamanan informasi pada Kantor Unit Sukomoro. Selama ini audit eksternal dari Bank Indonesia untuk Kantor Unit dari PT. Bank Rakyat Indonesia (Persero) Tbk. seluruh Indonesia dilakukan dengan mengambil *sampling*. Kantor Unit Sukomoro belum pernah menjadi *sampling* dari Bank Indonesia sehingga Kantor Unit Sukomoro perlu untuk mengetahui sejauh mana keamanan informasi yang diterapkan telah memenuhi peraturan Bank Indonesia. Untuk mengetahui tingkat keamanan informasi tersebut diperlukan audit keamanan informasi.

Audit keamanan informasi pada PT. Bank Rakyat Indonesia (Persero) Tbk. Unit Sukomoro menggunakan regulasi yang berlaku saat ini yaitu Surat Edaran Bank Indonesia Nomor 9/30/DPNP tanggal 12 Desember 2007. Dalam audit ini akan dibandingkan kesesuaiannya antara operasional dengan peraturan dari Bank Indonesia. Sesuai dengan Rahardjo (2005) yang menyatakan bahwa masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Audit Keamanan Informasi ini menggunakan penerapan manajemen risiko yang bertujuan untuk meminimalkan risiko yang dapat menggagalkan visi dan misi dari bank. Dalam penelitian ini juga menggunakan referensi ISO 27002 untuk membantu dalam hal pengecekan terutama dalam hal kontrol keamanannya. Pada ISO 27002 kontrol keamanan yang diperiksa cukup jelas sedangkan pada Surat Edaran Bank Indonesia berupa garis besarnya.

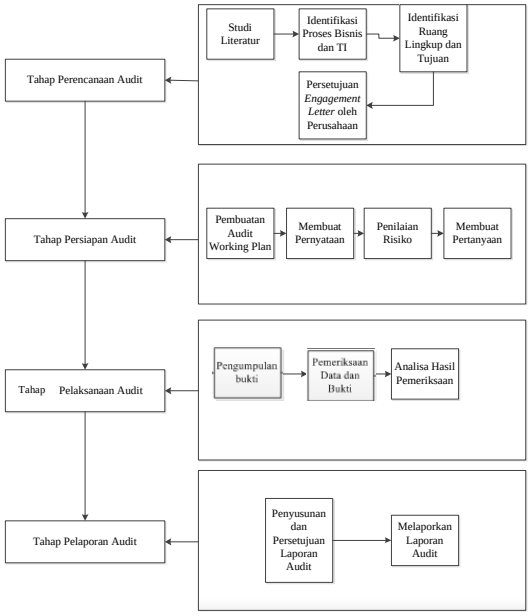
Pada audit ini terdapat dua prosedur yang tidak dapat dilakukan pada Kantor Unit Sukomoro yaitu tentang prosedur pengelolaan sumber daya manusia dan prosedur pengamanan logic. Kedua prosedur ini tidak dapat diaudit karena prosedur tersebut wewenang kantor pusat. Kantor Unit Sukomoro hanya bertindak sebagai pengguna.

Dengan adanya audit keamanan informasi yang menggunakan regulasi dari Bank Indonesia pada Kantor Unit Sukomoro ini diharapkan dapat membantu mengetahui tingkat keamanan informasi yang telah diterapkan. Hasil audit keamanan informasi ini menghasilkan

rekomendasi yang dapat digunakan untuk meningkatkan keamanan informasi pada Kantor Unit Sukomoro.

METODE

Metode penelitian yang digunakan langkah-langkah audit menurut Cannon dan Bergman (2006) yang disesuaikan dengan langkah-langkah penelitian tugas akhir, seperti terlihat pada Gambar 1.



Gambar 1.Alur Metode Penelitian

Pada metode penelitian ini terdapat empat tahapan yaitu tahap perencanaan audit, tahap persiapan audit, tahap pelaksanaan audit dan tahap pelaporan audit. Pada setiap tahapan terdapat beberapa proses yang harus dilakukan.

