Manajemen Risiko Teknologi Informasi Menggunakan Framework ISO 31000:2009 Studi Kasus : Pembobolan ATM BCA Tahun 2010

Anthon R. Tampubolon [#1], Suhardi [#3]

[#] *Sekolah Teknik Elektro dan Informatika*
Institut Teknologi Bandung
Jalan Ganesha 10 Bandung
[1] aront@students.itb.ac.id
[3] suhardi@stei.itb.ac.id

Abstract— Information Technology has succeeded change the paradigm of customer in the transaction. The transactions are beginning by coming to the bank teller, but now they can easily using a mobile phone, internet or ATM outlets that distributed in various strategic places by using an ATM card. In addition to facilitate customers in the transaction, Information Technology has also become a competitive advantage for banks to attract retail customers.

However Advancement of Information Technology is closely linked to the risk that must be faced by the customers and the bank. In order to optimize the target of Information Technology, a company must implement an integrated risk management in corporate management (ERM).

This paper presents a related case study of information technology issue that occur in company in the retail banking sector, the analysis performed using the ISO 31000:2009 framework. Framework considers the risk of Information Technology as an integrated part of the enterprise risk framework. This study uses secondary data from annual reports and company websites for research.

Keywords— Information Technologi Risk, ITRisk, ISO 31000:2009

I. PENDAHULUAN

Teknologi Informasi (TI) telah menjadi suatu kebutuhan hampir disemua bidang usaha. Baik itu di bidang perbankan, pemerintahan, maupun di bidang pendidikan. Di bidang perbankan retail misalnya, TI memberikan banyak pilihan bagi nasabah untuk memudahkan proses transaksi, transaksi dapat dilakukan dimana saja dan kapan saja dengan menggunakan layanan ATM (*Automatic Teller Machine*), EDC (*Electronic Data Capture)*, m-banking (*mobile Banking)*, maupun i-banking(*Internet Banking)*. Layanan-layanan TI ini bahkan telah mengubah paradigma nasabah dalam bertransaksi.

Namun kemajuan TI ini tidak terhindar dari risiko yang dapat membuat tidak terwujudnya tujuan dari penggunaan TI tersebut[1]. Pembobolan ATM adalah salah satu risiko yang harus dihadapi oleh pihak bank maupun pihak nasabah. Pihak Bank dapat mengalami ketidakpercayaan nasabah yang berdampak pada penurunan reputasi dimata nasabahnya, sedangkan pihak nasabah mengalami kerugian akibat kehilangan dana di rekeningnya.

Risiko-risiko tersebut dapat dihadapi dengan membuat suatu tata kelola(Manajemen Risiko) yang baik sehingga dapat memberikan pertimbangan kepada perusahaan secara terstruktur dengan memperhatikan segala bentuk ketidakpastian dalam pengambilan keputusan dan tindakan yang harus diambil guna menangani risiko tersebut. Tata kelola inilah yang disebut dengan *Enterprise Risk Managemen* (ERM)[2].

Pada bulan November tahun 2009, International Organization for Standardization (ISO) mengeluarkan *framework* standar untuk mengelola risiko yaitu ISO 31000:2009 dengan judul *"Risk Management-Principles and Guidelines on Implementation"*. Standar ini dikeluarkan untuk membantu perusahaan dalam mengelola risiko [3]. Karena sifatnya yang generik, *framework* ini dapat diaplikasikan di berbagai jenis perusahaan, grup atau individu. ISO 31000:2009 menyediakan panduan dalam mendesain, implementasi dan memelihara proses pengelolaan risiko di dalam sebuah organisasi.

Makalah ini membahas konsep dan implementasi *framework* ISO 31000:2009 kedalam sebuah perusahaan perbankan retail untuk mencegah risiko yang sama terjadi kembali. Kasus yang diangkat adalah pembobolan ATM pada Bank Central Asia(BCA) yang tejadi pada awal tahun 2010 di beberapa kota besar di Indonesia.

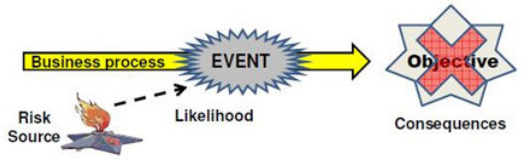
II. METODE

A. Enterprise Risk Management (ERM)

Konsep Manajemen Risiko

Deloitte mendefinisikan risiko sebagai potensi kerugian yang disebabkan oleh suatu peristiwa (atau serangkaian peristiwa) yang dapat mempengaruhi pencapaian tujuan perusahaan [4]. Sementara menurut Monahan Risiko adalah sebuah ketidak pastian untuk mencapai *strategic objective* sebuah perusahaan. Risiko dipengaruhi oleh *Risk Driver* dan *Risk Control*. *Risk Drivers* adalah faktor-faktor yang meningkatkan ketidak pastian. Sementara *Risk Control* adalah factor-faktor yang mengurangi ketidak pastian[5].

Leo Susilo mendefinisikan Risiko sebagai pengaruh dari ketidakpastian terhadap sasaran/tujuan (*objectives*)[1].



Gambar 1. Definisi Risiko[1]

ISACA mendefinisikan Risiko TI sebagai risiko bisnis yang berkaitan erat dengan penggunaan, kepemilikan, operasional, keterlibatan, pengaruh dan adopsi TI didalam perusahaan [6].

Manajemen risiko (*risk management*) adalah upaya terkoordinasi untuk mengarahkan dan mengendalikan kegiatan-kegiatan organisasi terkait risiko dalam operasional perusahaan untuk mengurangi berbagai kerugian dan untuk menetapkan sebuah standar operasional dalam sebuah perusahaan [1]. Manajemen risiko juga didefinisikan sebagai proses mengidentifikasi risiko, menganalisis dan menilai risiko, dan mengambil langkah-langkah untuk mengurangi risiko ke tingkat yang dapat diterima [7].

Manajemen risiko TI adalah penerapan manajemen risiko dengan konteks teknologi informasi untuk mengelola risiko TI. Manajemen risiko TI dapat dianggap sebagai komponen dari suatu sistem manajemen risiko yang lebih luas yaitu ERM [6].

Framework manajemen risiko merupakan seperangkat komponen yang memberikan landasan dan kerangka kerja untuk merencanakan, menerapkan, memonitor, *review* dan secara berkelanjutan memperbaiki proses manajemen risiko pada seluruh bagian organisasi [1].

