Analisis Manajemen Risiko Teknologi Informasi Pada Kasus Skimming ATM Bank X

Wahyu Firmandani[1], M. Malik[2]
Magister Akuntansi, Fakultas Ekonomi dan Bisnis, Universitas Indonesia, Jakarta, Indonesia[1]
Magister Akuntansi, Fakultas Ekonomi dan Bisnis, Universitas Indonesia, Jakarta, Indonesia[2]

Abtract. *The purpose of this study is to analyze the IT risk management constraints resulting in the appearance of Bank X ATM ATMs to anticipate similar events. The research method used in this study is qualitative with case study approach to deeply explore the constraints faced by Bank X in accordance with best practice RiskIT Framerowk by considering the three domains namely Risk Governance, Risk Evaluation, and Risk Response. The conclusions of this study are that Bank X has implemented IT risk management in accordance with the RIskTI Framework but there are still some weaknesses in governance processes, evaluation processes and the response processes, that are the MR Functional hierarchy and culture risk awareness, alignment of enterprise risk evaluation processes with risk based on audit processes, and constraints on the magnetic strip card migration process.*
Keywords. *ATM (Authomatic Teller Machine), RiskIT Framework, Risk Management Constraints.*

Abstrak. Tujuan penelitian ini adalah menganalisis kendala manajemen risiko TI yang mengakibatkan munculnya kasus skimming ATM Bank X untuk mengantisipasi kejadian serupa tidak terjadi lagi. Metode penelitian yang digunakan dalam penelitian ini adalah kualitatif dengan pendekatan studi kasus untuk menggali secara mendalam kendala yang dihadapi Bank X sesuai dengan *best practice* RiskIT Framerowk dengan mempertimbangkan ketiga domain yakni Risk Governance, Risk Evaluation, and Risk Response. Kesimpulan dari penelitian ini adalah Bank X telah menerapkan manajemen risiko TI sesuai dengan RIskTI Framework namun masih terdapat beberapa kelemahan pada proses tata kelola, pemanfaatan perangkat manajemen risiko operasional dan tindaklanjut (respon) atas kasus skimming ATM Bank X, yakni pada hierarki Fungsi MR dan budaya risk awareness, keselarasan proses evaluasi risiko perusahaan dengan risk based pada proses audit, dan kendala pada proses migrasi kartu magnetic strip.
Kata Kunci: ATM *(Authomatic Teller Machine)*, Framework RiskIT, Kendala Manajemen Risiko.
Correspondence. wahyu.firmandani@ui.ac.id, malik@ui.ac.id
History of article. Received: Oktober 2018, Revision: Januari 2019, Published: Maret 2019

1. PENDAHULUAN

Teknologi Informasi saat ini telah menjadi kebutuhan setiap organisasi bisnis atau perusahaan, terbukti bahwa saat ini nyaris semua organisasi bisnis atau perusahaan menggunakan Teknologi Informasi pada setiap *value chain* bisninya. Namun tidak dapat dipungkiri, adanya kemajuan Teknologi Informasi membawa risiko yang mengakibatkan tidak tercapainya tujuan dari penggunaan TI, jika risiko tersebut tidak dikelola dengan baik. Kemajuan teknologi yang pesat bisa menjadi peluang bagi bisnis untuk meningkatkan efektivitasnya, namun disisi lain juga dapat menjadi ancaman bagi keberlangsungan bisnis seperti yang dialami Bank X beberapa waktu lalu. Pada bulan Maret 2018, sebanyak 33 nasabah Bank X Kantor Cabang (KC) Kediri mengalami kehilangan dana secara misterius *(ilegal transaction)*. Direktur Digital Banking dan Teknologi Informasi Bank X memastikan kejadian tersebut merupakan bentuk kejahatan dengan mekanisme *skimming*. (Hidayat, 2018).

Dorongan untuk tumbuh yang tidak diiringi dengan manajemen risiko yang ketat, pada akhirnya membawa kerugian tidak hanya bagi Bank X tetapi juga para pemegang kepentingan (*stakeholder)*. Sesuai dengan teori keagenan *(agency cost)* Bank X sebagai penyedia jasa perbankan (sebagai agen) memiliki kewajiban untuk menjaga keamanan dana nasabah yang telah dipercayakan kepadanya, serta menjalankan proses bisnis perbankan yang aman sesuai peraturan OJK dalam rangka stabilitas perekonomian nasional dan menjaga amanah para pemegang saham mayoritas (pemerintah selaku pemegang saham dwiwarna) dan juga pemegang saham minoritas.

Berkaca dari krisis yang terjadi beberapa waktu lalu dan permasalahan yang muncul di industri perbankan yang memiliki risiko potensial bagi perekonomian, OJK melalui P.OJK No. 14/ SEOJK.03/ 2017 mewajibkan kepada seluruh Bank Umum untuk mengimplementasikan manajemen risiko pada aktivitas perbankannya, termasuk di dalamnya risiko teknologi informasi (OJK, 2017).Terdapat delapan risiko yang harus dikelola penyedia jasa perbankan di Indonesia, yakni risiko pasar, risiko kredit, risiko likuiditas, risiko hukum, risiko kepatuhan, risiko stratejik, risiko reputasi, dan risiko operasional. Kedelapan risiko tersebut wajib dikelola Bank Umum untuk mengantisipasi kegagalan perbankan yang pada akhirnya mengganggu stabilitas perekonomian nasional. Risiko Operasional yang wajib dikelola Bank meliputi: *People, Process,* dan IT. Meskipun Bank X berkomitmen untuk menanggung seluruh kerugian yang diakibatkan kasus skimming, namun tidak dapat dipungkiri pemberitaan dan citra buruk mempengaruhi kepercayaan masyarakat terhadap industri perbankan Indonesia. Apalagi Bank X merupakan Bank BUKU 4 dengan aset paling besar *(bank only)* posisi 31 Desember 2018 (Bank X, 2019)**.** Untuk menganalisis kendala penerapan manajemen risiko yang mengakibatkan adanya kasus skimming ATM Bank X , dapat dipergunakan bestpractise *Risk IT Framework* yang dirumuskan ISACA tahun 2009.

Kasus skimming ATM Bank X mengakibatkan kerugian finansial bagi 33 nasabah dengan total eksposur mencapai Rp 145.000.000,-. Kasus tersebut merupakan paparan dari Risiko Teknologi Informasi (bagian dari risiko operasional) yang wajib dikelola oleh Bank Umum karena dapat mempengaruhi reputasi dan kepercayaan masyarakat kepada sistem perbankan di Indonesia. Adanya paparan risiko operasional berupa kasus skimming ATM pada Bank X menunjukkan bahwa adanya manajemen risiko yang belum optimal di perusahaan. Padahal untuk mengurangi konflik yang muncul akibat kepentingan agen (manajemen) dan principal (pemilik saham dan nasabah), penerapan manajemen risiko menurut Schoeck (2002: 81) dalam Ichsan (2013) mampu mengurangi *agency cost* dan menambah value perusahaan. Manajemen risiko juga mampu menjadi alat pengawasan untuk mengurangi informasi asimetris antara agen dan principal, sehingga manajer dihindarkan dari tindakan dan pengambilan keputusan yang bersifat oportunis yang dapat merugikan *stakeholder*.