Pertama terdapat tahap perencanaan audit. Pada tahap perencanaan audit terdapat empat proses yang dilakukan yaitu studi literatur, identifikasi proses bisnis dan teknologi informasi, identifikasi ruang lingkup dan tujuan dan persetujuan *engagement letter* oleh perusahaan. Studi literatur ini dilakukan penulis untuk menentukan penelitian akan dikerjakan. Identifikasi proses bisnis dan teknologi informasi dilakukan untuk mengidentifikasi proses bisnis dan teknologi informasi yang terdapat di Bank Rakyat Indonesia Unit Sukomoro. Identifikasi ruang lingkup dan tujuan dilakukan untuk mengidentifikasi ruang lingkup dan tujuan dari penelitian. Persetujuan *engagement letter* oleh perusahaan untuk mempertegas hubungan antara auditor dengan perusahaan. *Engagement letter* berisi tentang poin-poin yang akan diaudit, indenpendensi (tanggung jawab) dari auditor, bukti kesepakatan dengan hal-hal yang diaudit dan kondisinya (kewenangan), menyetujui tanggal penyelesaian (akuntabilitas), sehingga menghasilkan persetujuan dari *auditee*.

Pada tahap persiapan audit terdapat empat proses yang dilakukan yaitu pembuatan *audit working plan*, membuat pernyataan, penilaian risiko dan membuat pertanyaan. Pembuatan *audit working plan* penulis membuat rancangan kerja audit dimana berisi tentang waktu dalam setiap kegiatan yang dilakukan. Hal ini dilakukan untuk membantu auditor tidak melampaui waktu yang ditentukan. Membuat pernyataan berdasarkan dari Surat Edaran Bank Indonesia Nomor 9/30/DPNP tanggal 12 Desember 2007. Pada setiap prosedur dapat ditentukan pernyataan yang menjelaskan implementasi dan kontrol yang dilakukan. Contoh dari membuat pernyataan dari prosedur pengelolaan aset yaitu "Aset Bank yang terkait dengan informasi harus diidentifikasikan, ditentukan pemilik /penanggungjawabnya dan dicatat agar dapat dilindungi secara tepat." dari prosedur ini menghasilkan pernyataan yaitu terdapat "kepemilikan/penanggung jawab aset informasi". Penilaian risiko untuk melakukan penilaian risiko adalah dengan membuat risk register. Membuat pertanyaan berdasarkan dari pernyataan yang telah dibuat berdasarkan analisis kerawanan dari penilaian risiko. Dalam satu pernyataan dapat memiliki lebih dari satu pertanyaan karena setiap pertanyaan harus mewakili pertanyaan pada saat dilakukan wawancara, dan observasi.

Pada tahap pelaksanaan audit terdapat tiga proses yang dilakukan yaitu pengumpulan bukti, pemeriksaan data dan bukti dan analisis pemeriksaan. Pengumpulan bukti dengan cara melakukan wawancara dan observasi, pemeriksaan data dan bukti penyusunan antara bukti wawancara dengan bukti observasi agar menjadi kesatuan yang utuh, sehingga memudahkan saat langkah selanjutnya melakukan analisis hasil pemeriksaan, dan analisis pemeriksaan.

Pada tahap pelaporan audit terdapat dua proses yang dilakukan yaitu penyusunan dan persetujuan laporan audit dan melaporkan laporan audit.

HASIL DAN PEMBAHASAN

Berdasarkan metode di depan penelitian ini melalui empat tahapan yaitu tahap perencanaan, tahap persiapan, tahap pelaksanaan dan tahap pelaporan. Keempat tahap tersebut telah selesai dikerjakan.

