Manajemen Risiko Teknologi Informasi Terkait Manipulasi dan Peretasan Sistem pada Bank XYZ Tahun 2020 Menggunakan ISO 31000:2018

I Putu Agus Eka Pratama[#1], Made Toby Sathya Pratika[#2]

[#]*Program Studi Teknologi Informasi, Universitas Udayana*
Jl. Raya Kampus UNUD, Bukit Jimbaran, Kuta Selatan, Badung-Bali, Indonesia
[1]eka.pratama@unud.ac.id
[2]tobysathya@unud.ac.id

Abstract*— PT XYZ is the largest private bank in Indonesia which was founded in 1955. The use of Information Technology (IT) at XYZ Bank has changed the mindset of the public in transactions. This can be seen from the ease with which online shopping and non-cash payments are made using the application. Along with the use of IT at XYZ Bank, it is necessary to pay attention to the risks that result from using IT. Risk is the possibility of an event occurring in making a decision. To meet the strategic objectives of using IT, a company must implement risk management called Enterprise Risk Management (ERM). Currently XYZ Bank has used the Operational Risk Management Framework (ORMF). This research will try to implement risk management using the ISO 31000: 2018 framework related to IT problems faced by XYZ Bank in 2020. The method used is the assessment process in ISO 31000: 2018 which includes risk identification, risk analysis, and risk evaluation. This research has obtained results in the form of a large enough chance of the problem to recur and it is necessary to reduce the risk impact. From this research, it is hoped that a conclusion can be drawn regarding the need for a review regarding the problems faced so that the business objectives of XYZ Bank can be achieved.

***Keywords*— Assessment, IT Risk Management, ERM, ISO 31000:2018, ORMF**

Abstrak*— PT XYZ adalah bank swasta terbesar di Indonesia yang berdiri pada tahun 1955. Penggunaan Teknologi Informasi (TI) pada Bank XYZ telah mengubah pola pikir masyarakat dalam bertransaksi. Hal ini terlihat dengan mudahnya belanja secara daring dan juga pembayaran secara nontunai menggunakan aplikasi. Seiring dengan penggunaan TI di Bank XYZ, perlu diperhatikan risiko yang diakibatkan dari penggunaan TI. Risiko adalah kemungkinan terjadinya suatu kejadian dalam pengambilan suatu keputusan. Untuk memenuhi tujuan strategis penggunaan TI, suatu perusahaan harus menerapkan manajemen risiko yang bernama *Enterprise Risk Management* (ERM). Saat ini Bank XYZ telah menggunakan Operational Risk Management Framework (ORMF). Penelitian ini akan mencoba untuk menerapkan manajemen risiko menggunakan *framework* ISO 31000:2018 terkait dengan permasalahan TI yang dihadapi oleh Bank XYZ di tahun 2020. Metode yang digunakan adalah dengan proses penilaian yang ada pada ISO 31000:2018 yang meliputi identifikasi risiko, analisis risiko, dan evaluasi risiko. Penelitian ini memperoleh hasil berupa peluang terjadinya kembali permasalahan tersebut cukup besar, sehingga perlu dilakukan pengurangan dampak risiko. Dari penelitian ini, diharapkan dapat diperoleh kesimpulan mengenai perlunya peninjauan ulang terkait masalah-masalah yang dihadapi, sehingga tujuan bisnis dari Bank XYZ dapat tercapai.

***Kata Kunci*— Penilaian, Manajemen Risiko TI, ERM, ISO 31000:2018, ORMF**

I. PENDAHULUAN

Kemajuan Teknologi Informasi (TI) saat ini sangatlah cepat dan telah menjadi suatu kebutuhan bagi umat manusia. Tidak menampik juga bahwa TI juga digunakan di hampir seluruh bidang usaha seperti pada bidang perbankan, Pendidikan, dan pemerintahan. Pada bidang perbankan retail, TI dapat memberikan berbagai kemudahan untuk para nasabahnya dalam melakukan transaksi. Transaksi tersebut dapat menggunakan *m-Banking* (*mobile banking*), *i-Banking* (*internet banking*), ATM (*Automatic Teller Machine*), dan layanan transaksi lainnya. Saat ini layanan transaksi TI tersebut telah mengubah pola pikir masyarakat dalam bertransaksi. Perilaku yang sangat mudah terlihat yaitu masyarakat dapat dengan mudah berbelanja secara daring (*online*) dan transaksi pembayarannya menggunakan rekening yang telah dimilikinya. Perilaku lainnya yang mulai marak terjadi yaitu penggunaan aplikasi dompet virtual dalam melakukan suatu pembayaran suatu barang/jasa sehingga pembayaran dapat dilakukan secara nontunai (*cashless*) di suatu usaha yang menerapkan metode tersebut.

Kemudahan yang diberikan dalam penggunaan TI tersebut tidak terhindar dari risiko-risiko yang dapat membuat tidak terwujudnya tujuan dari penggunaan TI dalam suatu perusahaan. Risiko seperti peretasan sistem adalah salah satu risiko yang harus dihadapi bersama, baik dari pihak bank maupun dari pihak nasabah. Dampak yang diakibatkan dari risiko tersebut adalah hilangnya rasa percaya beberapa nasabah bank dikarenakan bocornya data-data nasabah yang bersifat private sehingga menimbulkan kerugian bagi nasabah itu sendiri.