Framework manajemen risiko TI merupakan kerangka kerja yang didasarkan pada seperangkat prinsip-prinsip penuntun untuk manajemen risiko TI yang efektif, menyediakan kerangka kerja bagi perusahaan untuk mengidentifikasi, mengatur dan mengelola risiko TI [6].

Konsep ERM

Manajemen risiko perusahaan (*ERM*) mengambil perspektif yang luas pada identifikasi risiko yang dapat mengakibatkan suatu organisasi gagal untuk memenuhi strategi dan tujuan. Definisi *ERM* adalah suatu proses yang dipengaruhi oleh entitas dewan direksi, manajemen dan personel lain, yang diaplikasikan dalam penetapan strategi di dalam perusahaan, didesain untuk mengidentifikasikan *event* yang potensial yang dapat berpengaruh pada entitas dan mengelola risiko dengan penerimaan risiko yang diharapkan, memberikan jaminan yang masuk akal terhadap pencapaian tujuan dari entitas [2].

Definisi di atas menggambarkan konsep dasar dari *ERM*, yaitu: 1) Proses berkelanjutan dan mengalir melalui entitas, 2) Dipengaruhi oleh orang-orang disetiap level organisasi, 3) Diterapkan dalam penyusunan strategi, 4) Diterapkan di seluruh perusahaan, pada setiap tingkat dan unit, 5) Dirancang untuk mengidentifikasi kejadian potensial yang jika terjadi, akan mempengaruhi tujuan entitas dan dalam mengelola *risk appetite* (selera risiko), 6) Mampu memberikan kepastian yang sewajarnya kepada manajemen entitas dan dewan direksi, 7) Diarahkan untuk pencapaian tujuan pada satu atau lebih kategori yang terpisah.

ISO 31000 Risk Management-Principle and Guidelines

ISO 31000 "*Risk Management-Principle and Guidelines on Implementation*" adalah keluarga standar internasional pedoman penerapan manajemen risiko yang diterbitkan oleh *International Organization for Standardization* (*ISO*). Standar yang diterbitkan pada 13 November 2009 ini merupakan pengembangan standar *AS/NZS 4360:2004* yang dikeluarkan oleh *Standards Australia* [1].

Kelebihan *ISO* 31000:2009 dibandingkan dengan *framework* lain [1]: 1) Kemudahan dalam menerapkan, 2) Lingkup penerapan *ISO* 31000 lebih general, 3) *ISO* 31000 bukan untuk sertifikasi, 4) *ISO* 31000 telah diadopsi oleh banyak negara

Struktur *ISO* 31000 terdiri atas tiga elemen yang saling berkaitan yaitu 1) *Principles Risk Management,* 2) *Risk Management Framework*; dan 3) *Risk Management Process* [1].

Risk Management Framework digunakan satu untuk seluruh organisasi, sedangkan *Risk Management Process* adalah unik untuk setiap proses bisnis dan juga untuk setiap jenis risiko[1].

Prinsip Manajemen Risiko

(*Principles Risk Management*) dapat dikatakan efektif apabila memiliki kemampuan untuk menerapkan prinsip-prinsip sebagai berikut [1]: 1) Manajemen risiko harus memberi nilai tambah, 2) Manajemen risiko adalah bagian terpadu dari proses organisasi, 3) Manajemen risiko adalah bagian dari proses pengambilan keputusan, 4) Manajemen risiko secara khusus menangani aspek ketidakpastian, 5) Manajemen risiko bersifat sistematik, terstruktur dan tepat waktu, 6) Manajemen risiko berdasarkan pada informasi terbaik yang tersedia, 7) Manajemen risiko adalah khas untuk penggunaannya, 8) Manajemen risiko mempertimbangkan faktor manusia dan budaya, 9) Manajemen risiko harus transparan dan inklusif, 10) Manajemen risiko bersifat dinamis, berulang dan tanggap terhadap perubahan, 11) Manajemen risiko harus memfasilitasi terjadinya perbaikan dan peningkatan organisasi secara berlanjut.

***Framework* Manajemen Risiko**

(*Risk Management Framework),* Manajemen risiko harus diletakkan dalam suatu *framework* manajemen risiko supaya dapat berhasil dengan baik. *Framework* ini akan menjadi dasar penataan yang mencakup seluruh kegiatan manajemen risiko disemua tingkatan organisasi. Selain itu, dapat membantu organisasi mengelola risiko secara efektif melalui penerapan proses manajemen risiko, memastikan informasi risiko yang lengkap dan memadai yang digunakan sebagai landasan untuk pengambilan keputusan. Gambar 2. menggambarkan komponen-komponen dari *framework* manajemen risiko yang diperlukan dan hubungannya satu dengan yang lainnya[1].

Gambar 2. Komponen *framework* Manajemen Risiko

a. Mandat dan komitmen

Penerapan manajemen risiko yang efektif diperlukan komitmen yang kuat dan berkelanjutan dari manajemen organisasi. Untuk itu, diperlukan perencanaan yang matang dan strategi yang tepat dalam pelaksanaannya.

b. Perencanaan *framework* manajemen risiko

Memahami organisasi dan konteksnya, Menetapkan kebijakan manajemen risiko, Akuntabilitas, Integrasi ke dalam proses bisnis, Sumber daya, Pembentukan mekanisme komunikasi internal dan sistem pelaporan, Pembentukan mekanisme komunikasi eksternal dan sistem pelaporannnya.

c. Penerapan *framework* manajemen risiko

Manajemen risiko risiko dapat dikatakan telah terlaksana dengan baik apabila proses manajemen risiko telah terlaksana di semua tingkatan dan fungsi organisasi.

d. *Monitoring* dan *review*

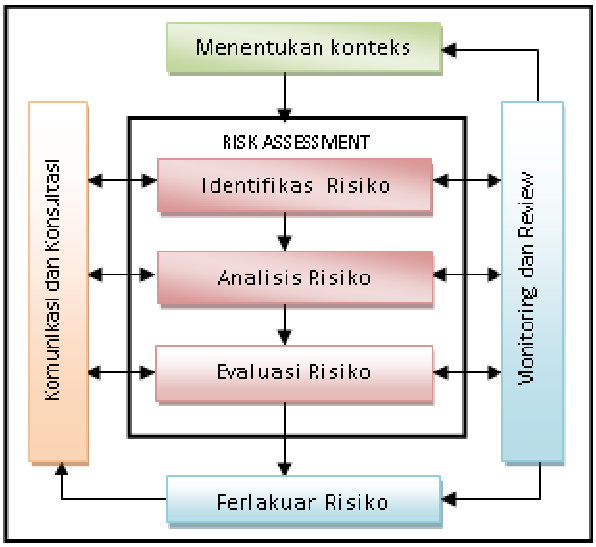
Menetapkan ukuran kinerja, meninjau secara berkala *framework* manajemen risiko, kebijakan risiko dan rencana penerapan risiko tetap sesuai dengan konteks internal dan eksternal organisasi.

e. Perbaikan kerangka kerja secara berkelanjutan.