Tahap perencanaan

Tahap ini terdiri dari empat proses yaitu studi literatur, identifikasi proses bisnis dan teknologi, identifikasi ruang lingkup dan tujuan, dan persetujuan *engagement letter*. Proses pertama adalah studi literatur dengan melakukan studi literatur untuk menambah literasi tentang audit, keamanan informasi, Surat Edaran Bank Indonesia Nomor 9/30/DPNP tanggal 12 Desember 2007 dan ISO 27002. Proses selanjutnya yaitu identifikasi proses bisnis dan teknologi informasi yang menghasilkan visi dari PT. Bank Rakyat Indonesia (persero) Tbk. yang ingin menjadi bank komersial terkemuka dengana mengutamakan kepuasan nasabah oleh karena itu kenyamanan dan kepuasan nasbah sangat penting.

Proses ketiga adalah menentukan ruang lingkup dan tujuan audit. Ruang lingkup audit yang digunakan adalah tentang prosedur pengamanan aset, prosedur pengamanan fisik dan lingkungan, prosedur keamanan operasional teknologi informasi, dan prosedur penanganan insiden keamanan informasi. Prosedur sumber daya manusia dan prosedur pengamanan *logic* tidak digunakan karena kedua prosedur tersebut merupakan wewenang kantor pusat. Setelah keamanan informasi menjadi fokus dari penelitian ini maka perlu dilihat bagaimana struktur organisasinya dan tujuan dari audit tersebut. Proses keempat adalah persetujuan *engagement* sebagai kontrak pengikat antara auditor dengan perusahaan. *Engagement letter* yang disetujui oleh perusahaan menjadi kunci utama untuk melaksanakan audit pada perusahaan.

Tahap persiapan

Setelah *engagement letter* disetujui oleh perusahaan maka auditor dapat segera melakukan persiapan audit. Dalam penelitian yang berfokus pada keamanan informasi ini tahap persiapan audit dibagi empat proses yaitu pembuatan *audit working plan,* pembuatan pernyataan, penilaian risiko dan membuat pertanyaan. Proses pertama pada tahap persiapan adalah membuat *audit working plan* yang berguna untuk mengatur waktu seorang auditor dalam melaksanakan dan menyelesaikan audit tepat waktu terlihat pada Tabel 1.

Tabel 1. *Audit Working Plan*

No	Pekerjaan	Auditor	Estimasi Waktu (hari)	Realisasi (hari)	Minggu 01	02	03	04	05	06	07	08	09	10	11	12	13	14	15
1	Perencanaan Audit	Onky P. W	9																
	Identifikasi Proses Bisnis dan Teknologi Informasi		2																
	Identifikasi Ruang Lingkup dan Tujuan		2																
	Persetujuan Engagement Letter oleh Perusahaan		4																
2	Persiapan Audit	Onky P. W	20																
	Membuat Audit Working Plan		4																
	Membuat Pernyataan		4																
	Penilaian Risiko		4																
	Membuat Pertanyaan		4																
3	Pelaksanaan Audit	Onky P. W	20																
	Pemeriksaan Data dan Bukti		8																
	Pengumpulan Bukti		4																
	Analisa Hasil Pemeriksaan		8																
4	Pelaporan Audit	Onky P. W	10																
	Penyusunan dan Persetujuan Laporan Audit		8																
	Melaporkan Laporan Audit		2																

Proses selanjutnya dalam tahap persiapan audit adalah membuat pernyataan, pernyataan yang dibuat berdasarkan pedoman yang sudah ada dalam lampiran Surat Edaran Bank Indonesia Nomor 9/30/DPNP tanggal 12 Desember 2007. Langkah selanjutnya adalah membuat penilaian risiko. Penilaian risiko merupakan sesuatu yang utama dalam penelitian ini. Penilaian risiko dalam penelitian ini menggunakan pendekatan aset sehingga identifikasi risiko pengamanan informasi dilakukan dengan melihat klasifikasi terhadap aset. Pada analisis aset, aset diklasifikasikan dengan memperhatikan *confidentiality* (kerahasiaan), *integrity* (kelengkapan) dan *availability* (ketersediaan). Analisis aset yang telah dilakukan menghasilkan daftar aset seperti pada Tabel 2.