Pada tahun 2009, ISACA (didirikan pada tahun 1967 di Amerika Serikat) mengeluarkan *framework* standar untuk mengelola risiko teknologi informasi yaitu *Risk IT Framework* yang menggabungkan *Risk Governance, Risk Evaluation, and Risk Response* untuk membantu perusahaan dalam mengelola risiko teknologi informasi.*Risk IT Framework* merupakan metode manajemen risikoTI yang dapat dijadikan pedoman bagi perusahaan agar kasus serupa tidak terjadi kembali. Rumusan masalah yang dijawab melalui penelitian ini adalah "Bagaimanakah kendala penerapan manajemen risiko Teknologi Informasi (TI) pada kasus *skimming* ATM Bank X sesuai dengan *Risk IT Framework*?". Dengan tujuan yang hendak dicapai yakni untuk menganalisis kendala manajemen risiko Teknologi Informasi pada Kasus *Skimming* Bank X sesuai dengan *Risk IT Framework* untuk mencegah risiko yang sama terjadi kembali.

Menurut Ellet (2007) manfaat penelitian ialah untuk memperbaiki faktor negatif dan meningkatkan nilai positif, untuk meningkatkan kondisi yang ada dengan mengatasi masalah, untuk mengefektifkan implementasi keputusan, dipergunakan membantu untuk menganalisis dan mengevaluasi masalah, serta dipergunakan untuk menyusun ketentuan. Penelitian ini diharapkan memberikan manfaat sebagai berikut: (1) Memberikan rekomendasi penerapan manajemen risiko pada kasus skimming ATM sesuai dengan Risk IT *Framework* agar permasalahan serupa tidak terjadi di masa mendatang, (2) Memberikan masukan *(inside)* kepada regulator, khususnya OJK sebagai penyusun kebijakan manajemen risiko dan bagi pelaku industri perbankan untuk membangun dan menerapkan manajemen risiko yang baik dalam menghadapi risiko teknologi informasi perbankan, dan (3) Memberikan wawasan bagi keilmuan dan akademisi mengenai konsep dan penerapan manajemen risiko teknologi informasi

dalam menghadapi risiko TI yang muncul seiring dengan kemajuan teknologi dengan pendekatan *Risk IT Framework*

2. KERANGKA PENELITIAN & HIPOTESIS

Penelitian terdahulu mengenai risiko TI telah dilakukan oleh Fleischmann (2011) dan Iskandar (2011). Dalam penelitiannya menjelaskan adanya perkembangan TI mendorong berkembangnya pula risiko TI yang harus dikelola, begitupun berkembangnya metode dan framework yang dapat dipergunakan untuk mencegah risiko TI seperti kasus skimming tidak terjadi kembali. Sebagaimana tergambar pada teori keagenan, terdapat dua pelaku ekonomi yang saling bertentangan yaitu prinsipal dan agen. Akibat adanya kepentingan yang berbeda di antara keduanya dan asimetris informasi antara pengelola (agen) yang memiliki informasi lebih dalam dibanding dengan pemilik (prinsipal) maka muncullah yang dinamakan dengan *agency conflict,* sehingga dibutuhkan metode untuk menjembatani konflik yang ada, yakni salah satunya dengan menerapkan manajemen risiko yang baik. *Risk ITFramework* merupakan *bestpractice methode* untuk mengetahui kendala penerapan manajemen risiko yang mengakibatkan kasus skimming ATM Bank X.

Penelitian sebelumnya pernah dilakukan Fleischmann (2011) yang membahas mengenai manajemen risiko IT pada industri perbankan. Dari hasil penelitian Fleischmann, sistem manajemen risiko di industri perbankan memiliki banyak kelemahan pada *IT Governance* dan *IT Resource* yang mendorong adanya krisis di beberapa negara yang pada akhirnya membutuhkan intervensi dari pemerintah. Bank – bank yang bertahan setelah krisis juga masih akan memiliki paparan risiko yang harus dikelola untuk menghindari kegagalan yang sama di kemudian hari. Oleh karenanya, berkembang pendekatan untuk meningkatkan manajemen risiko dan tata kelola IT diantaranya ialah *Risk IT Framework* di sektor perbankan. Dalam penelitiannya, Fleischmann memberikan pemahaman atas manajemen risiko dalam mengelola krisis dan kerangka yang paling tepat dalam menyelesaikan masalah TI di sektor perbankan.

Penelitian lainnya juga pernah dilakukan Iskandar (2011) yang membahas manajemen risiko TI dengan pendekatan *Risk IT Framework* pada kasus pembobolan EDC Bank Permata. Dalam penelitiannya, Iskandar menyajikan implementasi konsep manajemen risiko pada kasus pembobolan nasabah Bank Pemata melalui EDC dengan pendekatan Risk IT Framework melalui tiga tahapan yakni *Risk Governance (RG), Risk Evaluation (RE), dan Risk Response (RR).* Dari hasil penelitiannya, disimpulkan bahwa Risk IT *Framework* merupakan pendekatan yang tepat untuk melakukan menyelesaikan kasus yang terjadi pada Bank Permata. Perbedaan penelitian ini dengan yang dilakukan oleh Iskandar (2011) terletak pada kasus dan unit analisisnya. Jika pada penelitian sebelumnya kasus yang dianalisis merupakan kasus *carding* pada saat nasabah bertransaksi menggunakan kartu kredit di EDC, maka kasus yang dianalisis pada penelitian ini ialah kasus *skimming* kartu ATM.*Carding* merupakan kejahatan *cybercrime* yang mencuri data nasabah kartu kredit maupun debet pada saat menggesekkan pada alat pembayaran yang ada (EDC), sedangkan *skimming* merupakan pencurian data nasabah yang ada pada *magnetic strip* kartu debet/ ATM.

Teori keagenan oleh Jensendan Meckling (1976) dalam Ichsan (2013) mengemukakan tentang pertentangan prilaku dua pelaku ekonomi antara prinsipal dan agen. Agen merupakan satu atau lebih orang yang diperintah oleh orang lain (principal) untuk melakukan suatu jasa dan mengambil keputusan terbaik atas nama principal (Ichsan, 2013). Adanya konflik kepentingan antara manajemen yang memiliki informasi lebih dalam terkait dengan kondisi perusahaan dan pihak principal yang mempercayakan kewenangan kepada agen, maka memunculkan masalah yang disebut dengan *agency conflict*, yakni konfik yang muncul antara principal dan agen karena memiliki kepentingan yang saling berlawanan. Menurut Meisser, et al., (2006:7) dalam Ichsan (2013) hubungan keagenan memunculkan dua masalah, yakni : (a) adanya informasi asimetris, yakni kondisi di mana agen (manajemen) memiliki lebih banyak informasi baik terkait dengan kondisi

keuangan perusahaan maupun kondisi operasional entitas dibandingkan dengan infromasi yang dimiliki pemilik (principal); dan (b) adanya konflik kepentingan, disebabkan perbedaan tujuan yang ingin dicapai, yakni manajemen sering kali bertindak bersebrangan dengan kepentingan pemilik.

Untuk mengurangi konflik yang muncul akibat kepentingan agen dan principal, penerapan manajemen risiko menurut Schoeck (2002: 81) dalam Ichsan (2013) mampu mengurangi *agency cost* dan menambah value perusahaan. Manajemen risiko juga mampu menjadi alat pengawasan untuk mengurangi informasi asimetris antara agen dan principal, sehingga manajer dihindarkan dari tindakan dan pengambilan keputusan yang bersifat oportunis yang dapat merugikan *stakeholder*.

