Kontrol Keamanan Sistem Informasi Akuntansi Bank Perkreditan Rakyat (BPR) Sumatera Barat

Sulastri
Sekolah Tinggi Ilmu Ekonomi Sumatera Barat, Padang, Indonesia
Email: ulastrisyam79@yahoo.com

Abstract

This study aims to determine the security control of accounting information systems that exist in West Sumatra Rural Banks. The study was conducted on 91 rural banks in the province of West Sumatra, but only 41 returned questionnaires. The results of the study show that the BPR has implemented the security control of the accounting information system well.

Keywords: Security control, accounting, information system.

Abstrak

Penelitian ini bertujuan untuk mengetahui kontrol keamanan sistem informasi akuntansi yang ada pada Bank Perkreditan Rakyat Sumatera Barat. Penelitian dilaksanakan pada 91 BPR yang ada di propinsi Sumatera Barat, namun hanya 41 kuisioner yang kembali. Hasil penelitian menunjukan bahwa BPR telah melaksanakan kontrol keamanan sistem informasi akuntansi dengan baik.

Kata kunci: Kontrol keamanan, sistem informasi, akuntansi.

I. PENDAHULUAN

Salah satu cara perusahaan dalam memudahkan dan menghasilkan informasi yang tepat waktu, akurat dan terpercaya adalah dengan menggunakan sistem informasi akuntansi berbasis komputer. Suatu sistem yang berbasis computer sangat diperlukan oleh perusahaan untuk membantu mereka dalam pengolahan data dan pengambilan keputusan. Sejalan dengan peningkatan kompleksitas dan ketergantungan pada sistem informasi akuntansi, perusahaan akan menghadapi peningkatan resiko atas sistem tersebut (Romney dan Paul, 2006). Tingkat pelanggaran keamanan dan penipuan transaksi meningkat dari hari ke hari, kebutuhan untuk identifikasi keamanan system informasi menjadi sangat penting terutama di sektor perbankan dan keuangan (Venkatraman dan Indika, 2008). Pentingnya mengamankan CAIS (*Computerized Accounting Information Systems*) dan pengembangan IT (*Information Technology*) untuk keberhasilan bisnis perusahaan (Musa, 2007).

Bank Perkreditan Rakyat (BPR) yang ada di propinsi Sumatera Barat telah menggunakan tekhnologi informasi dalam rangka meningkatkan efisiensi operasional dan kualitas pelayanan kepada masyarakat pengguna jasa perbankan. Hal ini diatur dalam salinan peraturan OJK nomor 75/POJK.03/2016 pasal 2 yang menyatakan bahwa BPR dan BPRS yang memiliki modal inti kurang atau paling sedikit lima puluh milliar, wajib menyelenggarakan teknologi informasi yang paling sedikit berupa aplikasi inti perbankan

Article Tract:
Submission : Februari 20, 2018
Final Review : Mei 23, 2018

dan pusat data. Hasil pemeriksaan Departemen Pengendalian Kualitas Pengawasan (BPKP) Otoritas Jasa Keuangan (OJK) tahun 2015, terdapat sejumlah masalah penerapan TIK (Teknologi Informasi Komputer) di BPR terutama aplikasi TIK yang belum selaras BI/OJK. Permasalahan tersebut berupa kurangnya kontrol aplikasi TIK, manajemen operasional dan minimnya standar operasi prosedur, kondisi staf dan infrastruktur serta maintenance.

Pertahanan dari sistem informasi sering disebut dengan pengendalian dan keamanan sistem informasi (information systems control and security) yang didefinisikan sebagai penjagaan terhadap fasilitas dan proses komputer dari gangguan-gangguan yang disengaja maupun yang insidental tidak disengaja yang dapat menyebabkan perubahan-perubahan, kerusakan-kerusakan atau pencurian-pencurian sumber-sumber daya sistem informasi secara tidak sah (Jogiyanto, 2003).

Keamanan sistem informasi merupakan suatu subsistem dalam suatu organisasi yang bertugas mengendalikan resiko terkait dengan sistem informasi berbasis komputer. Keamanan sistem informasi merupakan sebuah aplikasi prinsip-prinsip pengendalian internal yang secara khusus digunakan untuk mengatasi masalah-masalah dalam sistem informasi (Bodnar dan William, 2004).