Penanggulangan risiko dapat dilakukan dengan cara melakukan manajemen risiko yang baik sehingga dapat dijadikan pertimbangan bagi perusahaan dalam mengambil suatu keputusan guna menanggulangi risiko tersebut.

Manajemen risiko suatu perusahaan ini disebut ERM (*Enterprise Risk Management*).

Bank XYZ sebagai salah satu bank terbesar di Indonesia, menyediakan sejumlah fasilitas berbasis TI untuk meningkatkan keamanan dan kenyamanan para nasabahnya. Dalam hal ini, Bank XYZ memperoleh nilai dari pemanfaatan TI di dalam organisasi mereka (*IT Value*) yang berujung kepada peningkatan kepercayaan nasabah dan masyarakat. Namun di sisi lain, Bank XYZ menghadapi sejumlah kasus yang terkait dengan layanan berbasis TI tersebut, di antaranya penipuan dan peretasan yang mencakup: pembobolan rekening, OTP, dompet virtual, serta layanan dengan pihak ketiga (OVO). Kasus-kasus ini menjadi sebuah masalah dan perlu adanya manajemen resiko untuk mencegah terulangnya hal atau kejadian serupa.

Untuk itu, di dalam penelitian ini dilakukan analisis dari sisi IT Risk Management menggunakan ISO 31000:2018 terkait dengan kasus-kasus yang dihadapi oleh Bank XYZ sehingga diharapkan dapat diperoleh kesimpulan mengenai peninjauan ulang terkait masalah yang dihadapi, peningkatan keamanan dan layanan, serta pencapaian tujuan bisnis Bank XYZ.

II. METODOLOGI

A. Risiko dan Masalah

Risiko (*risk*) adalah pengaruh ketidakpastian pada suatu tujuan. Pengaruh adalah penyimpangan dari hasil yang diharapkan, hasilnya bisa positif, negatif atau keduanya sehingga dapat mengatasi, menciptakan, atau menghasilkan peluang dan ancaman [1]. Masalah (*problem*) memiliki perbedaan dengan risiko. Risiko merupakan akibat yang belum tentu terjadi sehingga dapat dihindari dengan manajemen risiko, sedangkan masalah merupakan akibat yang sudah terjadi sehingga harus diberikan solusi dan diperbaiki [2].

B. ERM (Enterprise Risk Management)

Manajemen risiko (*risk management*) adalah kegiatan terkoordinasi untuk mengarahkan dan mengendalikan organisasi terkait dengan risiko [1]. Tujuan dilakukannya manajemen risiko adalah untuk memahami kemungkinan kegagalan dari tujuan yang ingin dicapai suatu organisasi. Teknologi Informasi (TI) berperan untuk mendukung mencapai tujuan tersebut. *IT Value* adalah hasil yang diperoleh suatu organisasi setelah diterapkannya TI di organisasi tersebut. *IT Risk* adalah kemungkinan munculnya permasalahan setelah diterapkannya TI pada organisasi yang menghambat dalam mencapai tujuan sehingga perlu dilakukan manajemen risiko TI.

Manajemen risiko TI (IT *risk management*) adalah penerapan dari manajemen risiko terkait dengan pemanfaatan TI pada suatu organisasi dan dilakukan oleh orang yang ahli di bidang tersebut. Hambatan yang mungkin terjadi terhadap sistem TI dibagi menjadi 2, yaitu hambatan umum dan hambatan kriminal [3]. Hambatan umum meliputi kerusakan perangkat keras, *malware* komputer, *virus* computer, dan kesalahan pengguna (*human error*). Hambatan kriminal meliputi peretas (*hackers*), manipulasi data (*fraud*), penyerangan sistem (*denial-of-service*), dan pencurian data dari internal (*staff dishonesty*).

C. Penilaian Risiko TI

Penilaian risiko TI (*IT Risk Asessment*) harus dilakukan oleh orang yang memiliki pengetahuan yang baik tentang manajemen risiko. Penilai harus mengikuti langkah-langkah penilaian sesuai dengan *framework* manajemen risiko yang dipahami dan juga harus dilakukan secara sistematis, literatif, kolaboratif, dan memanfaatkan berbagai sumber informasi.

Penilaian dalam penelitian ini dilakukan dengan menggunakan *framework* manajemen risiko ISO 31000:2018.

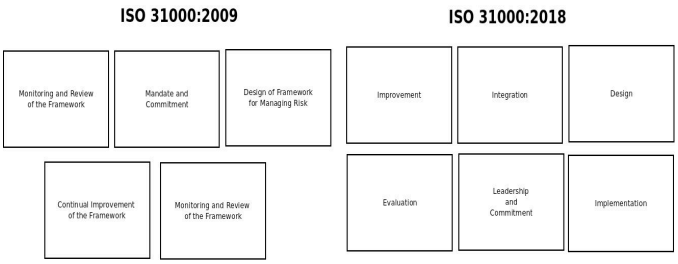
D. ISO 31000:2018

ISO 31000 adalah panduan penerapan risiko yang terdiri atas tiga elemen, antara lain: prinsip (*principle*), kerangka kerja (*framework*), dan proses (*process*) [4]. Panduan ini disusun oleh organisasi yang bernama International Organization for Standardization (ISO). Pada tahun 2018 ISO mengeluarkan *framework* terbarunya untuk manajemen risiko, yaitu ISO 31000:2018 dengan judul "*Risk Management-Guideline*". *Framework* tersebut merupakan penyederhanaan dari ISO 31000:2009 sehingga dapat lebih ringkas dan mudah dipahami poin-poinnya.