Berdasarkan hasil monitoring dan *review* diambil tindak lanjut untuk meningkatkan *framework* manajemen risiko, kebijakan risiko dan rencana manajemen risiko.

Proses Manajemen Risiko (*Risk Management Process)*

Proses manajemen risiko hendaknya merupakan bagian yang tidak terpisahkan dari manajemen umum. Manajemen risiko harus menjadi bagian dari budaya organisasi, praktik terbaik organisasi dan proses bisnis organisasi. Proses manajemen risiko meliputi 5 (lima) kegiatan yaitu komunikasi dan konsultasi, menentukan konteks, asesmen risiko, perlakuan risiko, monitoring dan *review* seperti yang digambarkan pada gambar 3. proses manajemen risiko di bawah ini[1]:



Gambar 3. Proses Manajemen Risiko[1]

a. **Komunikasi dan konsultasi**

Komunikasi dan konsultasi dengan pemangku kepentingan sangat penting karena mereka dapat memberikan pertimbangan dan penilaian terhadap risiko yang didasarkan atas persepsi mereka terhadap risiko tersebut. Persepsi terhadap risiko ini sangat berbeda dari masing-masing pemangku kepentingan, baik dari segi nilai, konsep, kebutuhan, maupun kepentingan. Hal inilah yang dijadikan pertimbangan dalam proses pengambilan keputusan. Rencana komunikasi dan konsultasi hendaknya 1) Merupakan forum untuk bertukar informasi di antara para pemangku kepentingan, 2) Tempat menyampaikan pesan secara jujur, akurat, mudah dimengerti, dan didasarkan pada fakta yang ada, 3) bermanfaat dan besar kontribusinya harus dapat dinilai.

b. **Menetapkan konteks**

Dengan ditetapkannya konteks berarti manajemen organisasi menentukan batasan atau parameter internal dan eksternal yang akan dijadikan pertimbangan dalam pengelolaan risiko, menentukan lingkup kerja dan kriteria risiko untuk proses-proses selanjutnya. 4 kegiatan yang dapat dilakukan dalam menentukan konteks ini adalah

1) Menentukan Konteks Eksternal

Konteks Eksternal adalah lingkungan eksternal dimana organisasi tersebut mengupayakan pencapaian sasaran yang ditetapkannya. Memahami konteks eksternal dilakukan untuk memastikan siapa saja pemangku kepentingan eksternal, apa saja kepentingan dan sasarannya sehingga dapat dipertimbangkan dalam menentukan kriteria risiko.

2) Menentukan Konteks Internal

Konteks Internal adalah segala sesuatu di dalam organisasi yang dapat mempengaruhi cara organisasi

dalam mengelola risiko. Konteks internal dapat berupa struktur organisasi, proses bisnis, dll

3) Menetapkan Konteks proses Manajemen Risiko
Konteks proses Manajemen Risiko adalah konteks dimana proses manajemen risiko diterapkan. Hal ini meliputi sasaran organisasi, strategi, lingkup, parameter, kegiatan organisasi, atau bagian lain dimana manajemen risiko diterapkan.

4) Mengembangkan Kriteria Risiko
Organisasi harus menyusun criteria risiko yang akan digunakan untuk mengevaluasi tingkat bahaya suatu risiko. Kriteria yang perlu dipertimbangkan antara lain 1) Kriteria dampak (*consequence*), 2) Kriteria kemungkinan (*likelihood*), 3) Kriteria pemeringkat risiko (*risk level*), 4) Kriteria selera risiko (*risk appetite*)

c. **Assessment Risiko**

1) Identifikasi risiko
Sasaran dari tahapan ini adalah membuat daftar risiko secara komperehensif dan luas yang dapat mempengaruhi pencapaian sasaran baik meningkatkan, menghalangi, memperlambat atau bahkan mengagalkan pencapaian sasaran organisasi. Beberapa metode untuk mengidentifikasi risiko adalah Risk Breakdown Structure(RBS), Failure Mode and Effect Analysis (FMEA), Controlled Risk Self-Assessment (CRSA) dan document review

2) Analisa risiko
Analisa risiko meliputi kegiatan-kegiatan yang menganalisa sumber risiko dan pemicu terjadinya risiko, dampak positif dan negatifnya serta kemungkinan terjadinya serta atribut lain risiko.
Menurut jenisnya, analisa risiko dibagi menjadi 2 jenis yaitu Analisa Kualitatif yang meliputi teknik pemeringkatan risiko dan analisa sebab-akibat. Dan Analisa Kuantitatif yang meliputi teknik Bencmarking, Analisa Sensitivitas dan Simulasi Monte Carlo.

3) Evaluasi risiko
Tujuan dari evaluasi risko adalah membantu proses pengambilan keputusan berdasarkan hasil analisa risiko. Proses evaluasi risiko akan menentukan risiko-risiko mana yang memerlukan perlakuan dan bagaimana prioritas perlakuan atas risiko-risiko tersebut. Hasil evaluasi risiko akan menjadi masukan bagi proses perlakuan risiko.

d. **Perlakuan Risiko**
Perlakuan terhadap risiko pada dasarnya terdiri dari 4 jenis yaitu:

1. *Risk avoidance* / menghindari risiko
2. *Risk reduction* / mengurangi risiko/mitigasi risiko
   a. Mengurangi *likelihood*
   b. Mengurangi dampak
3. *Risk sharing*/ berbagi risiko kepada pihak ketiga
   Risk acceptance/ menerima risiko

III. STUDI KASUS: PEMBOBOLAN ATM BCA

Studi Kasus *event*

Pada awal tahun 2010, perhatian masyarakat Indonesia tertuju pada beberapa kasus pembobolan ATM yang melibatkan sindikat internasional[b]. Media elektronik[c] maupun media cetak[d] mengangkatnya menjadi tajuk utama yang menyebabkan kepanikan bagi hampir seluruh nasabah bank di Indonesia termasuk nasabah BCA[e]. Modus yang digunakan adalah Pelaku Tindak Kejahatan (PTK) memasang "*Skimmer"* di mulut ATM dan memasang alat perekam di bilik ATM, kemudian membuat kartu ATM palsu yang digunakan untuk melakukan transaksi di ATM[f].