Bodnar dan William (2004) menyatakan ada enam metode yang dapat digunakan untuk melakukan kecurangan sistem informasi, yaitu : manipulasi input, mengubah program, perubahan file secara langsung, pencurian data, sabotase, dan penyalahgunaan atau pencurian sumber daya informasi. Sedangkan menurut Romney dan Paul (2006) ada empat jenis ancaman atas sistem informasi akuntansi yang dihadapi oleh perusahaan, yaitu : (1) kehancuran karena bencana alam dan politik, seperti kebakaran, banjir, gempa bumi, (2) kesalahan pada software dan tidak berfungsinya peralatan, seperti kerusakan pada software, gangguan dan fluktuasi listrik, (3) tindakan tidak disengaja, seperti hilangnya atau salah letaknya data, (4) tindakan sengaja (kejahatan komputer), seperti sabotase, penipuan melalui komputer, pencurian.

Kategori pengendalian secara umum atas sistem menurut Boockholdt (1999) adalah; (a) pengendalian pusat data operasi, (b) pengendalian perolehan sistem software dan pemeliharaan, (c) pengendalian keamanan akses, (d) pengendalian pengembangan sistem aplikasi dan pemeliharaan.

Bawaneh (2014) mengemukakan bahwa bank-bank dalam melindungi diri terhadap penipuan komputer, merumuskan prosedur pengendalian berhubungan dengan kontrol input, control pengolahan, kontrol output, dan keamanan fisik. Selanjutnya, bank dan akuntan dalam praktek mereka menyesuaikan beberapa metode untuk menggagalkan (mitigasi) kejahatan komputer, pelanggaran, dan penipuan. Menilai langkah-langkah keamanan dan melindungi password, menerapkan kontrol yang didasarkan pada kepercayaan bahwa kebanyakan kejahatan computer dan penyalahgunaan berhasil karena tidak adanya kontrol.

Otoritas Jasa Keuangan dalam salinan peraturan OJK nomor 75/POJK.03/2016 tentang Standar Penyelenggaraan Tekhnologi Informasi bagi Bank Perkreditan Rakyat dan Bank Pembiayaan Rakyat Syariah mengatur tentang pengamanan penyelenggaraan tekhnologi informasi yang dituangkan dalam pasal 20, yaitu :

a. BPR dan BPRS wajib menerapkan upaya pengamanan yang diperlukan untuk mencegah gangguan keamanan dalam penyelenggaraan Teknologi Informasi yang berpotensi merugikan BPR, BPRS dan/atau nasabahnya.
b. Dalam rangka menerapkan upaya pengamanan sebagaimana dimaksud pada ayat (1), BPR dan BPRS wajib menjaga kerahasiaan *(confidentiality)*, integritas *(integrity)*,

ketersediaan *(availability)*, dan dapat ditelusurinya suatu informasi elektronik dan/atau dokumen elektronik yang terkait dengan nasabah dan seluruh aktivitas BPR atau BPRS sesuai dengan ketentuan peraturan perundang-undangan.

c. BPR dan BPRS wajib melakukan pengendalian otorisasi *(authorization of control)* dalam penyelenggaraan Teknologi Informasi.

II. METODE PENELITIAN

Penelitian ini dilakukan dengan teknik wawancara dan kuesioner, dimana responden dalam penelitian ini adalah Pejabat Eksekutif/ Internal Audit/ Petugas pengguna aplikasi sistem informasi akuntansi yang bekerja pada Bank Perkreditan Rakyat yang ada di propinsi Sumatera Barat terdiri dari 91 BPR (berdasarkan data statistik Bank Indonesia tahun 2016). Namun dalam penelitian ini data yang berhasil dikumpulkan hanya 41 BPR saja.