Risko TI Framework merupakan suatu kerangka pengelolan risiko TI yang didasarkan pada seperangkat prinsip pengelolaan risiko TI yang efektif. *RiskIT Framework* merupakan salah satu perangkat COBIT yang merupakan kerangka tata keloladan pengendalian yang komprehensif berbasis TI dan layanan. Jika COBIT menyediakan satu perangkat kontrol untuk mengurangi risiko TI, maka *RiskIT Framework* merupakan kerangka untuk mengidentifikasi, mengatur, dan mengelola risiko IT. **Gambar 2.1 *Risk IT Framework*** memperlihatkan tiga domain dalam *Risk IT Framework* yakni tata kelola risiko, evaluasi risiko, dan respon terhadap risiko. Setiap domain terdapat tujuan yang harus dicapai, dan dibagi dalam beberapa sasaran proses serta aktivitas yang dilakukan untuk mencapainya. Dalam definisi RiskIT, risiko IT disorot sebagai risiko bisnis. Di banyak perusahaan, TI terkait resiko dianggap sebagai komponen risiko operasional, misalnya, dalam industri keuangan atau perbankan.

Sumber : ISACA (2019) Hlm 15

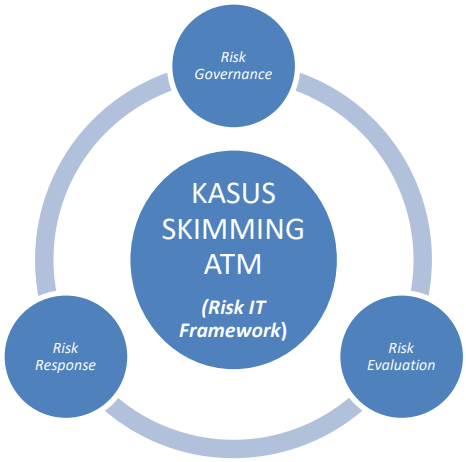
Gambar 1. *Risk IT Framework*

Ketiga domain dari Risk TI Framework dipergunakan sebagai pedoman bagi perusahaan yang menjadikan TI sebagai enabler dalam proses bisnisnya sebagaimana yang disampaikan oleh Iskandar (2011) riskIT Framework merupakan kerangka yang tepat untuk untuk menghasilkan sebuah keputusan bermanfaat dalam pembaharuan risiko TI pada bank.

Tujuan pada domain *Risk Governance* pada *Risk IT Framework* ialah untuk memastikan bahwa praktek manajemen risiko TI tertanam dalam perusahaan, memungkinkan perusahaan untuk mengamankanrisiko yang optimal untuk disesuaikan kembali melalui sasaran proses sebagai berikut: (1) Membangun Pandangan Perusahaan Mengenai Risiko, (2) Integrasikan dengan ERM, dan (3) Pengambilan Keputusan berbasis Risiko. Tujuan pada domain *Risk Evaluation* pada *Risk IT Framework* ialah memastikan bahwa risiko dan peluang TI disajikan dengan relevan melalui sasaran proses sebagai berikut: (1) Pengumpulan Data, (2) Analisis risiko, dan (3) Menjaga Profil Risiko. Tujuan pada domain *Risk Response* pada *Risk IT Framework* ialah memastikan bahwa isu-isu risiko terkait TI, kesempatan dan peristiwa ditangani dengan efektif dan sejalan dengan prioritas bisnis melalui sasaran proses sebagai berikut: (1) Mengartikulasikan Risiko, (2) Mengelola Risiko, dan (3) Bereaksi Terhadap Peristiwa.

Peneliti akan melakukan analisis kendala manajemen risiko teknologi informasi pada kasus skimming ATM Bank X menggunakan *Risk IT*

Framework dengan kerangka penelitian digambarkan pada **Gambar 2.2** yang meliputi fase: *Risk Governance (RG), Risk Evaluation (RE),* dan *Risk Response (RS). RG m*embahas mengenai pandangan perusahan mengenai risiko, integrasi dengan strategi perusahaan dan pengambilan keputusan berbasis risiko. *RE m*embahas mengenai pengumpulan data, analisis risiko dan control atas profil risiko *(maintenance). RS m*embahas mengenai mengartikan risiko, mengelola risiko dan bereaksi pada suatu peristiwa. *Risk IT Framework* dipergunakan untuk mengantisipasi risiko TI yang ada agar tidak muncul di kemudian hari.



Sumber: Olahan Penulis, 2019.

Gambar 2. Kerangka Penelitian

Munculnya kasus skimming ATM Bank X menunjukkan adanya kelemahan dari penerapan manajemen risiko operasional yang tampak dari penurunan profil risiko operasional Bank X dibandingkan dengan tahun sebelumnya. Oleh karenanya analisis menggunakan ketiga domain *RiskTI Framework* bermaksud untuk mengetahui kendala yang dihadapi Bank X dari segi tata kelola risiko, evaluasi risiko dan tindak lanjut (response) risiko. Fleischmann (2011) menyatakan dari beberapa pendekatan manajemen risiko yang dapat dipergunakan sebagai rujukan, Risk TI merupakan salah satu kerangka pada kuadran 4 yang menunjukkan relevansinya dengan industri perbankan dengan penggunaan TI yang masif.

3. METODE PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dengan jenis penelitian studi kasus. Studi kasus menurut Ellet (2007) studi kasus dipergunakan untuk menganalisis suatu kasus dengan memberikan makna antara konsep bisnis dengan permasalahan yang dihadapi. Penelitian menggunakan metode studi kasus dipilih karena pertanyaan penelitian mengenai fenomena kasus skimming ATM Bank X dikaitkan dengan manajemen risiko teknologi informasi berdasarkan ketiga fase manajemen risiko TI pada *Risk IT Framework* hanya dapat digali melalui studi kasus. Penelitian ini menggunakan pendekatan kualitatif. Penelitian kualitatif merupakan penelitian yang berguna untuk memahami fenomena yang dialami oleh objek penelitian seperti motivasi, persepsi, perilaku, tindakan, secara holistik dengan cara mendeskripsikan dalam bentuk kata-kata dan bahasa (Moleong, 2010). Jenis penelitian yang digunakan dalam penelitian ini adalah studi kasus. Penelitian menggunakan metode studi kasus dipilih karena pertanyaan penelitian mengenai fenomena kasus skimming ATM Bank X dikaitkan dengan manajemen risiko teknologi informasi berdasarkan ketiga fase manajemen risiko TI pada *Risk IT Framework* hanya dapat digali melalui studi kasus. Studi kasus menurut Ellet (2007) studi kasus dipergunakan untuk menganalisis suatu kasus dengan memberikan makna antara konsep bisnis dengan permasalahan yang dihadapi.