Sebanyak 200 nasabah BCA menjadi korban kejahatan ini, dan BCA menanggung kerugian sampai dengan 5 Miliar Rupiah[d]. Selain kerugian tersebut, BCA juga berpotensi mengalami risiko kerugian yang lebih besar lagi jika masalah tersebut tidak ditangani dengan baik, yaitu ketidakpercayaan nasabah terhadap penggunaan IT sebagai alat untuk melakukan transaksi.

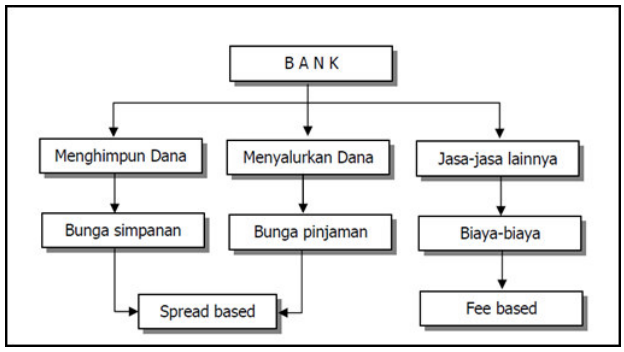
Sebagai Antisipasi, BCA menerapkan beberapa tindakan yaitu : 1) Memasang *anti-skiming,* penutup pin, dan kamera CCTV di bilik ATM, 2) Menganjurkan nasabah untuk mengganti PIN[a].

Rumusan Kasus :

Risk Event	: Pembobolan ATM
Risk Driver	: 1. Keamanan Mesin ATM
Risk Control	: Memasang *anti-skimming*, penutup PIN, dan kamera CCTV.
Risk Driver	: 2. Kesalahan Nasabah
Risk Control	: Menganjurkan Nasabah untuk mengganti PIN

Unit Analisis

Menurut Undang-undang No. 7 Tahun 1992 tentang Perbankan yang diperbaharui dengan Undang-undang No. 10 Tahun 1998. Bank dapat didefinisikan sebagai Badan usaha yang menghimpun dana dari masayarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit dan/ atau bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak. Sedangkan Perbankan adalah Segala sesuatu yang menyangkut tentang bank, mencakup kelembagaan, kegiatan usaha, serta cara dan proses dalam melaksanakan kegiatan usahaanya.



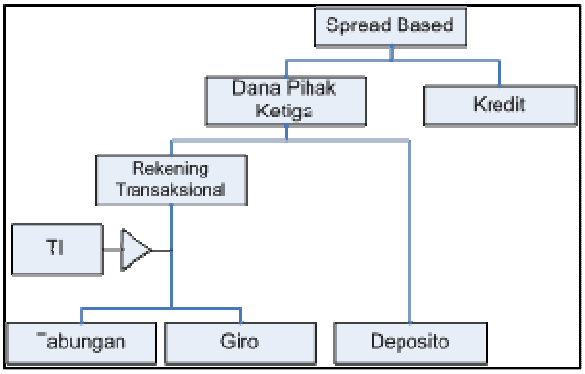
Gambar 4. Model Bisnis Bank[8]

Bank mendapatkan keuntungan dari selisih antara bunga simpanan dan bunga pinjaman, dan keuntungan ini disebut dengan *Spread based*, serta *Fee Based* dari pelayanan jasa-jasa perbankan lainnya seperti transfer, kliring, safe deposit box dll. Terdapat 2 hal yang mempengaruhi *Spread Based*, yaitu jumlah dana pihak ketiga (proses penghimpunan dana masyarakat) sebagai variabel pertama serta jumlah dana yang di pinjamkan kepada pihak lain sebagai variable kedua. Dengan demikian semakin tinggi dana pihak ketiga yang dapat dikumpulkan oleh sebuah bank akan meningkatkan penyaluran dana kepada pihak lain yang berakibat naiknya margin dari *Spread Based*[8].

Salah satu pelaku dalam bisnis perbankan nasional adalah PT. Bank Central Asia, Tbk (BCA). BCA tumbuh sebagai bank umum dengan kepemilikan swasta, serta memilih menjadi *Perbankan Retail* dimana bank dapat bertransaksi dengan konsumen secara langsung, dengan layanan rekening transaksional, pinjaman pribadi, deposito, kartu debet, kartu kredit dan sebagainya.

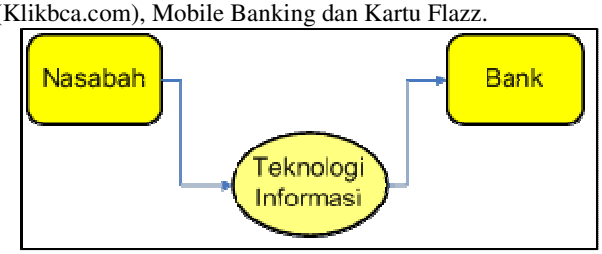
Tujuan Penggunaan IT di BCA

Sebagai Bank Retail dengan rekening transaksional sebagai bisnis utama, BCA menerapkan teknologi informasi sebagai alat untuk menciptakan kemudahan dalam melakukan transaksi nasabahnya sehingga para nasabah dapat mengurangi dana cash dan beralih menggunakan Paspor BCA (kartu ATM) untuk melakukan transaksi. Dengan demikian, BCA akan mendapatkan dana transaksi masyarakat sekaligus meningkatkan jumlah dana pihak ketiga dan juga meningkatkan *Spread Based* yang merupakan keuntungan bagi industri perbankan.



Gambar 5. TI dalam Strategi BCA

Untuk mendukung transaksi para nasabahnya, BCA menerapkan beberapa teknologi informasi diantaranya : Mesin ATM, *Electronic Data Capture* (EDC), Internet Banking (Klikbca.com), Mobile Banking dan Kartu Flazz.



Gambar 6. Diagram Posisi TI dalam Strategi BCA

Antusiasme nasabah BCA terhadap teknologi informasi sebagai alat untuk membantu bertransaksi sangat tinggi, ini terbukti dengan jumlah transaksi melalui Teknologi Informasi yang terpaut jauh daripada jumlah transaksi di kantor cabang. Hal ini terjadi karena tingkat kepercayaan nasabah terhadap keamanan transaksi dengan menggunakan Teknologi Informasi yang diterapkan oleh BCA cukup tinggi.