Perbedaan antara versi 2009 dengan 2018 terletak pada pembahasan dari elemen prinsip, kerangka kerja, dan proses. Versi 2009 menggambarkan ketiga elemen tersebut menjadi rangkaian unsur yang berurutan, sedangkan pada versi 2018 ketiga elemen tersebut digambarkan sebagai elemen yang terbuka dan saling berkaitan antara satu dengan lainnya. Perbedaan tersebut dapat dilihat pada Gambar 1.

Gambar 1 merupakan perbedaan ISO 31000 tahun 2009 dengan 2018. Prinsip manajemen risiko berubah dari 11 prinsip pada versi 2009 menjadi 1 tujuan (*purpose*) dan 8 prinsip pada versi 2018. Delapan prinsip lain disederhanakan pernyataannya menjadi terintegrasi (*integrated*), terstruktur dan komprehensif (*structured and comperhensive*), disesuaikan (*customized*), inklusif (*inclusive*), dinamis (*dynamic*), tersedia informasi terbaik (*best available information*), faktor manusia dan budaya (*human and cultural factors*), serta peningkatan berkelanjutan (*continual improvement*) [4]. Penjelasan dari ketiga elemen dalam ISO 31000:2018 diperlihatkan pada Gambar 2.

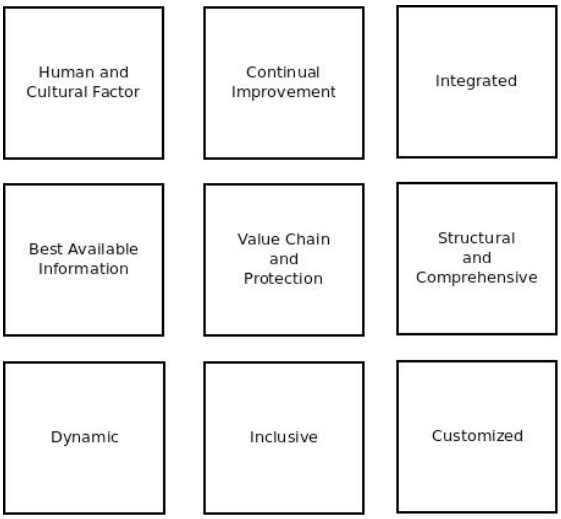
Prinsip manajemen risiko adalah dasar praktik atau filosofi manajemen risiko [4]. Tujuan manajemen risiko adalah penciptaan dan perlindungan nilai (*value creation and protection*). Tujuan ini meningkatkan kinerja, mendorong ino-



Gambar 1 Perbedaan ISO 31000 tahun 2009 dengan 2018 [4]

vasi, dan mendukung pencapaian tujuan. Prinsip-prinsip yang ditampilkan pada Gambar 2 memberikan panduan tentang karakteristik manajemen risiko yang efektif dan efisien, mengkomunikasikan nilainya, dan menjelaskan maksud dan tujuannya. Prinsip-prinsip tersebut adalah dasar untuk mengelola risiko dan harus dipertimbangkan ketika menetapkan kerangka kerja dan proses manajemen risiko organisasi. Prinsip-prinsip ini harus memungkinkan organisasi untuk mengelola efek ketidakpastian pada tujuannya. Elemen-elemen prinsip yang ditunjukan pada Gambar 2 akan dijelaskan sebagai berikut [1]:

- Terintegrasi (*integrated*). Manajemen risiko adalah bagian integral dari semua kegiatan organisasi.
- Terstruktur dan komperhensif (*structured and comperhensive*). Pendekatan terstruktur dan komprehensif untuk manajemen risiko berkontribusi pada hasil yang konsisten dan dapat dibandingkan.
- Disesuaikan (*customized*). Kerangka kerja dan proses manajemen risiko disesuaikan dan proporsional dengan konteks eksternal dan internal organisasi terkait dengan tujuannya.
- Inklusif (i*nclusive*). Keterlibatan pemangku kepentingan yang tepat dan tepat waktu memungkinkan pengetahuan, pandangan, dan persepsi mereka dipertimbangkan. Ini menghasilkan peningkatan kesadaran dan manajemen risiko informasi.
- Dinamis (*dynamic*). Risiko dapat muncul, berubah, atau menghilang ketika konteks eksternal dan internal organisasi berubah. Manajemen risiko mengantisipasi, mendeteksi, mengakui, dan merespons perubahan dan kejadian tersebut dengan cara yang tepat dan tepat waktu.
- Tesedia informasi terbaik (*best available information*). Masukan untuk manajemen risiko didasarkan pada informasi historis dan saat ini, serta harapan masa depan. Manajemen risiko secara eksplisit memperhitungkan segala keterbatasan dan ketidakpastian yang terkait dengan informasi dan harapan tersebut. Informasi harus tepat waktu, jelas, dan tersedia untuk pemangku kepentingan terkait.
- Faktor manusia dan budaya (*human and cultural factors*). Perilaku dan budaya manusia secara signifikan mempengaruhi semua aspek manajemen risiko di setiap tingkatan dan tahap.
- Peningkatan berkelanjutan (*continual improvement*). Manajemen risiko terus ditingkatkan melalui pembelajaran dan pengalaman.