Kontrol keamanan sistem informasi akuntansi diukur menggunakan indikator yang diambil dari penelitian Abu Musa (2006) yang dilihat dari 6 (enam) aspek keamanan dan diajukan dengan 14 (empat belas) item pertanyaan. Keenam aspek tersebut terdiri dari ;

1. Kontrol Keamanan Organisasi
2. Kontrol Keamanan Hardware dan Akses Fisik
3. Kontrol Keamanan Software dan Keamanan Akses
4. Kontrol keamanan Data dan integritas
5. Pembagian Tugas
6. Kontrol keamanan output

III. HASIL PENELITIAN

Saaat ini kontrol keamanan sistem informasi akuntansi yang ada pada bank perkreditan rakyat di Sumatera Barat telah dilakukan dengan baik. Hal ini dapat kita lihat dari enam (6) aspek penilaian kontrol keamanan sistem informasi yang telah dilaksanakan pada Bank Perkreditan Rakyat di Sumatera Barat.

1. Kontrol Keamanan Organisasi

Dalam hal ini BPR yang ada di propinsi Sumatera Barat 81% telah melaksanakan rotasi karyawan yang nantinya dapat digunakan untuk melihat penyimpangan-penyimpangan yang ada. Liburan wajib karyawan juga telah menjadi hal penting yang telah dilakukan oleh BPR. Hanya 27% BPR saja yang masih belum melaksanakan liburan wajib ini karena masih minimnya jumlah karyawan. Liburan ini nantinya akan mampu memberikan peluang untuk melihat kinerja dari karyawan yang bersangkutan dan dapat juga digunakan untuk melihat kesalahan-kesalahan yang mungkin terjadi selama karyawan tersebut melaksanakan pekerjaanya.

2. Kontrol Keamanan Hardware dan Akses Fisik

BPR yang telah melaksanakan pengawasan terhadap instalasi komputernya sebesar 76% dari 41 BPR. Hal ini membuktikan bahwa umumnya BPR telah menyadari pengamanan tersebut sebagai suatu hal yang penting. Sebanyak 93% BPR telah melaksanakan pembatasan akses komputernya. Seperti yang kita ketahui bahwa pembatasan akses komputer merupakan hal yang dapat mengurangi kesalahan atau kerusakan yang mungkin akan terjadi. Jika akses komputer ini tidak dibatasi, maka akan

membahayakan data-data penting yang ada dalam komputer dan sulitnya menelusuri siapa yang bertanggungjawab terhadap kerusakan atau kesalahn tersebut.

Kesadaran untuk menyediakan alat pemadam kebakaran juga cukup besar (88%). Alat pemadam kebakaran seharusnya diletakkan di tempat yang mudah dijangkau sehingga apabila terjadi kebakaran segera dapat di gunakan. Polusi disekitar hardware juga telah cukup diperhatikan oleh BPR di Sumatera Barat dengan menerapkan aturan untuk tidak merokok atau larangan lainnya yang dianggap akan menjadi hal-hal yang akan merusak hardware.

3. Kontrol Keamanan Software dan Keamanan Akses

Dalam penggunaan komputer sebagai alat dalam menghasilkan laporan keuangan, BPR telah menggunakan anti virus untuk mencegah terjadinya kehilangan atau data error. Sekitar 90% BPR telah menggunakannya dan selalu melakukan update terhadap anti virus yang mereka gunakan. Selain itu untuk menjaga keamanan akses, 98% BPR yang ada telah melaksanakan penggantian password secara berkala guna mencegah adanya kebocoran password. Kebocoran password akan memudahkan pihak yang tidak berwenang masuk dan mengakses data yang ada dalam sistem. Ini tentu saja akan mengakibatkan kerugian jika data itu disalah gunakan oleh pihak lain dan mengurangi tingkat kepercayaan nasabah terhadap kerahasiaan data di BPR.

4. Kontrol keamanan Data dan integritas

Untuk mengamankan data, semua BPR telah melakukan back up data harian setelah proses dalam sistem informasi akuntansinya selesai. Hal ini dilakukan untuk mencegah terjadinya kehilangan data apabila terjadi kerusakan pada aplikasi sistem informasi akuntansi BPR. Ada dua macam back up data yang dilakukan oleh BPR, yaitu back up data harian dan back up data bulanan. Back up data harian dilakukan setiap hari dan back up data bulanan dilakukan setiap akhir bulan setelah semua transaksi diproses. Selain melakukan back up data, BPR telah melakukan cetak data atau informasi yang penting yang dihasilkan dari aplikasi sistem informasi akuntansi BPR. Hasil cetakan tersebut diarsipkan dan disimpan dalam lemari terkunci.