TABEL 1. JUMLAH JARINGAN LAYANAN (UNIT)

	2010	2009	2008	2007
Kantor Cabang	902	875	844	809
ATM	7459	6.611	5.997	5.654
EDC	>129.164	129.164	81.750	65.645

TABEL 2. JUMLAH TRANSAKSI MELALUI DELIVERY CHANEL

	2010	2009	2008
Kantor Cabang			
• Jumlah Transaksi (Jutaan)	182,4	174,3	171,9
• Nilai Transaksi (Triliun)	10.450,1	9.134,2	8.956,9
ATM (termasuk EDC)			
• Jumlah Transaksi (Jutaan)	904,1	848,9	793,6
• Nilai Transaksi (Triliun)	936,9	858,8	807,6

Internet Banking			
• Jumlah Transaksi (Jutaan)	402,5	230,5	135,0
• Nilai Transaksi (Triliun)	1.907,7	1.355,6	991,8
Mobile Banking			
• Jumlah Transaksi (Jutaan)	164,7	120,9	85,8
• Nilai Transaksi (Triliun)	187,4	135,3	95,5

Manajemen Risiko di BCA

Struktur Manajemen Risiko

BCA memiliki suatu kerangka kerja manajemen risiko yang terintegrasi, yang mencakup kebijakan Bank dan pembagian tanggung jawab agar pengelolaan risiko berjalan secara efektif di seluruh aspek Bank. Dewan Komisaris dan Direksi BCA bekerja sama untuk memastikan keberhasilan penerapan sistem manajemen risiko. Dewan Komisaris melaksanakan fungsinya untuk mengawasi dan mengevaluasi penerapan kebijakan-kebijakan manajemen risiko, sedangkan Direksi melaksanakan tanggung jawabnya dalam proses penyusunan, evaluasi, implementasi dan pengembangan sistem manajemen risiko. Salah satu anggota Direksi ditunjuk untuk menjalankan fungsi sebagai Direktur Manajemen Risiko yang bertanggung jawab untuk memastikan pengawasan sehari-hari atas kepatuhan setiap unit bisnis terhadap kebijakan manajemen risiko yang berlaku[a].

BCA memiliki unit-unit kerja dan beberapa komite yang bertanggung jawab untuk menangani berbagai jenis risiko. Satuan Kerja Manajemen Risiko (SKMR) dibentuk untuk membantu Direksi dalam memastikan bahwa kerangka kerja manajemen risiko yang diterapkan memberikan perlindungan yang memadai terhadap *enterprise risk* yang dihadapi BCA. SKMR bekerja secara independen terhadap unit-unit operasional dan Audit Internal, serta bertanggung jawab kepada Direktur yang membawahi manajemen risiko. Struktur organisasi SKMR disesuaikan dari waktu ke waktu agar selaras dengan perkembangan bisnis Bank. Pada tahun 2010, Satuan Kerja Manajemen Risiko Cabang dibentuk dibawah *Strategic Business Unit* (SBU) Perbankan Cabang. Tugas satuan kerja tersebut adalah membantu Direktur yang membawahi Perbankan Cabang dalam meningkatkan kualitas manajemen risiko pada setiap tingkatan unit kerja pada SBU Perbankan Cabang melalui penerapan kerangka kerja manajemen risiko yang tepat. Satuan kerja tersebut berkoordinasi dengan Direktur yang membawahi manajemen risiko untuk memastikan independensi dalam hubungannya dengan SBU Perbankan Cabang.

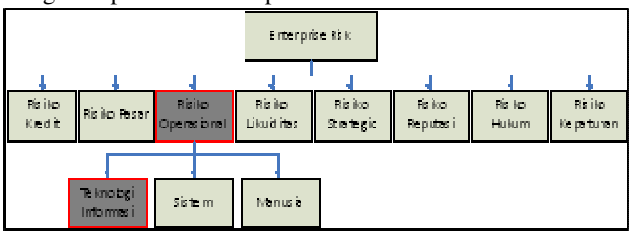
Bank juga memiliki Komite Manajemen Risiko yang berfungsi memberikan rekomendasi kebijakan dan membahas seluruh aspek risiko yang dihadapi Bank. Selain itu, Direksi telah membentuk komite-komite khusus yang bertugas untuk menangani risiko yang lebih spesifik, yaitu Komite Kebijakan Perkreditan, Komite Kredit, dan Komite Aset dan Liabilitas (ALCO). BCA juga membentuk Komite Pemantauan Risiko yang membantu Dewan Komisaris untuk memastikan penerapan kerangka kerja manajemen risiko yang tangguh.

Kategori Risiko

Satuan Kerja Manajemen Risiko memonitor menelaah, dan menganalisa risiko-risiko bersama dengan unit-unit terkait untuk memastikan penerapan manajemen risiko yang tepat menyangkut delapan kategori risiko yang dihadapi BCA. Pengukuran dan pengawasan terhadap kedelapan risiko ini menghasilkan profil risiko untuk setiap risiko maupun keseluruhan risiko, yang kemudian disatukan ke dalam laporan profil risiko triwulanan dan dilaporkan kepada Bank Indonesia sesuai peraturan yang berlaku. Kedelapan kategori risiko tersebut adalah sebagai berikut: 1) Risiko Kredit, 2) Risiko Pasar, 3) Risiko Operasional, 4) Risiko Likuiditas, 5) Risiko Strategis, 6) Risiko Reputasi, 7) Risiko Hukum, 8) Risiko Kepatuhan.

BCA menghadapi risiko operasional yang disebabkan oleh kesalahan manusia atau kesalahan dalam proses dan kegagalan pengawasan dalam kegiatan operasional sehari-hari, termasuk yang terjadi di *back office* dan cabang, maupun penipuan dan tindakan pelanggaran hukum lainnya. Bank menerapkan *Operational Risk Management Information System* (ORMIS) berbasis web yang dilengkapi dengan aplikasi *Key Risk Indicator* untuk menyediakan deteksi dini terhadap risiko operasional. Sistem ORMIS ini meliputi *Risk Control Self Assessmen*t dan *Loss Event Database*, yang memberikan informasi berguna untuk meminimalkan risiko operasional.

BCA memiliki cadangan atas pusat teknologi informasi yang brfungsi secara *mirroring* dengan pusat teknologi informasi utama untuk memastikan terpeliharanya arus transaksi jika terjadi kerusakan besar di pusat data utama. Selain itu, jaringan distribusi BCA didukung oleh sistem cadangan ganda untuk menjaga kelangsungan operasional cabang, ATM dan jaringan distribusi lainnya apabila terjadi gangguan listrik atau komunikasi jaringan. Pada tahun 2010, BCA memulai program jangka panjang untuk meningkatkan organisasi dan infrastruktur teknologi informasi serta rencana untuk mendirikan *Disaster Recovery Center* (DRC) baru. DRC baru tersebut diharapkan akan memperkuat sistem teknologi informasi dan manajemen risiko BCA dalam mengelola potensi risiko operasional.