Data yang dipergunakan dalam penelitian ini merupakan data kualitatif yang mencakup hasil wawancara staf senior manajemen operasional, staf Fungsi MR UKO, serta dokumentasi atas kebijakan dan prosedur tata kelola dan manajemen risiko TI, modul perangkat Manajemen Risiko berupa modul RCSA *(Risk Control Self Assessment)*, modul MI (Manajemen Insiden), modul MR (Manajemen Risiko), modul Maturitas, dan laporan audit TI untuk mengetahui kendala dalam penerapan manajemen risiko yang mengakibatkan munculnya kasus skimming nasabah Bank X. Dalam studi kasus ini, peneliti melakukan pengumpulan data melalui dua sumber data, sumber data primer melalui hasil wawancara *(interview)*. Moleong (2010:186) wawancara

merupakan sebuah percakapan yang dilakukan oleh kedua belah pihak yang memiliki maksud tertentu, yakni pewawancara yang mengajukan pertanyaan dan terwawancara yang memberikan jawaban. Adapun tahapan yang dilakukan pada saat wawancara menurut Wilkinson dan Birmingham seperti yang dikutip Shauki (2018) dapat dilakukan sebagai berikut: (1) *Draft the interview, (2) Pilot your question, (3) Selected your interviewees, (4) Conduct the interviews,* dan (5) *Analyse the interview data.* Dalam melakukan wawancara, peneliti mengunakan pendekatan petunjuk umum wawancara *(semi structured)*. Dalam penelitian ini wawancara mendalam dilakukan kepada staf senior manajemen risiko dan staf senior Fungsi Manajemen Risiko (FMR) UKO. Sumber data sekunder, menurut Maulidi (2016) merupakan sumber data yang diperoleh dengan media perantara atau tidak langsung yang dapat berupa catatan, dokumentasi, buku,bukti yang telah ada, atau arsip baik yang dipublikasikan maupun yang tidak dipublikasikan. Sumber data sekunder didapat melalui dokumentasi proses manajemen risiko yang meliputi: *risk governance, risk evaluation* dan *risk response.* Dokumen yang dianalisis ialah kebijakan dan prosedur tata kelola dan manajemen risiko TI, modul perangkat Manajemen Risiko berupa modul RCSA *(Risk Control Self Assessment)*, modul MI (Manajemen Insiden), modul MR (Manajemen Risiko), modul Maturitas, dan laporan audit TI.

Shauki (2018) pendekatan kualitatif dapat dilakukan menggunakan beberapa cara diantaranya: (1) *Content Analysis, (2) Thematic Analysis, dan (3) Constant Comparative Analysis.* Dalam melakukan analisis, penelitian ini menggunakan metode *content analysis* atas hasil wawancara, dan dokumentasi untuk mendapatkan informasi yang komperhensif mengenai kendala yang dihadapi perusahaan dalam mengelola risiko TI yang mengakibatkan munculnya kasus *skimming* sebagai bentuk eksposur risiko operasional perbankan yang tidak dikelola dengan baik. *Content analysis* atas keseluruhan data bertujuan untuk mendapatkan informasi yang relevan mengenai fenomena kendala penerapan manajemen risiko dari ketiga fase proses manajemen risiko pada *Risk IT Framework*. Fase yang dimaksud meliputi: (1) *Risk Governance, (2) Risk Evaluation, dan (3)Risk Response*

Unit analisis data dalam penelitian ini adalah *single unit* dengan *single case study* yakni menyoroti kasus *skimming* pada ATM Bank X. Fokus kasus yang akan diteliti ialah menganalisis kendala manajemen risiko TI pada kasus skimming Bank X melalui pendekatan *Risk IT Framework* agar kejadian serupa tidak terulang kembali.

4. HASIL DAN PEMBAHASAN

Skimming kepada nasabah simpanan Bank X KC Kediri dilakukan dengan sangat rapi melibatkan beberapa perangkat teknologi yang dipasang di ATM, yakni: Kamera Pencuri PIN, *Skimmer, Deep Insert Skimmer,* dan PIN Pad Palsu. *Skimming* dilakukan dengan cara memasang kamera pencuri PIN yang berukuran kecil dengan kisaran diameter 0,5 – 1 cm yang diletakkan di sekitar PIN pad/ PIN pad cover atau disamarkan di dalam benda-benda seperti lampu ruangan, speaker, dan bagian atas monitor untuk merekam PIN yang dimasukkan saat transaksi. Selain itu, pelaku juga menempelkan skimmer di atas atau depan *card reader* asli untuk menyadap data di garis magnetik kartu ATM saat kartu dimasukkan. Skimmer merupakan alat untuk menyecan data atau informasi yang ada pada garis magnetik kartu ATM atau kartu debet yang berbentuk sangat mirip dengan *card reader* asli di ATM. Proses menempelkan skimmer menggunakan deep insert skimmer yang merupakan varian *skimmer* dengan dimensi mirip dengan kartu ATM, berbahan logam, dan dilengkapi dengan magnet atau pengait agar ketika dimasukkan ke dalam lubang *card reader* dapat menempel dengan sempurna. Selanjutnya, penggunaan PIN Pad Palsu diletakkan di atas PIN pad aslinya untuk merekam PIN yang dimasukkan saat transaksi.

Setelah pelaku berhasil menggandakan informasi nasabah yang ada di magnetic strip dan mengetahui PIN nasabah, maka pelaku melakukan transaksi tarik tunai maupun melakukan transfer dana nasabah ke rekening milik pelaku. Sehingga jika dikaitkan dengan

otorisasi transaksi, seolah-olah transaksi dilakukan oleh nasabah pemilik rekening dengan PIN yang masih berlaku, namun pada kenyataannya transaksi tersebut merupakan transaksi illegal yang dilakukan oleh tersangka.

Sumber: Divisi TI Bank X (2018)

Gambar 1. Perangkat Skimming ATM Bank X

Tata Kelola Risiko Bank X

Selaku Bank BUKU 4 yang memiliki aset TI dan jaringan yang sangat luas, Bank X menjadikan TI tidak hanya sebagai *support* (pendukung) bisnis, tetapi juga *enabler* (penggiat) bisnis. Dengan kesadaran tentang pentingnya TI sebagai bagian dari pengelolaan proses bisnis, Bank X menjalakan tata kelola risiko penggunaan TI pada setiap pengambilan keputusan melalui beberapa kebijakan dan prosedur, yakni yang menyangkut Organisasi dan Fungsi MR, Kebijakan Tata Kelola dan Manajemen Risiko TI serta Budaya Sadar Risiko.

Organisasi dan Fungsi Manajemen Risiko Bank X

Sesuai dengan *RiskIT Framework*, Bank X telah menjalankan tata kelola risikonya dengan baik dan *embaded* pada setiap pengambilan keputusan, hal tersebut dibuktikan dengan pembentukan Direktur bidang yang membawahi Divisi Manajemen Risiko. Direktur bidang manajemen risiko membawahi lima divisi yakni Divisi Kebijakan Risiko Kredit, Divisi Risiko Enterprise dan Manajemen Portofolio, Divisi Manajemen Risiko Operasional dan Pasar, Divisi Analisis Risiko Kredit dan Divisi Restrukturisasi dan Penyelesaian Kredit. Bank X mempertimbangkan risiko pada setiap pengambilan keputusannya dengan mendirikan satu divisi khusus yang mengintegrasikan risiko dengan tujuan strategik perusahaan yakni Divisi Enterprise dan Manajemen Portofolio (EMP). Sedangkan untuk Risiko Operasional yang menyangkut penggunaan teknologi informasi, pengelolaannya dilakukan oleh Divisi Teknologi Informasi Bank X yang bekerja sama dengan Divisi Manajemen Operasional dan Pasar (MOP) karena Risiko Teknologi Informasi merupakan bagian dari risiko operasional. Direktur Bidang Digital Banking dan Teknologi Informasi menyupervisi Divisi Perencanaan dan Pengembangan TI, Divisi Operasional TI, Divisi Satelit dan Jaringan Telekomunikasi dan Divisi Digital Centre OF Execellence. Bank X memahami betul bahwa posisi dan fungsi Teknologi Informasi (TI) pada industri perbankan sangat strategis dan penting mengingat peran TI bukan hanya sebagai support, melainkan sebagai enabler bagi kegiatan bisnis serta dengan adanya pengunaan TI dalam kegiatan operasional bank meningkatkan risiko yang dihadapi, sehingga diperlukan penerapan manajemen risiko yang efektif. Oleh karenanya, dalam tata kelola TI Bank X, peran dan tanggung jawab pejabat tinggi pada Satuan Kerja TI, meliputi: merumuskan, mengoordinasikan, menerapkan kebijakan dan pengembangan TI, memastikan kecukupan, melakukan pengawasan, pelaporan pelaksanaan TI sampai dengan memastikan kontrak tertulis Bank dengan penyedia jasa TI diatur dengan aman.