5. Pembagian Tugas

Dalam menjalankan kegiatan usahanya, 93% Bank Perkreditan Rakyat di Sumatera Barat telah melakukan pemisahan tugas terhadap bagian-bagian pekerjaan yang sangat vital. Masing-masing karyawan memiliki tugas atau tanggung jawab yang berbeda.Ini dilakukan untuk mencegah terjadinya penyalahgunaan wewenang yang akan menimbulkan terjadinya fraud atau kecurangan.

6. Kontrol keamanan output

Output sistem informasi akuntansi yang ada dicetak oleh pihak yang berwenang saja, agar data tersebut tidak disalahgunakan oleh pihak-pihak tertentu. Output tersebut di simpan ditempat yang aman di lemari terkunci untuk menghindari pencurian data. Perbandingan terhadap hasil/output sistem informasi akuntansi tersebut sewaktu-waktu diperbandingkan dengan data input untuk memastikan informasi/output yang dihasilkan benar. Biasanya ini dilakukan rutin setiap hari untuk menghindari kondisi/keadaan hilangnya data input.

Tabel 1. Aspek Penilaian Kontrol Keamanan Sistem Informasi Akuntansi

NO	KETERANGAN	YA (%)	TIDAK (%)
1	Rotasi tugas di BPR Saudara /i digunakan untuk meningkatkan kesempatan memaparkan kesalahan dan penyimpangan	81	19
2	Liburan wajib di BPR Saudara/i dilakukan untuk mengurangi kemungkinan penipuan atau penggelapan	73	27
3	Adanya pembatasan akses komputer sistem informasi akuntansi BPR Saudara/i untuk karyawan dengan kebutuhan yang ditetapkan.	93	7
4	Instalasi komputer BPR Saudara/i hanya di daerah yang terkunci dan disimpan di bawah pengawasan ketika tidak digunakan.	76	24
5	Adanya alat pemadam kebakaran di BPR Saudara/i dan dekat dari jangkauan	88	12
6	Adanya pelaksanaan larangan merokok dan menghindari polutan potensial (misalnya; debu, makanan, dan kopi) disekitar komputer di BPR Saudara/i	83	17
7	Adanya perangkat lunak perlindungan Virus komputer BPR Saudara/i.	90	10
8	Ada prosedur yang memadai di BPR Saudara/i untuk memastikan bahwa password secara berkala berubah, disimpan rahasia, tidak mudah ditebak, dan dibatalkan untuk karyawan yang diberhentikan atau dipindahkan.	98	2
9	Adanya backup data di BPR Saudara yang disiapkan secara rutin	100	0
10	Ada hard copy yang dicetak secara rutin di BPR Saudara/i untuk data yang sangat penting	98	2
11	Pemisahan tugas akuntansi (yaitu otorisasi; pencatatan, dan hak lainnya) telah baik dan memadai di BPR Saudara/i	93	7
12	Output komputer (laporan) yang sensitif (penting) di BPR Saudara/i diamankan di lemari terkunci	90	10
13	Percetakan dan distribusi data dan informasi akuntansi yang ada di BPR Saudara/i dilakukan di bawah kontrol keamanan yang tepat, dan hanya oleh orang yang berwenang di bank	98	2
14	Perbandingan output / input sembarang di BPR Saudara/i secara teratur dilakukan untuk memverifikasi pengolahan yang benar	73	27

IV. KESIMPULAN

Penilaian terhadap kontrol keamanan sistem informasi akuntansi yang telah dilakukan memperlihatkan hasil bahwa Bank Perkreditan Rakyat di Sumatera Barat telah melaksanakan kontrol keamanan yang memadai terhadap sistem informasi akuntansinya. Keenam aspek penilaian tersebut memperlihatkan hasil yang cukup bagus dimana hampir semua BPR melaksanakan kontrol keamanan sistem informasi akuntansinya. Ini tentu saja akan menambah tingkat kepercayaan masyarakat umumnya dan nasabah BPR khususnya dalam melaksanakan aktifitas perbankan.