Gambar 7. Kategori Risiko BCA

IV. HASIL ANALISIS

Pembobolan ATM telah merugikan 200 nasabah BCA, yang sekaligus dapat menimbulkan ketidak percayaan nasabah terhadap keamanan transaksi menggunakan TI, Bahkan dapat mengancam reputasi dari BCA sebagai perbankan retail. Oleh karena itu, manajemen harus mengambil tindakan cepat dan mencegah risiko tersebut terulang kembali.

ISO 31000: 2009 dapat diimplementasikan kedalam kasus pembobolan ATM ini untuk mencegah kejadian serupa terjadi kembali.

A. ***Menentukan Konteks***

Konteks Internal

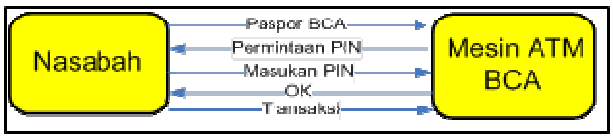
Dalam *Risk Event* Pembobolan ATM, Kategori Risiko yang terpengaruh adalah Risiko Operasional Teknologi Informasi dalam hal ini alat teknologi informasi ATM. Selain Risiko Operasional, Pembobolan ATM ini juga mengancam Kategori yang lain yaitu Risiko Reputasi, karena dapat mengakibatkan ketidakpercayaan nasabah terhadap transaksi menggunakan TI, sehingga nasabah akan memindahkan dananya kepada *competitor* lain yang dianggap aman. Bahkan dapat berdampak lebih besar lagi dengan kekhawatiran nasabah akan dananya, Sehingga mereka akan menarik dananya dari Bank. Hal ini dapat mengakibatkan "Bencana" bagi dunia perbankan.

Proses Bisnis

BCA menyadari perannya sebagai bank transaksi sehingga BCA terus menginvestasikan mesin-mesin ATM untuk melayani transaksi sehingga para nasabah tetap terlayani walaupun jam kerja telah usai. Inovasi-inovasi yang terus dikembangkan oleh BCA sangat menarik hati para nasabah, antara lain dengan mengeluarkan mesin ATM non tunai yang dapat mengurangi antrian-antrian pada mesin ATM serta ATM setoran tunai yang memungkinkan nasabahnya melakukan setoran bahkan pada malam hari atau hari libur sekalipun. Jumlah ATM BCA pun terus ditambah seiring dengan pertumbuhan transaksi yang terjadi, pada tahun 2010 BCA telah memiliki 7.459 mesin ATM yang tersebar di dalam negeri maupun di luar negeri.

Setiap Nasabah BCA berhak memiliki Paspor BCA(Kartu ATM) dengan mengajukan permohonan kepada pihak bank untuk mendapatkan Paspor BCA. Paspor BCA terdiri dari 3 jenis yaitu silver dengan biaya administrasi Rp. 30,000/bulan, Gold dengan biaya Rp. 35,000/bulan serta Platinum Rp. 40,000/bulan.

Gambar 8. Prosedur Permohonan Paspor BCA



Gambar 9. Prosedur Penggunaan Mesin ATM BCA

Keamanan Transaksi

Dalam melakukan transaksi menggunakan mesin ATM, nasabah bertanggung jawab terhadap Paspor BCA yang merupakan representasi dari nomer rekening nasabah dan PIN ATM yang merupakan kata sandi/kunci untuk melakukan transaksi yang telah diberikan oleh pihak BCA. Sementara BCA bertanggung jawab terhadap keamanan Mesin ATM yang dimilikinya Pada tahun 2010, BCA telah memiliki piranti *anti-skimming*, penutup PIN, dan kamera CCTV sebagai langkah prefentif untuk mencegah terjadinya pembobolan rekening lewat mesin ATM.

Kriteria Risiko

Kriteria Kemungkinan(*likelihood*)

Dalam membentuk Kriteria kemungkinan, penulis menggunakan table Matrik probabilitas.

TABEL 3. MATRIKS PROBABILITAS[1]

Tingkat	Sebutan	Uraian	Frekuensi
A	Hampir pasti	Terjadi setiap tahun	1 kali dalam 1tahun atau lebih
B	Mungkin sekali	Menurut pengalaman kejadian ini muncul beberapa kali	1 kali dalam 3 tahun
C	Mungkin	Menurut pengalaman baru terjadi saru kali	1 kali dalam 10 tahun
D	Kecil kemungkinan	Kejadian ini sangat jarang muncul	1 kali dalam 30 tahun
E	Jarang	Pernah mendengar ada kejadian semacam itu	1 kali dalam 100 tahun

Kriteria Dampak(*consequence*)

Dalam membentuk Kriteria Dampak, penulis menggunakan table Matrik Dampak.

TABEL 4. MATRIKS DAMPAK[1]

Sebutan	Uraian	Peringkat
Sangat Kecil	Dampak kecil terhadap sasaran yang dapat diabaikan	I
Kecil	Kerusakan kecil yang mudah diperbaiki kembali	II
Sedang	Mempengaruhi pencapaian	III

Besar	beberapa sasaran Sasaran-sasaran penting tidak dapat tercapai	IV
Bencana	Semua sasaran tidak dapat tercapai	V

Kriteria Pemeringkat Risiko(*Risk Level)*

Dalam menentukan kriteria pemeringkat risiko, penulis menggunakan Tabel 5. Penentuan Peringkat Risiko.

TABEL 5 PENENTUAN PERINGKAT RISIKO[1]

Sebutan	Dampak				
	I	II	III	IV	V
A	M	T	T	ST	ST
B	M	M	T	T	ST
C	R	M	T	T	T
D	R	R	M	M	T
E	R	R	M	M	T

B. *Assesment Risiko*

1) *Identifikasi Risiko*

Untuk melalakukan identifikasi risiko, penulis menggunakan metode *document viewer.*

Nama Risiko : Pembobolan ATM

Uraian Risiko

Paspor BCA nasabah digunakan oleh pihak yang tidak bertanggung jawab untuk melakukan transaksi di ATM BCA.

Perkiraan Sumber Risiko

Penggunaan *Skimer* yaitu alat untuk mengambil No Kartu Nasabah yang diletakakn di mulut mesin ATM dan menggunakan kamera pemantau untuk mendapatkan PIN dari nasabah tersebut.

