Journal Sistem Informasi, dan Teknologi Informasi

Vol. 2, No 2, Agustus 2023

https://journal-siti.org/index.php/siti/ Published By HPTAI

Analisis Manajemen Risiko Teknologi Informasi Perusahaan Menggunakan Framework ISO 31000 (Studi Kasus: PT. Bank BTPN, Tbk)

Luqman Hakim[1], Ni'matus Shofiyah[2], Halimah Masruroh[3], Firnanda Elysia Puspita Sari[4], Prasasti Karunia Farista Ananto[5]

[1,2,3,4,5]UIN Sunan Ampel Surabaya, Jawa Timur, Indonesia
Email: [1]luqmanhakim396@gmail.com, [2]shofishofiy@gmail.com,
[3]masrurohhalimah143@gmail.com, [4]Firnandaelysiapuspita.s@gmail.com,
[5]prasasti.ananto@uinsby.ac.id

Abstract

Bank BTPN merupakan bank yang bergerak dibidang perbankan umum dengan hasil gabungan dari PT. Bank Tabungan Pensiunan Nasional Tbk dengan PT. Bank Sumitomo Mitsui Indonesia. Semakin berkembangnya jaman, teknologi informasi sudah diterapkan dalam aktivitas bisnis perusahaan perbankan. Dengan menjalankan proses bisnis tentunya ada beberapa risiko berdampak negatif timbul dari aktivitas bisnis tersebut. Maka dari itu, perlu diterapkannya manajemen risiko teknologi informasi. Tujuannya yaitu untuk menganalisis dan mengidentifikasi risiko-risiko yang akan maupun sudah terjadi agar dapat dibentuk proses mitigasinya. Salah satu metode yang akan digunakan dalam analisis manajemen risiko pada PT. Bank BTPN tbk adalah dengan menggunakan standar framework ISO 31000. Dalam prosesnya akan melalui fase identifikasi risiko, penilaian risiko dan evaluasi risiko. Hasil dari proses manajemen risiko tersebut menciptakan matriks kemungkinan dan dampak dari risiko yang telah teridentifikasi. Dengan menerapkan manajemen risiko TI menggunakan framework ISO 31000 diharapkan dapat membantu PT Bank BTPN tbk dalam mencegah risiko dan mengatasi dampak negatif dari risiko tersebut.

Keywords: Manajemen risiko, Teknologi informasi, Analisis risiko, ISO 31000

1. PENGANTAR

Teknologi sistem informasi sangat penting dalam aktivitas bisnis perusahaan. Dalam perbankan, teknologi ini mempermudah nasabah dalam proses transaksi, meningkatkan efisiensi kinerja. Nasabah dapat melakukan transaksi dengan mudah dimana saja dan kapan saja dari layanan teknologi yakni ATM (*Automatic Teller Machine*) dan m-banking (*Mobile Banking*).

PT Bank BTPN Tbk menjadi salah satu bank yang menggunakan teknologi untuk mempermudah nasabah. Bank BTPN merupakan perusahaan yang bergerak pada bidang perbankan umum dengan jasa penanaman modal sesuai dengan prinsip syariah dalam kegiatan usaha tersebut [1]. PT. Bank BTPN Tbk ini memberikan pelayanan pembukaan tabungan, giro dan deposito. Dalam mempermudah nasabah dalam melakukan transaksi, Bank BTPN memberikan teknologi m-banking untuk para nasabah dalam melakukan transaksi melalui aplikasi Jenius. Aplikasi Jenius ini sudah digunakan sejak 2016 dan kini sudah mencapai 7 tahun aplikasi beroperasi.

Dalam perkembangan sistem informasi yang memiliki kemajuan, risiko kegagalan dapat mencapai tujuannya. Risiko adalah kejadian yang merugikan atau menghambat pencapaian tujuan yang diharapkan [2]. Kemajuan teknologi memberi peluang meningkatkan efisiensi bisnis, tapi juga mengancam aplikasi seperti Jenius yang terbukti saat nasabahnya mengalami pembobolan akun sebanyak 3 kali.

Pada bulan Juni dan Juli 2021, terdapat tiga nasabah yang mengalami kerugian akibat penipuan. Nasabah pertama kehilangan 584 juta karena mengatasnamakan admin Jenius BTPN. Nasabah kedua mengalami pembobolan sebesar 110 juta di aplikasi Jenius, sementara nasabah ketiga kehilangan deposito 220 juta dan 21,5 juta di rekening aktif. Total kerugian mencapai 241,5 juta [3]. Untuk menghindari risiko lebih lanjut, perlu dilakukan analisis risiko di PT. Bank BTPN Tbk.

Oleh karena itu, maka diperlukan manajemen risiko IT pada *Framework* ISO 31000, yang digunakan dalam mengurangi kerugian perusahaan pasca kejadian tersebut. Tujuan penelitian ini adalah menganalisis dan memberikan rekomendasi mengenai risiko di PT. Bank BTPN Tbk, dengan menggunakan *Framework* ISO 31000 untuk pencegahan risiko yang efisien.