Selanjutnya BPR yang ada di Sumatera Barat diharapkan untuk mengoptimalkan kontrol keamanan terhadap sistem informasi akuntansinya untuk menghindari hal-hal yang tidak diinginkan. Pengamanan yang optimal akan mampu memberikan tingkat kepercayaan masyarakat yang lebih tinggi lagi terhadap Bank Perkreditan Rakyat. Ini merupakan kunci bagi keberlangsungan usaha perbankan yang di jalankan oleh Bank Perkreditan Rakyat.

DAFTAR PUSTAKA

Bawaneh, Shamsi, H. 2014. *Information Security for Organizations and Accounting Information System: A Jordan Banking Sector Case*,. International Review of Management and Business Research. Vol.3. Issue 2.

Bodnar, George, H. and Hopwood, William, S. 2004. *Accounting Information Systems*. Ninth Edition. Upper Saddle River. New Jersey 07458: Pearson Education Inc. hal 614.

Boockhold, J. L. 1999. *Accounting Information Systems*. International Editions.

Hall, James, H. and Singleton, Tommie. 2009. *Audit dan Assurance Teknologi Informasi*. Edisi 2. Salemba Empat. hal 466

Hayale, Talal, H,. dan Khadra, Husam, A, Abu. 2008. *Investigating Perceived Security Threats of Computerized Accounting Information Systems: An Empirical Research applied on Jordanian Banking Sector*. Journal of Economic & Administrative Sciences. Vol. 24. No. 1. 41-67.

Jogiyanto, 2003. *Sistem Tekhnologi Informasi*. Penerbit Andi. Yogyakarta. Hal 644.

Musa, Ahmad, A, Abu, 2004. *Investigating the security controls of CAIS in an emerging economy: An empirical study on the Egyptian banking industry*. Managerial Auditing Journal. Vol 19. No. 2. pp. 272-302.

Musa, Ahmad, A, Abu. 2006,. *Perceived security threats of computerized accounting information systems in the Egyptian Banking Industry*,. Journal Information Systems. Vol. 2. No. 1. pp. 187-203.

Musa, Ahmad, A, Abu. 2007. *Evaluating the security controls of CAIS in developing countries: An examination of current research*. Information Management & Computer Security. Vo. 15. No. 1. pp. 46-63.

Mukhtar, Ali, Masjono. 2002. *Audit Sistem Informasi.* Rineka Cipta. Jakarta.

O'Brien, James. A. 2008. *Pengantar Sistem Informasi*. Edisi 12. Salemba Empat. Jakarta. Hal 742.

Romney, Marshall, B, dan Steinbart, Paul, John. 2006. *Sistem Informasi Akuntansi*. Edisi. Salemba Empat: Jakarta. Hal 510.

Romney, Marshall, B, dan Steinbart, Paul, John. 2009. *Accounting Information Systems*. Eleventh Edition. Pearson International Edition. by Pearson Education, Inc. Upper Saddle River, New Jersey. 07458.

Salinan peraturan OJK nomor 75/POJK.03/2016 tentang *Standar Penyelenggaraan Teknologi Informasi bagi Bank Perkreditan Rakyat dan Bank Pembiayaan Rakyat Syariah.*

Taiwo, 2016. *Effect of ICT on Accounting Information System and Organisational Performance: The Application of Information and Communication Technology on Accounting Information System*,. European Journal of Business and Social Sciences. Vol. 5. No. 02. pp.01-15.

Venkatraman, Sitalakshmi dan Delpachitra, Indika. 2008. *Biometrics in banking security: a case study*. Information Management & Computer Security. Vol. 16. No. 4. pp.

415-430.

Wahyono, Teguh, 2004. *Sistem Informasi Akuntansi, Desain dan Pemrograman Komputer*. Andi Offset: Yogyakarta.

Widjajanto, Nugroho, 2001. *Sistem Informasi Akuntansi*. Penerbit Erlangga: Jakarta.

Winarno, Wing, Wahyu. 2006. *Sistem Informasi Akuntansi*. YKPN: Yogyakarta.

www.m.detik.com.27 Juni 2016 (Mahayana, Dimitri. *Tuntutan Melek TI untuk Bank Perkreditan Rakyat).*

http://www.exemplarglobalcollege.org/management-commitment/(diakses tanggal 7 April 2017).