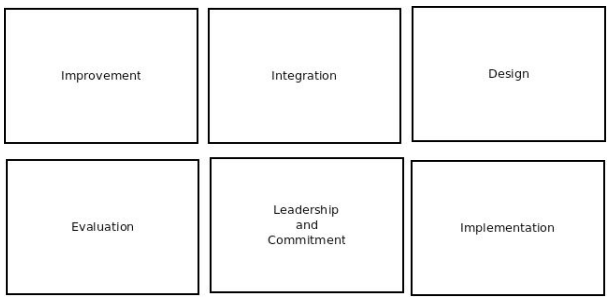


Gambar 2 Prinsip manajemen risiko ISO 31000:2018 [1]

Kerangka kerja adalah pengaturan sistem manajemen risiko secara terstruktur dan sistematis di seluruh organisasi [4]. Tujuan kerangka kerja manajemen risiko adalah untuk membantu organisasi dalam mengintegrasikan manajemen risiko ke dalam kegiatan dan fungsi yang signifikan. Elemen-elemen kerangka kerja yang ditunjukan pada Gambar 3 akan dijelaskan sebagai berikut [1]:

- Kepemimpinan dan komitmen (*leadership and commitment*). Manajemen puncak dan badan pengawas, jika ada, harus memastikan bahwa manajemen risiko terintegrasi ke dalam semua kegiatan organisasi dan harus menunjukkan kepemimpinan dan komitmen.
- Integrasi (*integration*). Mengintegrasikan manajemen risiko bergantung pada pemahaman tentang struktur dan konteks organisasi.
- Desain (*design*). Ketika merancang kerangka kerja untuk mengelola risiko, organisasi harus memeriksa dan memahami konteks eksternal dan internalnya.
- Implementasi (*implementation*). Keberhasilan implementasi kerangka kerja membutuhkan keterlibatan dan kesadaran para pemangku kepentingan.
- Evaluasi (*evaluation*). Organisasi harus mengukur kinerja kerangka kerja manajemen risiko secara berkala terhadap tujuannya, rencana implementasi, indikator, dan perilaku yang diharapkan dan menentukan apakah tetap cocok untuk mendukung pencapaian tujuan organisasi.
- Peningkatan (*improvement*). Organisasi harus terus memantau dan mengadaptasi kerangka kerja manajemen risiko untuk mengatasi perubahan eksternal dan internal. Dengan demikian, organisasi dapat meningkatkan nilainya.

Proses adalah aktifitas pengelolaan risiko yang sistematis dan saling terkait [4]. Proses manajemen risiko hendaknya merupakan bagian yang tidak terpisahkan dari manajemen u-



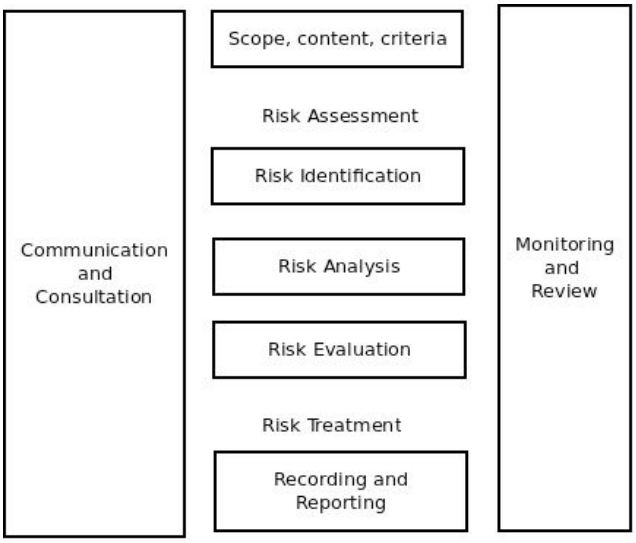
Gambar 3 Kerangka kerja manajemen risiko ISO 31000:2018 [1]

mum. Proses manajemen risiko meliputi 6 kegiatan, yaitu komunikasi dan konsultasi (*communication and consultation*), penentuan konteks (*scoope, context, criteria*), asesmen risiko (*risk assessment*), perlakuan risiko (*risk treatment*), *monitoring* dan *review* (*monitoring and review*), serta pencatatan dan pelaporan (*recording and reporting*). Elemen-elemen proses yang ditunjukan pada Gambar 4 akan dijelaskan sebagai berikut [1]:

- Komunikasi dan konsultasi (*communication and consultation*). Tujuan komunikasi dan konsultasi adalah untuk membantu pemangku kepentingan yang relevan dalam memahami risiko, dasar pengambilan keputusan, dan alasan suatu tindakan tertentu diperlukan.
- Penentuan konteks (*scoope, context, criteria*). Tujuan membangun ruang lingkup, konteks, dan kriteria adalah untuk menyesuaikan proses manajemen risiko, memungkinkan penilaian risiko yang efektif, dan perlakuan risiko yang tepat.
- Penilaian risiko (*risk assessment*). Penilaian risiko adalah keseluruhan proses identifikasi risiko, analisis risiko, dan evaluasi risiko.
- Perlakuan risiko (*risk treatment*). Tujuan dari perawatan risiko adalah untuk memilih dan menerapkan opsi untuk mengatasi risiko.
- *Monitoring* dan *review* (*monitoring and review*). Tujuan pemantauan dan peninjauan adalah untuk memastikan dan meningkatkan kualitas dan efektivitas desain proses, implementasi, dan hasil.
- Pencatatan dan pelaporan (*recording and reporting*). Proses manajemen risiko dan hasilnya harus didokumentasikan dan dilaporkan melalui mekanisme yang tepat.

E. *Profil Bank XYZ*

PT XYZ adalah salah satu bank swasta terbesar di Indonesia yang saat ini (2019) memiliki 1.256 cabang dan 17.928 mesin penarikan tunai (ATM). Tahun 1990 merupakan awal penggunaan teknologi ATM sebagai alternatif layanan penarikan uang yang memang pertama kali dikembangkan oleh Bank XYZ [2].



Gambar 4 Proses manajemen risiko ISO 31000:2018 [1]

Bank XYZ telah menyediakan banyak produk dan layanan yang ditujukan untuk memenuhi kebutuhan nasabahnya. Produk dan layanan yang ditawarkan Bank XYZ, yaitu Simpanan, Kartu Kredit, Fasilitas Kredit, Layanan Transaksi Perbankan, Layanan Cash Management, Bancassurance, Bank Garasi, Fasilitas Ekspor Impor, Fasilitas Valuta Asing dan Perbankan Elektronik [2].

F. *Visi dan Misi Bank XYZ*

Visi Bank XYZ adalah bank pilihan utama andalan masyarakat yang berperan sebagai pilar penting perekonomian Indonesia. Misi Bank XYZ terdapat 3 poin, yaitu [5]:

- Membangun institusi yang unggul di bidang penyelesaian pembayaran dan solusi keuangan bagi nasabah bisnis dan perorangan.
- Memahami beragam kebutuhan nasabah dan memberikan layanan finansial yang tepat demi tercapainya kepuasan optimal bagi nasabah.
- Meningkatkan nilai *francais* dan nilai *stakeholders* XYZ.

Kesimpulan dari visi misi di atas yaitu Bank XYZ adalah bank yang sangat mementingkan kenyamanan nasabahnya. Kenyamanan itu coba dibangun oleh Bank XYZ dengan cara membangun pelayanan dan fasilitas yang baik, sehingga nantinya dapat meningkatkan kepercayaan masyarakat kepada Bank XYZ.

G. *Tujuan Strategis TI Bank XYZ*

Tujuan strategis TI (IT *strategic objectif*) dari Bank XYZ terdapat 4 poin penting untuk meningkatkan kenyamanan para nasabahnya. Poin-poin tersebut dijelaskan sebagai berikut [5]:

1. Meningkatkan inovasi dan produktivitas melalui teknologi.
2. Memperkuat kapabilitas infrastruktur teknologi informasi.
3. Memperkuat keamanan sistem transaksi perbankan.
4. Rencana pengembangan di masa mendatang.

H. *Operational Risk Management Framework (ORMF) Bank XYZ*

Bank XYZ menggunakan ERM yang bernama *Operational Risk Management Framework* (ORMF) untuk mengelola, memitigasi dan meminimalkan risiko operasional yang disebabkan oleh kesalahan manusia, ketidakcukupan proses internal, kegagalan sistem, dan atau kejadian eksternal. Upaya yang telah diimplementasikan yaitu dengan membangun *Operational Risk Management Information System* (ORMIS) dalam bentuk aplikasi berbasis *web* yang meliputi *Risk Control Self Asessment* (RCSA), *Loss Event Database* (LED), dan *Key Risk Indicator* (KRI). Bank XYZ saat ini sedang membangun aplikasi *Integrated Risk Management Information System* (IRMIS) yang nantinya dapat menampilkan Laporan Profil Risiko (LPR), Laporan

Profil Risiko Terintegrasi (LPRT), dan Laporan Kecukupan Permodalan Terintegrasi (LKPT) [5].

I. Tahapan Penelitian

Metode penelitian menggunakan proses penilaian risiko dari ISO 31000:2018. Proses penilaian tersebut dapat dilihat pada Gambar 5.

Gambar 5 merupakan proses penelitian risiko ISO 31000:2018 yang digunakan untuk menilai risiko sehingga dapat dilakukan secara sitematis. Proses tersebut meliputi identifikasi risiko, analisis risiko dan evaluasi risiko.

Proses identifikasi risiko (*risk identification*) adalah untuk menemukan, mengenali, dan menggambarkan risiko yang mungkin membantu atau mencegah organisasi mencapai tujuannya [1]. Informasi yang relevan, tepat, dan terkini penting dalam mengidentifikasi risiko. Organisasi dapat menggunakan berbagai teknik untuk mengidentifikasi ketidakpastian yang dapat memengaruhi satu atau lebih tujuan. Organisasi harus mengidentifikasi risiko, terlepas dari apakah sumbernya terkendali atau tidak. Pertimbangan harus diberikan bahwa mungkin ada lebih dari satu jenis hasil yang dapat menghasilkan berbagai konsekuensi nyata atau tidak berwujud.