Tabel 2. Daftar Aset

No.	ASET
1.	Berkas pinjaman berupa *hardcopy*
2.	Berkas simpanan berupa *hardcopy*
3.	Server
4.	*Uninteruptible Power Supply* (UPS)
5.	*Air Conditioner* (dalam ruang server)
6.	Brankas Tanam
7.	Clash Anti Api
8.	Lemari besi anti api

Lanjutan Tabel 2.

No.	ASET
9.	Parabola BRINET
10.	Bukti transaksi harian berupa *hardcopy*
11.	Aplikasi BRINET
12.	Aplikasi BRIVA
13.	Aplikasi LAS
14.	Printer pasbook
15.	Brankas jinjing
16.	Laporan transaksi harian berupa *hardcopy*
17.	Laporan transaksi harian berupa *softcopy*
18.	Informasi pinjaman nasabah berupa *softcopy*
19.	Informasi simpanan nasabah berupa *softcopy*
20.	Mesin ATM (Anjungan Tunai Mandiri)

21.	Printer laser
22.	Hardisk eksternal
23.	Genset
24.	Close Circuit Television (CCTV)
25.	Personal Computer (PC)
26.	Parabola ATM
27.	Printer Inkjet
28.	Tabung pemadam

Setelah penentuan aset langkah selanjutnya adalah penentuan risiko yang dapat terjadi bila tidak ada pengendalian risiko terhadap aset tersebut. Setiap deskripsi risiko ditentukan analisis kerawanannya. Setelah analisis kerawanan dilakukan penilaian inheren diberikan pada setiap deskripsi risiko. Penilaian inheren terdiri dari kecenderungan, dampak dan Nilai Risiko Dasar (NRD) seperti pada Tabel 3.

Tabel 3. Penilaian Inheren

No. Aset	Deskripsi Risiko		Inheren		
			Kecenderungan	Dampak	Nilai Risiko Dasar
1.	1.1.	Kebocoran data berkas pinjaman	3	4	High
	1.2.	Berkas pinjaman hilang	4	4	High
	1.3.	Berkas pinjaman rusak	4	4	High
2.	2.1.	Pencurian data berkas simpanan	4	4	High
	2.2.	Berkas simpanan hilang	4	4	High
	2.3.	Berkas simpanan rusak	4	4	High
3.	3.1.	Server rusak	5	5	High
	3.2.	Server hilang	5	5	High
	3.3.	Data server hilang tidak dapat dipulihkan	5	5	High
4.	4.1	UPS rusak	4	5	High
	4.2	UPS hilang	4	4	High
5.	5.1.	AC rusak	4	4	High
	5.2.	AC hilang	4	4	High
6.	6.1.	Brankas tanam rusak	5	4	High
7.	7.1.	Clash anti api rusak	3	5	High
8.	8.1	Lemari besi rusak	3	4	High
9.	9.1.	Parabola rusak	3	3	Medium
	9.2.	Parabola hilang	4	3	High
10.	10.1.	Bukti transaksi harian hilang	5	5	High
	10.2.	Bukti transaksi harian bocor kepada pihak tidak	5	5	High
	10.3.	Bukti transaksi harian rusak	5	5	High
11.	11.1.	Kerusakan aplikasi	4	4	High
12.	12.1.	Kerusakan aplikasi	4	4	High
13.	13.1	Kerusakan aplikasi	4	4	High
14.	14.1	Printer rusak	5	4	High
	14.2	Printer hilang	5	4	High
15.	15.1.	Brankas jinjing rusak	3	4	High
	15.2.	Brankas jining hilang	3	4	High
16.	16.1.	Laporan transaksi harian bocor kepada pihak tidak berwenang	5	5	High
	16.2.	Laporan transaksi harian hilang	5	5	High
	16.3.	Laporan transaksi harian rusak	5	5	High
17.	17.1.	Laporan transaksi harian bocor	5	5	High
	17.2.	Laporan transaksi harian rusak	5	5	High
	17.3.	Laporan transaksi harian hilang	5	5	High
18.	18.1.	informasi Pinjaman nasabah bocor	4	4	High
	18.2.	informasi Pinjaman nasabahrusak	4	4	High
	18.3.	informasi pinjaman nasabah hilang	4	4	High

Lanjutan Tabel 3.