Pengelolaan risiko yang ada di Bank tidak hanya berhenti pada level Kantor Pusat (Head Office) tetapi setiap pengambilan keputusan sudah melekat atau embadded dengan seluruh level bisnis terkecil atau unit entity perusahaan dengan membentuk Fungsi Manajemen Risiko di setiap Unit Kerja Operasional Bank. Adapun lingkup pelaksanaan fungsi MR meliputi seluruh aktivitas unit kerja operasional (UKO) yang terkait dengan aktivitas perbankan baik langsung maupun tidak langsung dari Kantor Pusat (KP) sampai dengan tingkat Kantor Cabang (KC), Kantor Cabang Khusus (KCK), Kantor Cabang Pembantu (KCP), Sentra Layanan Prioritas (SLP), dan unit kerja Luar Negeri (UKLN). Termasuk di dalamnya sebagai UKO Bank X ialah Divisi Manajemen Risiko, Divisi Kepatuhan dan Audit Intern.

Kebijakan Tata Kelola dan Manajemen Risiko TI (KTKMRTI) Bank X

Dalam melakukan pengelolaan risiko teknologi informasi yang melekat sejalan dengan penggunaan TI pada proses bisnisnya, Bank X menyusun KTKMRTI sebagai bentuk pengamanan atas risiko yang berpotensi membawa dampak negative bagi bisnis Bank. Adapun dalam kebijakan tersebut domain yang diatur telah mencakup keseluruhan proses bisnis yang melibatkan penggunaan IT yang secara spesifik mengatur hal-hal mengenai: Manajemen, Pengembangan dan Pengadaan TI, Aktivitas Operasional Teknologi Informasi, Jaringan Komunikasi, Pengamanan teknologi Informasi, Rencana Pemulihan Bencana, Layanan Perbankan Elektronik, Audit Intern Teknologi Informasi, Penggunaan Pihak Penyedia Jasa TI, Penyediaan Jasa Teknologi Informasi oleh Bank, dan Pelaporan Teknologi Informasi. Seluruh Satuan Kerja Teknologi Informasi Bank dan pihak-pihak yang berkaitan diwajibkan untuk mematuhi KTKMR TI Bank X.

Budaya Sadar Risiko Bank X

Bank X menyusun kebijakan mengenai budaya sadar risiko dengan maksud untuk memberikan arahan kepada seluruh pekerja dalam penerapan Budaya Sadar Risiko. Dengan fondasi visi, misi, core value dan budaya kerja, Bank X menyusun elemen budaya sadar risiko yang mencakup: komitmen, manajemen kinerja, tata kelola risiko, komunikasi, pelatihan dan pengembangan, pelaporan dan pemantauan. Di samping itu sesuai dengan yang disyaratkan OJK, Bank X menerapkan budaya sadar risiko yang meliputi empat pilar sebagai berikut: (1) Pengawasan aktif dari Direksi dan Dewan Komisaris, (2) Kecukupan Kebijakan dan prosedur MR serta penetapan limit, (3) Kecukupan proses identifikasi, pengukuran, pemantauan dan pengendalian serta SIM MR, (4) Sistem Pengendalian Intern yang Menyeluruh

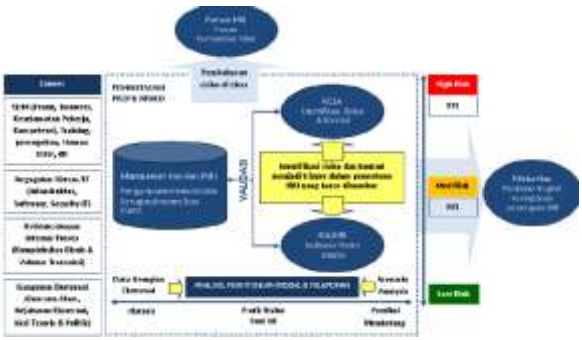
Kendala Penerapan Manajemen Risiko pada Tata Kelola Risiko Bank X

Secara umum Bank X telah menjalankan tata kelola risiko yang baik dalam rangka menjaga kelangsungan bisnisnya, namun ada beberapa kendala pada penerapannya yang pada akhirnya membawa dampak terjadinya kasus skimming ATM pada bulan Maret 2018 di UKO Kediri. Kendala tata kelola risiko yang dimaksud ialah sebagai berikut: (1) Pada kasus *Skimming* yang terjadi di ATM KC Kediri Bank X, meskipun merupakan risiko Teknologi Informasi tetapi lokasi kejadiannya merupakan unit kerja operasional (UKO) Bank X. Sesuai dengan prosedur yang berlaku pada Bank X, seharusnya aduan nasabah dan informasi apapun mengenai kejadian skimming di UKO Bank X dilaporkan ke kantor pusat sebagai bagian dari paparan risiko operasional perbankan melalui sistem pelaporan manajemen insiden maupun forum MR Bank X. Namun karena secara hierarki organisasi Fungsi MR tidak berada di bawah supervisi langsung Divisi Operasional dan Pasar (MOP), hal tersebut melemahkan objektivitas dan independensi FMR untuk melaporkan permasalahan yang dihadapi di unit kerjanya. UKO Bank X secara organisasi berada dibawah supervisi Divisi Jaringan, sedangakan FMR masing-masing unit kerja kantor pusat berada dibawah supervisi Divisi bisnis masing-masing, sedangkan pada dasarnya level antara Divisi Jaringan, Divisi MOP dan Divisi lainnya yang ada di Kantor Pusat adalah sejajar atau sama. (2) Kebijakan Budaya Risiko yang telah disusun sebagai pedoman seluruh lapisan bisnis untuk tanggap dan responsif atas berbagai risiko yang berpotensi melemahkan atau merugikan perusahaan pada kenyataan belum berjalan optimal sebagaimana yang diharapkan oleh perusahaan. Hal tersebut tercermin dari laporan forum MR yang wajib dilaporkan oleh masing-masing fungsi MR di UKO Bank X minimal satu kali dalam sebulan, tidak dipenuhi oleh setiap level entity Bank X. Beberapa dari UKO Bank X melewatkan laporan tesebut, padahal *inside* laporan risiko yang dihadapi oleh Bank X sangat bermanfaat dan berperan penting untuk menentukan arah pengendalian dan kebijakan perusahaan secara keseluruhan. Budaya sadar risiko yang *relative* masih rendah di beberapa UKO Bank X, tercermin dari Laporan Forum MR yang tidak dilaporkan oleh UKO Bank X kepada Divisi MOP. Selain itu, dari hasil wawancara Fungsi MR yang ada di UKO Bank X, didapati bahwa denda maupun sanksi dari regulator

terkait dengan penyampaian kewajiban perbankan yang seharusnya menjadi salah satu indikasi pengendalian atau kontrol atas risiko operasional yang tidak berjalan secara efektif, tidak dilaporkan sebagai bentuk lemahnya pengendalian yang ada pada perangkat Risk Operasional Assessment Bank X, sehingga realita yang ada tidak sepenuhnya terlaporkan pada saat UKO melakukan penilaian sendiri (RCSA) atas kontrol yang telah dibuat, sehingga awareness masing-masing individu yang terlibat sebagai fungsi MR di Bank X belum menjalankan budaya sadar risiko secara komprehensif pada setiap pengambilan keputusan penting perusahaan.