Proses analisis risiko (*risk analysis*) adalah untuk memahami sifat risiko dan karakteristiknya termasuk, jika sesuai, tingkat risiko [1]. Analisis risiko melibatkan pertimbangan terperinci tentang ketidakpastian, sumber risiko, konsekuensi, kemungkinan, peristiwa, skenario, kontrol, dan efektivitasnya. Suatu peristiwa dapat memiliki banyak penyebab dan konsekuensi dan dapat mempengaruhi banyak tujuan. Analisis risiko dapat dilakukan dengan berbagai tingkat detail dan kompleksitas, tergantung pada tujuan analisis, ketersediaan dan keandalan informasi, dan sumber daya yang tersedia. Teknik analisis dapat kualitatif, kuantitatif atau kombinasi dari ini, tergantung pada keadaan dan tujuan penggunaan. Analisis risiko memberikan masukan untuk evaluasi risiko, untuk keputusan apakah risiko perlu diperlakukan dan bagaimana, dan pada strategi dan metode perawatan risiko yang paling tepat.

Proses evaluasi risiko (*risk evaluation*) adalah untuk mendukung keputusan. Evaluasi risiko melibatkan perbandi ngan hasil analisis risiko dengan kriteria risiko yang ditetapkan untuk menentukan di mana tindakan tambahan diperlukan [1]. Keputusan harus mempertimbangkan konteks yang lebih luas dan konsekuensi aktual yang dirasakan oleh pemangku kepentingan eksternal dan internal. Hasil evaluasi risiko harus dicatat, dikomunikasikan, dan kemudian divalidasi pada tingkat organisasi yang sesuai.

Gambar 5 Proses penilaian risiko ISO 31000:2018

J. Tujuan Penelitian

Penelitian ini bertujuan untuk membahas konsep dan implementasi dari *framework* ISO 31000:2018 pada perusahaan perbankan (Bank XYZ) dalam menanggulangi suatu permasalahan, khususnya di bidang TI, agar tidak terjadi kembali di kemudian hari karena akan mempengaruhi tujuan (*objective*) dari perusahaan tersebut. Permasalahan yang diangkat dalam penelitian ini yaitu permasalahan yang menimpa Bank XYZ yang terjadi pada bulan Maret tahun 2020.

I. HASIL DAN PEMBAHASAN

A. Proses Bisnis Bank XYZ "Aplikasi Mobile Banking XYZ (m-XYZ)"

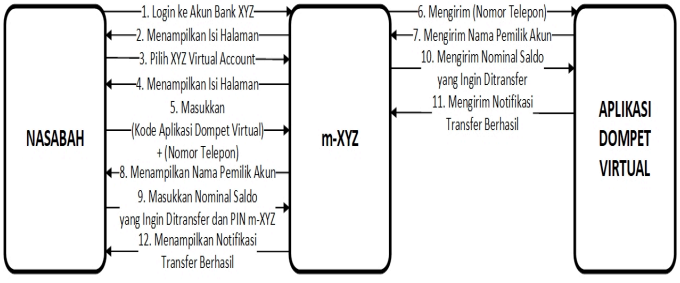
Pembahasan proses bisnis Bank XYZ pada bagian "Aplikasi *Mobile Banking* Bank XYZ (*m*-XYZ)" dilakukan karena adanya keterkaitan dengan permasalahan yang akan dibahas. Proses bisnis Bank XYZ pada bagian tersebut dapat dilihat pada Gambar 6.

Gambar 6 disusun berdasarkan penjelasan dari salah satu produk aplikasi dompet *virtual*, di mana terdapat relasi antara nasabah, aplikasi *mobile banking* Bank XYZ (*m*-XYZ) dan aplikasi dompet *virtual* [6]. Terdapat 12 proses yang berjalan ketika nasabah ingin melakukan transfer (*top-up*) ke aplikasi dompet *virtual*. Analisis proses bisnis Bank XYZ pada bagian "Aplikasi *Mobile Banking* Bank XYZ (*m*-XYZ)" ke depannya akan sangat membantu dalam pembahasan mengenai permasalahan yang terjadi.

B. Proses Identifikasi Permasalahan TI pada Bank XYZ Tahun 2020

Permasalahan yang terjadi pada Bank XYZ pada tahun 2020 yang berkaitan dengan TI adalah kasus pembobolan sistem sehingga merugikan bank senilai 22 miliar rupiah. Pelaku berjumlah 12 orang yang ditangkap pada bulan Maret di Provinsi Sumatera Selatan.