No. Aset	Deskripsi Risiko		Inheren		
			Kecenderungan	Dampak	Nilai Risiko Dasar
19.	19.1.	informasi simpanan nasabah bocor	4	4	High
	19.2.	informasi simpanan nasabah rusak	4	3	High
	19.3.	informasi simpanan nasabah hilang	4	4	High
20.	20.1.	Mesin ATM rusak	4	5	High
	20.2.	Mesin ATM hilang	4	4	High
21.	21.1.	Printer rusak.	5	4	High
	21.2	Printer hilang	5	4	High
22.	22.1.	Hardisk eksternal rusak	5	4	High
	22.2.	Hardisk eksternal hilang	5	5	High
23.	23.1.	Genset rusak	4	3	High
	23.2.	Genset hilang	4	3	High
24.	24.1.	CCTV rusak	3	3	Medium
	24.2.	CCTV hilang	4	3	High
25.	25.1.	PC rusak	4	5	High
	25.2.	PC hilang	4	5	High
	25.3.	PC terserang virus	4	5	High
	25.4.	PC diakses oleh pihak tidak berwenang	4	5	High
26.	26.1.	Parabola rusak	2	3	Medium
	26.2.	Parabola hilang	4	3	High
27.	27.1.	Printer rusak	4	3	High
	27.2.	Printer hilang	5	3	High
28.	28.1.	Tabung pemadam rusak	3	3	Medium
	28.2.	Tabung pemadam hilang	3	3	Medium

Setelah ditentukan penentuan NRD langkah selanjutnya adalah menentukan nilai risiko yang diharapkan. Nilai risiko yang diharapkan diisi berdasarkan keinginan dari perusahaan seberapa ingin mereka mengharapkan keamanan terhadap aset informasi mereka. Nilai risiko yang diharapkan diisi dengan nilai *Low*, *Medium* dan *High.*

Proses selanjutnya adalah membuat pertanyaan dalam membuat pertanyaan satu pernyataan dapat memiliki banyak pertanyaan yang bertujuan untuk mengetahui secara jelas apakah dari setiap pernyataan tersebut telah diimplementasikan dengan baik.

Tahap pelaksanaan

Pada tahap ini dibagi tiga proses yaitu pengumpulan bukti, pemeriksaan data dan bukti dan analisis hasil pemeriksaan. Dalam proses pengumpulan bukti dilakukan dengan cara observasi dan wawancara. Observasi dilakukan terhadap lingkungan perusahaan dan kegiatan operasional pada perusahaan. Proses selanjutnya melakukan wawancara dalam penelitian ini wawancara dilakukan kepada Kepala Unit. Proses selanjutnya adalah proses analisis yang berdasarkan hasil dari observasi dan wawancara yang telah didapat. Hasil dari analisis menjadi dasar untuk mengisi kecenderungan residu dan dampak residu dan Nilai Risiko Akhir (NRA). Penilaian residu akan menjadi dasar *auditor* dalam memberikan rekomendasi kepada bank. Penilaian residu dapat dilihat pada Tabel 4.

Tabel 4. Penilaian Residu

Nomor Aset	Deskripsi Risiko	Inheren		
		Kecenderungan	Dampak	Nilai Risiko Akhir
1.	1.1.	2	2	Low
	1.2.	2	2	Low
	1.3.	2	2	Low
2.	2.1.	2	3	Medium
	2.2.	2	2	Low
	2.3.	2	2	Low
3.	3.1.	2	3	Medium
	3.2.	3	2	Low
	3.3.	2	2	Low
4.	4.1	2	2	Low