Uraian Dampak Risiko

Dampak yang timbul adalah pencurian dana nasabah oleh pihak yang tidak bertanggung jawab yang menimbulkan kerugian bagi nasabah, serta menurunya kepercayaan nasabah untuk melakukan transaksi di mesin ATM yang mengakibatkan kerugian tak ternilai bagi sebuah perbankan retail.

Uraian Kemungkinan terjadinya Risiko

Kemungkinan terjadinya risiko pembobolan ATM cukup besar, karena letak mesin ATM yang tersebar di berbagai lokasi baik, yang dijaga oleh bagian security(Satpam) maupun yang ditempatkan di daerah-daerah yang tidak tejaga oleh bagian security(Satpam).

Status Risiko

Risiko Pembobolan ATM masih aktif, bahkan mungkin saja berkembang dengan modus yang lainnya.

2) *Analisis Risiko*

Untuk melakukan analisis terhadap risiko pembobolan ATM, penulis menggunakan analisis kualitatif dengan menggunakan Analisis Peluang dan metode analisis Sebab-Akibat.

Analisis Peluang

Kriteria Kemungkinan:

Pembobolan ATM menggunakan alat *Skimmer* telah terjadi sejak tahun 2009[g], dan polisi telah melakukan penangkapan terhadap komplotan tersebut. Namun polisi dan pihak bank sepakat untuk merahasiakan penangkapan komplotan tersebut. Kejadian terulang pada tahun 2010 yang merugikan 200 nasabah BCA. Dengan demikian, Tingkat probabilitas Risiko Pembobolan ATM adalah Tingkat **A** dengan sebutan **Hampir Pasti.**

Kriteria Dampak:

Pembobolan ATM selain merugikan 200 nasabah BCA dengan nilai 5 Miliar Rupiah, Pembobolan ATM juga dapat menurunkan tingkat kepecayaan nasabah terhadap keamanan transaksi menggunakan ATM, bahkan juga dapat menyebabkan penarikan dana nasabah karena kekhawatiran dananya diambil oleh pelaku tindak kejahatan. Dengan demikian Risiko Pembobolan ATM dapat dikategorikan berdampak Besar dengan peringkat IV, karena sasaran-sasaran penting tidak dapat tercapai.

Dari Kriteria Kemungkinan tingkat **A** dan Kriteria Dampak peringkat **IV**, maka dapat disimpulkan bahwa Risiko Pembobolan ATM memiliki peringkat risiko **Sangat Tinggi**. Oleh karena itu Risiko Pembobolan ATM membutuhkan penanganan yang cepat dan hati-hati, serta harus melibatkan Manajemen Puncak.

Metode Sebab-Akibat

Metode Sebab Akibat digunakan untuk mencari penyebab dasar dari risiko Pembobolan ATM.

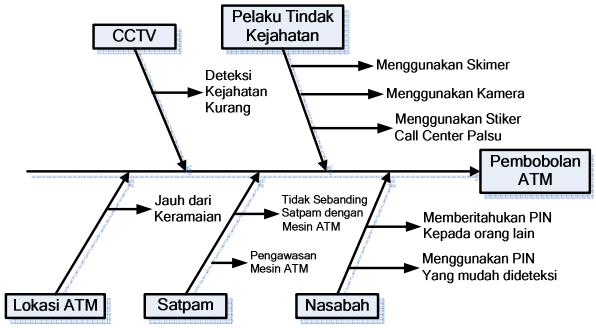
Langkah 1: Membuat Daftar Tanya Jawab Analisis Sebab-Akibat

TABEL 6. DAFTAR TANYA JAWAB ANALISIS SEBAB-AKIBAT

No	Pertanyaan	Jawaban
1	Mengapa Terjadi Pembobolan ATM?	1. Pencurian Nomer Kartu oleh Pelaku tindak kejahatan
		2. Kesalahan Nasabah
1.1	Mengapa Terjadi Pencurian Nomer Kartu?	Karena pelaku menggunakan Skimer di Mesin ATM
1.2	Mengapa Nasabah bisa salah?	1. Karena Nasabah memberitahukan PIN kepada orang lain
		2. Karena Nasabah menggunakan PIN yang mudah dideteksi
1.1.1	Mengapa pelaku bisa menggunakan peralatan skimmer dan kamera di dalam bilik ATM?	1. Karena pemeriksaan bilik dilakukan dengan selang waktu
		2. Karena pemantauan dengan CCTV hanya diperiksa jika terjadi insiden
1.2.1	Mengapa Nasabah memberitahukan	Karena Nasabah kurang sadar akan privasi PIN

	PIN kepada orang lain	ATM
1.2.2	Mengapa Nasabah menggunakan PIN yang mudah dideteksi	Karena Nasabah kurang memahami arti pentingnya keamanan PIN ATM
1.1.1.1	Mengapa Pemeriksaan bilik dilakukan dengan selang waktu	Karena prosedur pemeriksaan bilik dilakukan perhari
1.2.1.1	Mengapa Nasabah Kurang sadar akan privasi PIN ATM	Karena tidak adanya edukasi tentang ATM
1.2.2.1	Mengapa Nasabah Kurang memahami arti pentingnya keamanan PIN ATM	Karena tidak adanya edukasi tentang ATM

Langkah 2. Membuat Diagram Ishikawa



Gambar 10. Diagram Ishikawa untuk Risiko Pembobolan ATM

Langkah 3: Melakukan Analisis

Penyebab Dasar dari Risiko Pembobolan ATM.

1. Nasabah kurang memahami arti pentingnya keamanan PIN ATM.
2. Pemeriksaan Bilik ATM belum maksimal.
3. CCTV belum maksimal dalam mendeteksi terjadinya pembobolan ATM.
4. Lokasi ATM yang jauh dari pengawasan Satpam.

3) Evaluasi Risiko

Langkah BCA

Langkah yang ditempuh BCA menghadapi Pembobolan ATM 2009 adalah bekerja sama dengan Kepolisian RI untuk merahasiakan kasus tersebut dengan alasan dapat menimbulkan keresahan[g]. Pada awal tahun 2010, kasus pembobolan ATM terjadi kembali di beberapa kota besar di Indonesia diantaranya Bali, Jakarta, Bandung dan kota di Kalimantan timur[e], dengan menggunakan modus yang sama yang terjadi di tahun 2009.

Berikut Langkah-langkah yang ditempuh BCA menghadapi pembobolan BCA di awal tahun 2010.