Aksi kejahatan tersebut dilakukan dari tahun 2015 dengan menggunakan beberapa modus. Modus pertama yaitu dengan memanfaatkan sistem Bank XYZ yang sedang mengalami



Gambar 6 Proses bisnis Bank XYZ pada bagian "Aplikasi *Mobile Banking* (*m*-XYZ)"

perbaikan (*maintenance*). Para pelaku mengisi aplikasi dompet *virtual*-nya secara terus menerus ketika *maintenance* menggunakan aplikasi *mobile banking* Bank XYZ (*m*-XYZ), misalkan pelaku melakukan *top-up* saldo OVO senilai 500 ribu rupiah, saldo OVO pelaku bertambah, namun jumlah uang di rekening pelaku tidak berkurang sama sekali. Modus kedua yang digunakan oleh pelaku adalah dengan melakukan transaksi di toko belanja *online* menggunakan kartu kredit korbannya, yaitu nasabah Bank XYZ. Sistem secara otomatis mengirimkan kode *Once Time Password* (OTP) ke nomor telepon korban dan para pelaku langsung menelepon korban dengan berpura-pura menjadi pegawai bank agar mendapatkan kode OTP tersebut. Kode OTP tersebut selanjutnya dimasukkan oleh pelaku yang digunakan sebagai konfirmasi belanjaan dan berakibat pada berkurangnya uang di rekening korban [7], [8], [9].

C. *Proses Analisis Permasalahan TI pada Bank XYZ Tahun 2020*

Permasalahan di atas dapat terjadi karena kesalahan sistem, *staff dishonesty*, dan *fraud*. Modus pertama bisa terjadi karena pelaku pencurian dapat menemukan kecacatan pada sistem, entah itu dari sistem m-XYZ ataupun integrasi sistem Bank XYZ dan aplikasi dompet *virtual* tersebut. Bisa saja terdapat pegawai *internal* Bank XYZ yang memberitahu bahwa sistem bank sedang *maintenance*, sehingga pelaku dengan mudahnya melakukan pengisian pada aplikasi dompet *virtualnya* secara terus menerus. Modus kedua bisa terjadi karena penyalahgunaan data nasabah bank oleh pelaku. Data tersebut bisa saja didapatkan dari pegawai *internal* Bank XYZ atau dijual kepada pelaku. Penyebab lainnya mungkin dikarenakan kurangnya edukasi ataupun penyuluhan kepada nasabah Bank XYZ tentang tata cara menghindari tindakan pencurian uang di rekeningnya.

Permasalahan di atas sangat mempengaruhi tujuan (*objective*) dari Bank XYZ. Bisa dilihat dari kesimpulan visi dan misinya, Bank XYZ adalah bank yang sangat mementingkan nasabahnya. Kejadian ini membuat hilangnya rasa percaya beberapa nasabah bank dikarenakan bocornya data-data nasabah yang bersifat *private* sehingga menimbulkan kerugian bagi nasabah itu sendiri dan tidak menutup kemungkinan para nasabah memutus hubungan dan berpindah ke lain bank. Calon nasabah juga akan berpikir kembali untuk menjalin hubungan dengan Bank XYZ. Tentu saja dari pihak Bank XYZ akan sangat mengalami kerugian diluar dari kerugian kasusnya. IT *Strategic Objective* Bank XYZ akan mengalami gangguan dalam peningkatan layanannya.

D. *Proses Evaluasi Permasalahan TI pada Bank XYZ Tahun 2020*

Evaluasi yang dapat diberikan dalam penelitian ini terkait dengan permasalahan yang terjadi pada Bank XYZ adalah dengan melakukan manajemen risiko dengan menggunakan *framework* ISO 31000:2018. Penerapan ISO 31000:2018 pada Bank XYZ akan disajikan pada pembahasan berikutnya.

E. *Penerapan ISO 31000:2018 pada Bank XYZ*

Dalam penelitian ini digunakan ISO 31000:2018 sebagai panduan manajemen risiko atas permasalahan yang terjadi pada Bank XYZ. Perlakuan terhadap risiko terdiri dari 4 jenis penanganan antara lain menghindari risiko (*risk avoidance*), mengurangi risiko (*risk reduction*), membagi risiko (*risk sharing*), ataupun menerima risiko (*risk acceptance*) [9]. Jenis perlakuan risiko yang digunakan dalam penelitian ini adalah *risk reduction* dengan tata cara sebagai berikut:

- Menentukan kriteria kemungkinan (*likelihood*) risiko menggunakan tabel, sehingga risiko tersebut dapat dipertimbangkan.
- Menentukan strategi dalam pengurangan dampak risiko.

Penerapan dari *risk reduction* akan dijelaskan sebagai berikut.

Tabel I merupakan tabel kriteria kemungkinan (*likelihood*) dari permasalahan yang terjadi. Terlihat pada tabel tersebut bahwa terjadinya kembali permasalahan tersebut berada pada tingkatan ke-4 dengan kriteria kuantitatif sebesar 61 – 85 %. Penilaian ini didasari atas hasil analisis permasalahan yang sebelumnya dilakukan. Penyebabnya yaitu kesalahan sistem, *staff dishonesty*, dan *fraud*.