	4.2	2	3	Medium
5.	5.1.	2	3	Medium
	5.2.	2	1	Low
6.	6.1.	1	2	Low
7.	7.1.	1	1	Low
8.	8.1	1	2	Low
9.	9.1.	2	2	Low
	9.2.	1	1	Low
10.	10.1.	2	2	Low
	10.2.	2	2	Low
	10.3.	2	2	Low
11.	11.1.	2	2	Low
12.	12.1.	2	2	Low
13.	13.1	2	2	Low
14.	14.1	3	2	Low
	14.2	1	2	Low
15.	15.1.	2	2	Low
	15.2.	2	2	Low
16.	16.1.	2	2	Low
	16.2.	2	2	Low
	16.3.	2	2	Low
17.	17.1.	2	2	Low
	17.2.	2	2	Low
	17.3.	2	1	Low
18.	18.1.	2	1	Low
	18.2.	2	2	Low
	18.3.	2	1	Low
19.	19.1.	2	1	Low
	19.2.	2	2	Low
	19.3.	2	1	Low
20.	20.1.	2	2	Low
	20.2.	1	2	Low
21.	21.1.	3	2	Low
	21.2	1	2	Low
22.	22.1.	2	1	Low
	22.2.	2	1	Low
23.	23.1.	2	3	Medium
	23.2.	2	1	Low
24.	24.1.	1	1	Low
	24.2.	2	2	Low
25.	25.1.	2	2	Low
	25.2.	2	2	Low
	25.3.	2	2	Low
	25.4.	2	2	Low
26.	26.1.	1	2	Low
	26.2.	2	1	Low
27.	27.1.	1	2	Low
	27.2.	2	2	Low
28.	28.1.	1	2	Low
	28.2.	2	1	Low

Tahap pelaporan

Pada tahap ini terdapat dua proses yaitu penyusunan dan persetujuan laporan audit dan melaporkan laporan audit. Dalam menyusun laporan audit dilakukan pemberian rekomendasi yang berdasarkan penilaian residu yang telah diperoleh dari risk register contohnya nilai risiko akhir dari berkas pinjaman berupa hardcopy telah mencapai level *low* tetapi nilai yang diperoleh belum maksimal karena nilai yang diperoleh masih dua, maka masih belum maksimal dalam pengamanan informasinya. Penilaian yang belum mencapai hasil maksimal dikarenakan tidak terdapatnya dokumentasi prosedur dan kebijakan yang dimiliki oleh bank. Dari hasil analisis yang berdasarkan oleh *risk register* diperoleh hasil bahwa terdapat lima aset yang masih berada di posisi level *medium* diantaranya antara lain adalah berkas simpanan berupa *hardcopy*, *server*, *Utility Power Supply*, *air conditioner* dan generator set. Selain lima perangkat ini sudah mencapai level *low*, namun belum mencapai nilai satu sehingga masih terdapat kerkurangan yang harus segera dipenuhi supaya keamanan dan kenyamanan masyarakat dalam bertransaksi di bank menjadi lebih terjamin.

Setelah laporan audit disetujui oleh perusahaan. Proses selanjutnya adalah melaporkan laporan audit yang telah dilakukan. Setelah dilakukan pelaporan laporan audit dan diterima oleh pihak bank maka audit telah dianggap selesai.

Setelah empat tahapan dilakukan selanjutnya membuat rekomendasi terhadap keamanan informasi PT. Bank Rakyat Indonesia (persero) Tbk. Unit Sukomoro. Berdasarkan analisis dari *risk register* maka diperoleh rekomendasi pada beberapa pengendalian yang harus ditingkatkan oleh perusahaan diantaranya aset data, perlu penambahan pengendalian keamanan untuk tiga komponen yang ada yaitu,

1. Bukti transaksi harian *berupa hardcopy* yaitu dengan melakukan pembatasan hak akses tempat penyimpanan bukti transaksi, sehingga hanya orang yang berkepentingan saja yang dapat mengakses.
2. Pada laporan transaksi harian *berupa hardcopy* yaitu dengan melakukan penyimpanan pada *odner* sehingga lebih memudahkan saat pencarian dan melakukan pembatasan hak akses tempat penyimpanan laporan transaksi harian, sehingga hanya orang yang berkepentingan saja yang dapat mengakses.
3. Berkas simpanan *berupa hardcopy* yaitu dengan melakukan pembatasan hak akses tempat penyimpanan bukti transaksi, sehingga hanya orang yang berkepentingan saja yang dapat mengakses. Pengendalian keamanan ini dilakukan untuk menghindari risiko reputasi pada bank.