Evaluasi Risiko Bank X

Seiring dengan meningkatnya kompleksitas bisnis dan operasional bank, kemajuan Teknologi Informasi serta meningkatnya kompetisi pada industri perbankan, maka risiko yang dihadapi juga semakin meningkat. Dalam melaksanakan evaluasi dan *assessment* risiko operasional, Bank X telah mengembangkan sistem yang dapat mengidentifikasi risiko-risiko yang dapat berdampak negatif pada kinerja keuangan dan bisnis perbankan dengan sebutan *Operational Risk Assessor* (OPRA). OPRA merupakan perangkat manajemen risiko operasional yang meliputi modul *Risk Control Self Assessment* (RCSA), Manajemen Insiden (MI), Indikator Risiko Utama (IRU), Forum MR, dan Maturitas.



Sumber: Bank X, 2018

Gambar 2. Perangkat Manajemen Risiko Operasional

Berikut ini merupakan gambar hubungan antar perangkat Manajemen Risiko Operasional. Kelima perangkat MRO tersebut memiliki keterkaitan dan hubungan yang erat dalam proses penerapan Manajemen Risiko: (1) MI merupakan database kejadian kerugian yang digunakan untuk mengelola insiden/ *loss event* mulai ditemukan hingga penyelesaian, MI berfungsi sebagai alat kontrol untuk melakukan validasi penilaian *risk issue* dan kontrol pada penilaian RCSA. Dengan kata lain, penilaian prediksi risiko melalui perangkat RCSA harus mempertimbangkan MI sebagai sumber data. (2) MI juga berfungsi sebagai alat kontrol dalam validasi pemantauan KRI/ IRU. Hal ini dikarenakan MI juga dapat digunakan sebagai sumber data penetapan KRI/ IRU. (3) KRI/ IRU digunakan untuk memantau hasil penilaian prediksi risiko melalui perangkat RCSA sehingga Pemimpin UKO/ FMR dapat langsung memitigasi risiko apabila terdapat peningkatan potensi risiko. (4) Pembahasan permasalahan risiko dan pengelolaannya pada Forum MR dapat memanfaatkan hasil penilaian RCSA, hasil pemantauan KRI/ IRU dan kejadian kerugian yang dicatat dalam MI. (5) Implementasi perangkat Manajemen Risiko Operasional di UKO juga akan menggambarkan kematangan penerapan Manajemen Risiko yang tercermin dalam Penilaian Maturitas

Risk Control Self Assessment (RCSA)

RCSA adalah perangkat manajemen risiko operasional yang bersifat kualitatif dan prediktif yang digunakan untuk mengidentifikasi dan mengukur risiko operasional dengan menggunakan dimensi dampak (impact) dan frekuensi (likelihood). Pelaksanaan penilaian RCSA dilakukan oleh UKO secara periodik, yaitu setiap 6 bulan sekali pada bulan pertama di awal semester. Penilaian Risk Issue RCSA dilakukan oleh UKO terhadap Inherent Risk (IRS), Penilaian Efektifitas Kontrol (NEK) dan penilaian Residual Risk (RRS). Penilaian RCSA dilakukan dengan mempertimbangkan historis data kejadian kerugian dalam MI, Temuan Audit dan penilaian FMR apabila terdapat kelemahan kontrol. Pelaksanaan Penilaian RCSA di Bank X meliputi tahapan pertama Penentuan Risk Issue dan Risk Template. Penentuan risk issue untuk seluruh level UKO dilakukan oleh Divisi MR dan berkoordinasi dengan SAI, Unit Kerja Koordinator

Risiko Spesifik, Bagian MRK Kanwil dan UKO terkait. Pengkinian risk issue dan kontrol pada RCSA dilakukan setiap ada perubahan proses bisnis, adanya perubahan organisasi, Produk dan atau Aktivitas Baru (PAB) dll. Tahapan kedua Penilaian RCSA dan Pembuatan RTL. Penilaian RCSA memanfaatkan informasi dari Data kerugian di MI, perubahan trend KRI/IRU, LHA Internal maupun Eksternal, Hasil Penilaian RCSA sebelumnya, Progress Pelaksanaan RTL Periode sebelumnya. Pembuatan RTL dilakukan dalam perbaikan kontrol/ prosedur atau usulan kontrol baru. RTL disusun apabila skor NEK minimal 3/ rating kontrol minimum kuning. Tahapan ketiga Persetujuan RCSA. Persetujuan dilakukan dengan memastikan bahwa risk issue dan kontrol pada template RCSA telah dinilai sesuai dengan historis data UKO (hasil penilaian periode sebelumnya, progress RTL, LHA, Hasil Pemantauan KRI, insiden kerugian MI dan kelemahan sisdur di UKO). Selain itu, Pemimpin UKO wajib memperhatikan kesesuaian RTL dengan kelemahan kontrol yang di checklist. Tahapan keempat Verifikasi RCSA. Verifikasi atas hasil penilaian RCSA UKO dilakukan oleh Bagian MRK Kanwil/ Divisi MR setelah hasil penilaian RCSA disetujui oleh Pemimpin UKO. Verifikasi RCSA dilakukan dengan memastikan bahwa risk issue dan kontrol pada template RCSA telah dinilai sesuai dengan historis data UKO (hasil penilaian periode sebelumnya, progress RTL, LHA, Hasil Pemantauan KRI, insiden kerugian MI dan kelemahan sisdur di UKO) memperhatikan kesesuaian RTL dengan kelemahan kontrol yang di checklist. Tahapan kelima Pemantauan Pelaksanaan RCSA. Pemantauan Pelaksanaan RCSA dilaksanakan oleh FMR Unit Kerja, Pemimpin Unit Kerja, Bagian MRK Kanwil dan Divisi Manajemen Risiko sesuai kewenangan dan tanggung jawab masing-masing. Pemantauan pelaksanaan RCSA meliputi: (1) Pemantauan atas penilaian RCSA Unit Kerja pada saat siklus penilaian RCSA, (2) Progress pelaksanaan RTL atas risk issue yang telah dibuat Unit Kerja, dan (3) Efektifitas RTL atau mitigasi risiko yang dilakukan. Tahapan keenam Konsolidasi RCSA. Konsolidasi dilakukan untuk setiap risk issue yang telah dinilai oleh UKO. Konsolidasi dihitung by system setelah siklus RCSA ditutup.

***Key Risk Indicator (KRI)/* Indikator Risiko Utama (IRU)**

Indikator Risiko Utama (IRU) atau *Key Risk Indicator* (KRI) adalah perangkat Manajemen Risiko Operasional yang digunakan untuk memantau trend potensi risiko dengan menggunakan indikator-indikator yang telah ditetapkan *threshold*-nya. Pemantauan tersebut ditujukan sebagai early warning untuk mengetahui trend peningkatan atau penurunan potensi risiko. Pemantauan KRI/IRU oleh Unit Kerja dilakukan secara (a) Harian: Pembuatan RTL dilakukan Apabila hasil pemantauan KRI/IRU memiliki trend risiko dengan mayoritas tingkat risiko harian adalah sedang, dan tinggi selama 1 periode pemantauan yaitu 3 bulan (mayoritas = minimal 30 hari kerja dalam 1 periode pemantauan), dan (b)Bulanan : Pembuatan RTL KRI/ IRU dilakukan secara bulanan (setiap bulan) Apabila terdapat hasil pemantauan KRI/ IRU memiliki trend risiko sedang/ tinggi.