Langkah berikutnya yaitu menentukan strategi dalam pengurangan dampak risiko tersebut. Bank XYZ dapat melakukan beberapa tindakan untuk menanggulangi permasalahan tersebut agar ke depannya tidak terjadi kembali. Usulan yang diberikan adalah sebagai berikut:

1. Penerapan sanksi yang berat bagi siapapun pihak internal Bank XYZ yang kedapatan menyalahgunakan jabatannya untuk memperoleh keuntungan pribadi, sehingga memberikan dampak yang sangat buruk bagi Bank XYZ.
2. Pemberian edukasi ataupun penyuluhan kepada calon nasabah maupun sosialisasi berkala kepada nasabah Bank XYZ tentang tata cara menghindari tindakan pencurian uang di rekeningnya.
3. Perbaikan sistem yang mengalami kecacatan dan melakukan pengujian mendalam pada sistem tersebut.

III. SIMPULAN

Kesimpulan yang dapat ditarik setelah melakukan analisis terhadap manajemen risiko TI ada Bank XYZ menggunakan

TABEL I
KRITERIA KEMUNGKINAN (LIKELIHOOD)

No	Tingkat			Kriteria Kuantitatif	Kriteria Kualitatif
	Kode	Ket.	Nilai		
1	SK	Sangat Kecil	1	< 15%	Kemungkinan tidak terjadi.
2	K	Kecil	2	16% - 40%	Kemungkinan kecil terjadi.
3	S	Sedang	3	41% - 60%	Kemungkinan terjadi kecil / besar.
4	B	Besar	4	61% - 85%	Kemungkinan besar terjadi.
5	SB	Sangat Besar	5	86% - 95%	Kemungkinan sangat sering terjadi.

framework ISO 31000:2018 adalah Bank XYZ memiliki *framework* manajemen risiko ORMF dan telah dijalankan dengan baik, namun perlu dilakukan perbaikan setelah terjadinya masalah tersebut. Manajemen risiko TI sangat perlu dilakukan untuk menjaga objektivitas dari suatu perusahaan. ISO 31000:2018 dapat diimplementasikan dalam manajemen risiko TI pada sebuah perusahaan perbankan retail. *Risk reduction* dapat dijadikan pertimbangan penanganan untuk mencegah kembali terjadinya manipulasi dan peretasan sistem pada Bank XYZ.

DAFTAR REFERENSI

[1] I. P. A. E. Pratama dan Suhardi, "Manajemen risiko teknologi informasi di Bank Danamon terkait tiga masalah yang dihadapi di tahun 2011 (solusi permasalahan dengan usulan ISO 31000)," *Jurnal S@cies Stikom Indonesia*, vol.1, no.1, 2011.

[2] BS ISO 31000:2018, *Risk management – Guidelines*, 2018. [Daring]. Tersedia: https://www.iso.org/standard/65694.html [10 November 2020].

[3] N. Feronika, *IT Risk Management*, 2019. [Daring]. Tersedia: https://sis.binus.ac.id/2019/04/08/it-risk-management/ [10 November 2020].

[4] K. B. Mahardika, A. F. Wijaya, dan A. D. Cahyono, "Manajemen risiko teknologi informasi menggunakan ISO 31000:2018 (studi kasus: CV XY)", *Jurnal SEBATIK,* vol.23, no.1, 2019.

[5] PT Bank Central Asia Tbk., *Laporan Tahunan 2019 PT Bank Central Asia Tbk 2019*, 2019. [Daring]. Tersedia: https://www.bca.co.id/tentang-bca/hubungan-investor/laporan-tahunan [10 November 2020].

[6] Anonim, *How to Top-Up*, 2017. [Daring]. Tersedia: https://www.ovo.id/howtotopup [10 November 2020].

[7] A. Rahim, *Rugikan Bank 22 Miliar, Begini Modus Pelaku Pembobolan*, 2020. [Daring]. Tersedia: https://www.kompas.tv/article/70105/bca-rugi-22-miliar-begini-modus-pelaku-pembobolan [10 November 2020].

[8] Adhey, *Komplotan Pembobol Spesialis Rekening Diringkus, Bank BCA Alami Kerugian Capai 22 Miliar*, 2020. [Daring]. Tersedia: https://pojoksatu.id/news/berita-nasional/2020/03/06/komplotan-pembobol-spesialis-rekening-diringkus-bank-bca-alami-kerugian-capai-22-miliar/ [10 November 2020].

[9] A. R. Tampubolondan Suhardi, "Manajemen risiko teknologi informasi menggunakan *framework* ISO 31000:2009 (studi kasus: pembobolan ATM BCA tahun 2010", *Jurnal Telematika,* vol.7, no.2, 2011.

[10] Anonim, *Sindikat Mafia Perbankan Bobol Rekening dan Kartu Kredit, Kerugian Capai Rp22 M*, 2020. [Daring]. Tersedia: https://batampos.co.id/2020/03/07/sindikat-mafia-perbankan-bobol-rekening-dan-kartu-kredit-kerugian-capai-rp-22-m/ [10 November 2020].

I Putu Agus Eka Pratama, kelahiran kota Gianyar, Bali. Pendidikan S1 Informatika Institut Teknologi Telkom Bandung dan S2 Informatika Institut Teknologi Bandung. Staf pengajar di Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Udayana. Minat riset dan keilmuan pada sistem operasi, *smart city*, *IT Risk Management*, *network security*.

I Made Toby Sathya Pratika, kelahiran kota Singaraja, Bali. Sedang melangsungkan pendidikan S1 di Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Udayana. Minat *Internet of Things*, *network management*, *fiber optic*.

Halaman kosong