1. BCA mengadakan Jumpa Pers tanggal 22 Januri 2010 yang diadakan di gedung Bank Indonesia[h]. Wakil Direktur Utama BCA Jahja Setiaadmadja menyampaikan kronologis pembobolan ATM BCA di Bali.
2. BCA memblokir transaksi di 2 (dua) Negara yaitu Australia dan Kanada yang merupakan tempat penarikan dana yang signifikan dan dicurigai sumber sindikat internasional[h].
3. BCA mengganti semua kerugian nasabah yang dirugikan akibat Pembobolan ATM[i].
4. BCA menguatkan system pengamanan di bilik ATM dengan mengadakan patroli pengawasan terhadap ATM-ATM milik BCA[j].
5. BCA menganjurkan nasabah untuk mengganti PIN ATM[j].
6. BCA Mengadakan *anti-skimming*, penutup PIN, dan CCTV di semua bilik ATM pada tahun 2010[a].

C. *Perlakuan Risiko*

Perlakuan Risiko oleh BCA

BCA memilih *Risk acceptance* atau menerima risiko ketika menghadapi kasus pembobolan ATM di tahun 2009. Karena menurut BCA dampak akibat publikasi akan lebih besar apabila BCA menerima risiko. Namun kasus serupa terulang kembali diawal tahun 2010 yang merugikan 200 nasabah BCA.

Pada tahun 2010, BCA memilih untuk *Memitigasi* Risiko dengan melakukan mengurangi *likelihood*. Dengan menguatkan system keamanan di bilik ATM dan menganjurkan nasabah untuk mengganti PIN ATM.

Analisis

Mitigasi adalah pilihan yang tepat dalam perlakuan risiko terhadap pembobolan ATM. Walaupun pada awalnya nasabah resah, namun dengan melakuan *mitigasi* risiko nasabah akan merasa aman untuk melakukan transaksi di ATM dan nasabah akan lebih hati-hati dalam melakukan transaksi di ATM.

V. KESIMPULAN

Setelah melakukan analisis terhadap manajemen risiko terkait TI di PT. Bank Central Asia, Tbk. menggunakan *framework* manajemen risiko *ISO* 31000:2009, ternyata dapat diambil kesimpulan sebagai berikut:

1. Manajemen Risiko penting dilakukan untuk menjaga tercapainya Tujuan dari Perusahaan.
2. ISO 31000:2009 dapat diimplementasikan dalam Manajemen Risiko bidang TI pada sebuah industri perbankan.
3. Perlakuan Risiko yang tidak tepat dapat meningkatkan *likelihood* atau Kriteria Kemungkinan dari sebuah *Risk Event*.
4. Mitigasi adalah perlakuan risiko yang tepat dalam mencegah terulangnya pembobolan ATM di BCA.

DAFTAR PUSTAKA

[1] L. J. Susilo dan V. Riwu Kaho, *Manajemen Risiko Berbasis ISO 31000 Untuk Industri Non Perbankan*, Jakarta, PPM, 2010

[2] Anonim, "Enterprise Risk Management-Integrated Framework", *Committee of Sponsoring Organizations (COSO) of Treadway Commission*, 2004

[3] J. Shortreed, "Enterprise Risk Management and ISO 31000", *The Journal of Policy Engagement*, Volume 2/Number 3,2010

[4] T. T. Deloitte, *The Risk Intelligent Enterprise—ERM Done Righ,* Deloitte Development LLC, 2006
[5] G. Monahan, *Enterprise Risk Management A Methodology for Achieving Strategic Objectives,* Hoboken, New Jersey, John Wiley & Sons, Inc, 2008
[6] Anonim, *The Risk IT Framework*, ISACA,2009
[7] J. Kouns, D. Minoli, *Information Technology Risk Management in Enterprise Environments,* New Jersey, John Wiley & Sons, Inc., 2010
[8] S. Dahlan, *Manajemen Lembaga Keuangan Edisi 5*, BPFE UI, 2006

Online:

[9] Anonim, Annual Report 2010, http://www.klikbca.com, 2011
[10] A. Suryadhi, Pembobolan Dana Nasabah BCA Didalangi Orang Rusia, detik.com, http://www.detiknews.com/read/2010/01/20/161338/1282613/10/pembobolan-dana-nasabah-bca-didalangi-orang-rusia, 2011
[11] Anonim, Seluruh Polda dikirimi Telegram Terkait Pembobolan ATM, metrotvnews.com, http://metrotvnews.com/index.php/metromain/news/2010/01/22/9396/-Seluruh-Polda-Dikirimi-Telegram-Terkait-Pembobolan-ATM, 2011
[12] W. S. Ari Wulan, Pembobolan ATM, BCA Rugi Rp 5 Miliar, Kompas.com, http://megapolitan.kompas.com/read/2010/01/21/19193019/Pembobolan.ATM.BCA.Rugi.Rp.5.Miliar, 2011
[13] Anonim, Korban Pembobolan Terus Bertambah, kompas.com, http://nasional.kompas.com/read/2010/01/24/03403693/korban.pembobolan.terus.bertambah, 2011
[14] Anonim, Modus Diketahui, Polisi Buru Pembobol ATM, Kompas.com, http://www.kompas.com/lipsus052009/antasariread/2010/01/21/14141240/Modus.Diketahui..Polisi.Buru.Pembobol.ATM, 2011
[15] E. M. Amelia, Oktober 2009 Polda Metro Tangkap 7 Pelaku Skimming, Tapi Tak Diumumkan, detik.com, http://www.detiknews.com/read/2010/01/22/153658/1284115/10/oktober-2009-polda-metro-tangkap-7-pelaku-skimming-tapi-tak-diumumkan, 2011
[16] H. Purnomo, BCA: Pembobolan ATM Murni Lewat Penggandaan Kartu, detik.com, http://finance.detik.com/read/2010/01/22/155757/1284132/5/bca-pembobolan-atm-murni-lewat-penggandaan-kartu, 2011
[17] U. Kalsum dan A. D. Darmawan, BCA Juga Dibobol dari Australia, vivanews.com, http://cangkang.vivanews.com/ramadan/news/read/123571-sindikat_juga_bobol_bca_dari_australia, 2011
[18] H. Purnomo, *200 Nasabah BCA Dibobol, Kerugian Capai Rp 5 Miliar,* detik.com http://www.detiknews.com/read/2010/01/21/201755/1283644/10/200-nasabah-bca-dibobol-kerugian-capai-rp-5-miliar, 2011