Trend KRI/IRU wajib dibuatkan RTL apabila tingkat risiko sedang (kuning) dan tinggi (merah) dengan RTL. Tingkat risiko rendah (hijau), sedang (kuning), dan tinggi (merah) ditetapkan berdasarkan *threshold* yang ditentukan.

Manajemen Insiden (MI)/ *Loss Event Database (LED)*

Manajemen Insiden (MI) adalah pengelolaan suatu insiden yang dilakukan mulai dari insiden ditemukan sampai dengan penyelesaian. Setiap pekerja yang menemukan kejadian kerugian/insiden, wajib melaporkan kepada FMR dan/atau Pemimpin Unit Kerja, untuk segera ditindaklanjuti dan didokumentasikan kedalam modul LED/MI. Pencatatan insiden/loss event dilakukan FMR di masing-masing bidang sesuai Ketentuan Fungsi Manajemen Risiko di Unit Kerja Bank X atau Pejabat yang ditunjuk oleh Pemimpin Unit Kerja, diverifikasi oleh Pemimpin UKO dan di Review oleh Divisi MOP. Insiden*/loss event* wajib dicatatkan ke dalam modul Manajemen Insiden oleh FMR ditempat terjadinya insiden, baik oleh Unit Kerja Ybs maupun Unit Kerja Supervisi. Unit kerja terjadinya insiden/loss event adalah Unit kerja dimana terjadi kejadian kerugian.

Pendokumentasian Insiden dibagi kedalam dua kategori: fraud dan non fraud. Insiden akibat fraud wajib didokumentasikan dengan SLA H+1 sejak fraud teridentifikasi oleh SKAI, STO, KKD dan Tim Adhoc UKO, sedangkan insiden akibat non fraud memiliki SLA H+3 setelah insiden non fraud teridentifikasi. Insiden/loss event dapat dihapus, apabila terdapat kesalahan pencatatan insiden, yaitu insiden yang tidak termasuk hal-hal yang dicatatkan ke dalam modul LED/MI. Penghapusan insiden hanya dapat dilakukan dengan persetujuan dari Divisi Manajemen Risiko, sesuai kewenangan.

Forum Manajemen Risiko (Forum MR)

Forum Manajemen Risiko (Forum MR) adalah merupakan perangkat Manajemen Risiko Operasional yang digunakan untuk memfasilitasi proses pembahasan permasalahan risiko dan pengelolaannya di Unit Kerja, melalui komunikasi antara Pemimpin Unit Kerja, Fungsi Manajemen Risiko (FMR) dan pekerja. Forum MR dilaksanakan minimal 1 (satu) kali dalam 1 (satu) bulan, atau sesuai dengan kebutuhan Unit Kerja. Pelaksanaan Forum MR dapat berupa rapat evaluasi kinerja, pertemuan rutin (mingguan/bulanan) antara Pemimpin Unit Kerja dengan FMR, Pejabat lainnya, dan Pekerja, serta rapat lain yang membahas tentang permasalahan/risiko yang terjadi di Unit Kerja. Forum MR bukan merupakan wadah baru yang harus diadakan, tetapi merupakan nama lain dari pertemuan/rapat yang dilakukan Unit Kerja. Hasil pembahasan Forum MR harus mendapat persetujuan dari Pemimpin Unit Kerja/FMR/Pejabat Lain sesuai bidang pembahasan.

Penilaian Tingkat Maturitas Manajemen Risiko

Maturitas merupakan merupakan perangkat Manajemen Risiko Operasional yang digunakan untuk melakukan penilaian tingkat kemapanan penerapan Manajemen Risiko di Unit Kerja. Adapun peran fungsi manajemen risiko dalam pelaksanaan maturitas ialah (1) Menyiapkan dokumen sumber sebagai dasar penilaian tingkat maturitas penerapan Manajemen Risiko di Unit Kerja, dan (2) Merekomendasikan penilaian maturitas penerapan Manajemen Risiko kepada Pemimpin Unit Kerja berdasarkan dokumen sumber.

Pelaksanaan penilaian tingkat maturitas penerapan Manajemen Risiko dilakukan oleh Pemimpin Unit Kerja setiap 1 (satu) tahun sekali pada awal tahun, untuk menilai tingkat maturitas periode 1 (satu) tahun sebelumnya. Penilaian tingkat maturitas penerapan Manajemen Risiko didasarkan atas penerapan Manajemen Risiko yang telah dilakukan oleh Unit Kerja sesuai dokumen pendukung. Dalam melakukan penilaian maturitas penerapan MR, Bank X memiliki metodologi (1) Penilaian tingkat maturitas merupakan self assessment yang didasarkan pada penerapan implementasi MR (RCSA, KRI/IRU. MI, Forum MR) di UKO masing-masing, (2) Verifikasi oleh DMR/ Bagian MRK dilakukan dengan membandingkan hasil self assessment UKO dengan dokumen implementasi MR dan hasil pembinaan terhadap UKO Binaan (Untuk UKO Kanwil & Kanca, hasil verifikasi harus mendapat persetujuan dari Pinwil/ Wapinwil).

Kendala Penerapan Manajemen Risiko pada Evaluasi Risiko Bank X

Pada kasus skimming nasabah Bank X, risiko skimming ATM tidak terdapat pada KRI dan risk issue pada RCSA UKO, hal tersebut diketahui dari hasil wawancara dengan staf Manajemen Risiko Bank X. Kendala evaluasi pada manajemen risiko Bank X lebih pada proses identifikasi risiko, yang dipicu oleh beberapa hal yakni: (1) Pada saat penetapan KRI/IRU secara kebijakannya seharusnya Divisi Manajemen Risiko Operasional dan Pasar, berkoordinasi dengan divisi terkait termasuk di dalamnya ialah satuan pengendalian internal. Namun pada praktiknya, pada saat menetapkan IRU, Divisi MOP memiliki perangkat sendiri yang disebut dengan perangkat MRO yang ada pada *Operational Risk Assessor* (OPRA), sedangkan risiko yang dipergunakan sebagai dasar audit yang dilakukan oleh auditor internal tersimpan pada aplikasi audit internal di Satuan Audit Internal. Antara penetapan risiko pada OPRA oleh Divisi MOP dan SAI Bank X tidak terdapat koherensi yang optimal, padahal secara database risiko di unit kerja operasional Bank X sudah teridentifikasi melalui risk based yang dijadikan dasar audit internal maupun dari laporan hasil audit sesuai dengan temuan atas

permasalahan yang ditemui di unit kerja Bank X. (2) Dari hasil interview, Forum MR yang seharusnya dimanfaatkan oleh unit kerja untuk mulaporkan adanya risiko maupun isu dan masalah yang ada di UKO tidak dipergunakan pada saat kejadian skimming terjadi pada nasabah simpanan Bank X KC Kediri. Pada bulan Maret 2018, Bank X tidak melaporkan permasalahan tersebut pada forum manajemen risiko yang ada pada OPRA, sehingga pada proses identifikasi risiko, OPRA belum berjalan secara optimal untuk mengidentifikasi risiko yang dapat mengganggu pencapaian tujuan perusahaan.

***Risk Response* Bank X**

Pada kasus skimming ATM, Bank X telah melakukan tindaklanjut atas risiko yang terjadi baik yang bersifat preventif dan kuratif, yakni melakukan migrasi kartu ATM dari magnetic strip ke chip, melakukan pengembangan aplikasi transaksi fraud, dan mengganti seluruh kerugian nasabah yang terbukti menjadi korban skimming.