Pada aset perangkat keras, perlu penambahan pengendalian keamanan untuk tiga komponen yaitu,

1. server yaitu perlu adanya *maintenance* secara periodik 1 bulan 1 kali untuk mengurangi risiko terjadinya pengguna tidak dapat mengakses pada portal dan perlu adanya prosedur kebersihan peralatan akses informasi untuk membantu kantor unit dalam melakukan perawatan kebersihan server.
2. *Personal computer*, perlu adanya *maintenance* secara periodik 1 bulan 1 kali

untuk mengurangi risiko *personal computer* rusak saat pelayanan nasabah.

3. *ATM*, yaitu perlu adanya tabung pemadam. Tabung pemadam untuk membantu mematikan api jika terjadi kebakaran pada ATM karena letak ATM yang ada di bagian luar kantor.

Pengendalian keamanan ini dilakukan untuk menghindari risiko operasional dan reputasi pada bank.

Pada aset perangkat pendukung, perlu penambahan pengendalian keamanan untuk tiga komponen.

1. UPS yaitu dengan melakukan *maintenance* secara periodik 1 bulan 1 kali untuk meminimalkan terjadinya risiko yang dapat terjadi seperti UPS tidak berfungsi akibatnya saat listrik padam, server-pun mati sehingga pelayanan transaksi nasabah tidak dapat dilakukan.
2. AC pada ruangan *server* yaitu dengan melakukan *maintenance* secara periodik 1 bulan 1 kali untuk meminimalkan terjadinya risiko yang dapat terjadi seperti AC mati karena listrik padam/ tidak di*maintenance* (sehingga server menjadi panas).
3. Genset yaitu dengan melakukan *maintenance* secara periodik 1 bulan 1 kali untuk meminimalkan terjadinya risiko yang dapat terjadi seperti genset tidak berfungsi saat listrik padam (sehingga seluruh peralatan pemrosesan informasi mati).

SIMPULAN

Berdasarkan hasil audit keamanan sistem informasi yang telah dilakukan maka didapat kesimpulan berupa:

1. Nilai Risiko Akhir (NRA) keamanan informasi di PT. Bank Rakyat Indonesia (persero) Tbk. Unit Sukomoro 23 aset mencapai level *low* (82%), hanya 5 aset mencapai level *medium* (18%) sedangkan yang mencapai level *high* tidak ada.
2. Aset yang mencapai NRA pada level *low* keseluruhan masih berada level dua sehingga perlu melengkapi dokumen-dokumen tentang prosedur dan kebijakan yang berlaku untuk dapat berubah menjadi level satu.
3. Aset yang mencapai NRA pada level *medium* masih pada level tiga sehingga perlu adanya perbaikan dalam perawatan, pemeliharan, penyimpanan dan melengkapi dokumen prosedur dan kebijakan untuk dapat berubah menjadi level satu.

RUJUKAN

Canon, David L dan Timothy S. Bergmann. 2006 . *Cisa Certified Information Systems Auditor Study Guide*. Indianapolis : Wiley Publishing,Inc.

Direktorat Penelitian dan Pengaturan Perbankan. 2007. *Pedoman Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Informasi Oleh Bank Umum*. Jakarta : Bank Indonesia

Rahardjo, Budi. 2005. *Keamanan Sistem Informasi Berbasis Internet*. Bandung: PT. Insan Indonesia

Sarno, Riyanto. 2009. *Audit Sistem & Teknologi Informasi*. Surabaya : ITSPress Surabaya

Sarno, Riyanto dan Iffano, Irsyat. 2009 . *Sistem Manajemen Keamanan Informasi*. Surabaya : ITSPress Surabaya

Tampubolon, Robert. 2005. Risk and Systems-Based Internal Audit. Jakarta : PT. Elex Media Komputindo