Migrasi Kartu ATM Magnetik Strip ke Chip

Kejahatan *skimming* merupakan pencurian data yang ada pada magneik strip kartu ATM karena *security magnetic stripe* lebih rendah dibandingkan dengan chip. Dalam rangka mengatasi kejadian serupa tidak terulang, maka Bank X memobilisasi seluruh nasabah kartu ATM-nya untuk segera migrasi ke kartu berchip. Sesuai dengan Ketentuan BI, pembatasan penggunaan teknologi *magnetic stripe* untuk kartu ATM dan/atau kartu Debet dilaksanakan paling lambat tanggal 31 Desember 2021.

Pengembangan Aplikasi Transaksi Keuangan

Berdasarkan kasus dan temuan skimming ATM Nasabah KC Kediri, Bank X mengambil tindakan preventif dalam teknologi dan kebijakan untuk mengamankan uang nasabah dengan mengembangkan aplikasi monitoring transaksi keuangan yang mencurigakan atau tidak terotorisasi oleh pemilik. Aplikasi ini dimaksudkan untuk memitigasi kejadian serupa yang muncul pada Maret 2018.

Penggantian Dana Nasabah Yang Menjadi Korban

Seluruh kerugian nasabah yang diakibatkan oleh kejadian skimming diganti sepenuhnya oleh Bank X. Bank X bertanggung jawab penuh terhadap kerugian nasabah, apabila hasil investigasi menunjukkan terbukti *skimming.*

Kendala *Risk Response* Bank X

Penggunaan kartu magnetik strip pada kartu ATM maupun Debet memiliki isu risiko keamanan yang lebih besar dibandingkan dengan chip. Garis magnetik dapat dibaca dengan menggesekkan kartu pada magnetik reader, sedangkan kartu berteknologi chip hanya dapat dibaca jika PIN terotorisasi. Pada tahapan migrasi kartu magnetik strip ke kartu berteknologi chip di Bank X, masih terdapat beberapa kendala khususnya bagi nasabah yang berada di pelosok daerah, mengingat nasabah Bank X tersebar di seluruh lapisan masyarakat perkotaan maupun pedesaan. Bahkan untuk mempercepat akselesari migrasi kartu berteknologi chip, Bank X memberikan relaksasi program dengan cara penggantian kartu berchip tanpa membawa buku tabungan dilakukan dengan syarat nasabah membawa kartu lama yang bertatus aktif melalui mekanisme card renewal.

5. KESIMPULAN

Kendala manajemen risiko TI pada kasus skimming ATM dilihat dari tiga aspek *Risk IT Governance, Risk Evaluation dan Risk Response* ialah: (1)Hierarki FMR di UKO Bank X berada pada struktur unit level entity dan tidak secara langsung bertanggung jawab pada Divisi MOP, sehingga indepensensi dan objektivitasnya terpengaruh. (2) Meskipun telah disusun budaya kerja sadar risiko, pada kenyataannya *Risk Awareness* pada Bank X belum seluruhnya melekat pada tiap level FMR UKO. (3) *Risk Issue* skimming ATM terdapat pada database Satuan Audit Internal Bank X, yang seharusnya dapat dipergunakan sebagai sumber untuk penentuan *Key Risk Indicator/* Indikator Risiko Utama. (4) Perangkat Manajemen Risiko Operasional yang dipergunakan untuk mengidentifikasi isu UKO,

belum dimanfaatkan secara optimal untuk mengelola Risiko Perusahaan. (5) Nasabah Bank X yang banyak dan tersebar di seluruh pelosok Indonesia menjadi kendala proses migrasi dari kartu ATM magnetik strip ke kartu berteknologi Chip.

6. REKOMENDASI

Rekomendasi dalam penerapan manajemen risiko TI sebagai paparan dari risiko TI dapat dilakukan Bank X melalui peningkatan efektifitas FMR dengan memasukkan FMR sebagai bagian dari Divisi MR level Kanwil, sertifikasi MR level 1 mulai dari level jajaran staff, melakukan konsolidasi antara database perangkat manajemen risiko operasional dengan audit, dan memanfaatkan seluruh jaringan termasuk agen terkecil Bank X untuk mendukung akselerasi migrasi kartu magnetic strip ke kartu berteknologi chip. Diharapkan penelitian ini dapat membantu peneliti berikutnya untuk mengembangkan manajemen risiko TI dengan menggunakan pendekatan *best practise* lainnya seperti ISO 3100:2018. Dan memberikan sumbangsih bagi regulator untuk mengatasi kendala yang muncul di lembaga keuangan khususnya perbankan dalam menghadapi risiko TI yang meningkat sejalan dengan penggunaan perangkat TI sebagai penunjang bisnis perbankan.

7. DAFTAR PUSTAKA

Djojosoedarso, Soeisno, 2003. *Prinsip-Prinsip Manajemen Risiko dan Asuransi*. Edisi Pertama, Jakarta: Salemba Empat.

Ellet, William. 2007. *How to Read, Discuss, and Write Persuasively About Cases.* Harvard Business School

Bank X. 2019. *Quarterly Publication Financial Statement Dec, 31 2019*

Fleischmann, Martin dan Svata Vlasta. 2011. *IS/IT Risk Management In Banking Industry*. Parague: ISSN 0572-3043.

Hidayat, Sofyan. 2018. https://keuangan.kontan.co.id/news/bankx-pastikan-hilangnya-duit-nasabah-di-kediri-akibat-skimming

Ichsan Pamungkas, 2013.*"Analisis Faktor- Faktor Yang Mempengaruhi Good Corporate Governance Rating"*. Skripsi Fakultas Ekonomi Universitas Diponogoro Semarang.

ISACA. 2009. *The Risk IT Framework.*USA: Rolling Meadows.

Iskandar, Iwan. 2011. Manajemen Risiko Teknologi Informasi Perusahaan Menggunakan *Framework RiskIT* (Studi Kasus: Pembobolan PT. Bank Permata, Tbk). Jurnal Sains, Teknologi dan Industri Vol. 9. No. 1, 2011.

Jarrow, Robert A. 2007. *Operational Risk.* The Journal of Banking and Finance. Q-Group Research Grant: New York.

Librianty, Andina. 2015. https://www.liputan6.com/tekno/read/2302264/mengenal-modus-pembobolan-atm-melalui-teknik-skimming

Moeller, R. Robert. 2011. *COSO Enterprise Risk Management Establishing Effective Governance, Risk, and Compliance Processes*. Second Edition. Published by John Wiley & Sons, Inc., Hoboken, New Jersey.

POJK Nomor 18 /POJK.03/2016. *Penerapan Manajemen Risiko Bagi Bank Umum*. 16 Maret 2016.

POJK Nomor 38/ POJK.03/ 2016. Penerapan Manajemen Risiko Dalam Penggunaan Teknologi Infromasi Oleh Bank Umum.

Rotheli, Tobias. 2010. *Causes of the financial crisis: Risk misperception, policy mistakes, and banks' bounded rationality*. Germany. The Journal of Socio-Economics

Scandizzo, Sergio. 2005. *Risk Mapping and Key Risk Indicators in Operational Risk* Management. Economic Notes vol. 34, no. 2-2005, pp. 231–256. Oxford. USA: Blackwell Publishing Ltd

Shauki, ER. 2018. *Reasearch Instruments in Case Study and the Role of Researcher.* Handout Case Writing and Methodology, ECAM 809303.

Supriyanto, Aji. 2010. *Pengantar Teknologi Informasi*. Jakarta: Salemba Infotek.

Westerman, George and Richard Hunter. (2007). *IT Risk : Turning Business Threats Into Competitive Advantage*. Harvard Business School Press.