Tahun 2021, Miftakhun melakukan penelitian dengan menganalisis *website* Ecofo menggunakan ISO 31000 tahun 2021 untuk meneliti risiko pada aset teknologi informasi. Hasilnya adalah dokumentasi 24 risiko yang teridentifikasi: 3 high, 10 medium, dan 11 low yang dapat dipakai untuk pencegahan, penanganan, dan pemeliharaan di masa depan [4].

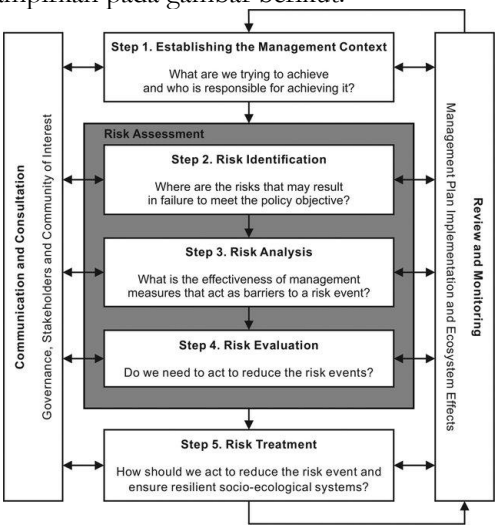
Penelitian yang dilakukan Joshua Ecleas dan Augie David Manuputty membahas mengenai risiko pada *software* PEGA menggunakan ISO 31000. Tujuannya adalah meminimalisir risiko dan mencapai tujuan perusahaan. Hasilnya, mereka mengidentifikasi risiko sistem PEGA melalui matriks kemungkinan dan dampak [5].

2. METODE

Penelitian ini melakukan metode deskriptif kualitatif yang menjelaskan permasalahan, solusi, dan kesimpulan. Pendekatan studi pustaka melibatkan sumber seperti buku, artikel, internet, dan pandangan ahli bidang terkait serta teori relevan yang sesuai dengan masalah yang diteliti.

2.1. Metode penelitian

Penelitian ini menggunakan metode penelitian dengan kerangka kerja ISO 31000, dengan adanya kerangka kerja ini potensi risiko dapat diminimalisir melalui proses *risk assessment* dan *risk treatment*. Dalam *International Organization for Standardization* (ISO 31000), ada dua fase dalam manajemen risiko. Fase awal merupakan penilaian risiko, yaitu proses di mana risiko yang mungkin menghambat pencapaian tujuan bisnis perusahaan dapat diidentifikasi [6]. Adapun metode penelitian manajemen risiko dengan menerapkan kerangka kerja ISO 31000 dapat dilampirkan pada gambar berikut.



Gambar 1. Struktur Manajemen Risiko

Fase penilaian risiko melibatkan tiga tahapan yang mencakup pengidentifikasian risiko, analisis risiko, dan juga penilaian risiko.

1. Pengidentifikasian Risiko: Pada tahap ini mencakup identifikasi risiko yang mungkin timbul selama pelaksanaan suatu kegiatan. Pengenalan yang akurat dan komprehensif merupakan aspek yang sangat penting dalam manajemen risiko.
2. Analisis Risiko: Tahap ini dilakukan evaluasi terhadap potensi risiko dan tingkat kerugian yang mungkin terjadi akibat risiko tersebut. Estimasi

probabilitas pada suatu peristiwa sangat dipengaruhi oleh sudut pandang yang subjektif, seringkali berdasarkan pada pengalaman dan pertimbangan rasional.

3. Penilaian Risiko: Tahap penilaian risiko dilakukan dengan membandingkan tingkat risiko dengan standar yang telah ditetapkan. Tujuan utama penilaian risiko adalah untuk menentukan tingkat prioritas dari yang paling tinggi ke yang paling rendah.

Tahap selanjutnya adalah *risk treatment*. Tahap ini merupakan tahapan dalam menyempurnakan beberapa pilihan yang dapat mengurangi probabilitas dan dampak dari risiko yang akan terjadi.

ISO 31000

ISO 31000, standar internasional manajemen risiko, memberikan panduan efektif bagi organisasi dalam mengelola risiko. Dirancang untuk digunakan oleh organisasi besar atau kecil, ISO 31000 bertujuan menjadi dasar penting dalam membangun kerangka kerja manajemen risiko yang sistematis dan terstruktur. Penerapan standar ini melibatkan tiga elemen: prinsip, kerangka kerja, dan proses [7].

***Framework* Manajemen Risiko**

Framework manajemen risiko adalah suatu sistem yang membantu mengontrol organisasi terhadap risiko secara menyeluruh, dengan tujuan meningkatkan nilai perusahaan [7]. Manajemen risiko melibatkan identifikasi, penilaian, evaluasi, pengukuran, dan pengelolaan risiko [8]. Ada beberapa fungsi yang turut membantu pengambil keputusan memahami risiko perusahaan, juga menghemat waktu, biaya, dan tenaga dalam mengatasi risiko bisnis.

3. HASIL DAN DISKUSI

3.1 Penilaian Risiko

Tahap penilaian risiko, langkah awal dalam penelitian sesuai panduan ISO 31000, dilaksanakan oleh Bank BTPN melalui tiga proses utama: identifikasi risiko, analisis risiko, dan evaluasi risiko [9]. Proses ini adalah langkah krusial dalam melanjutkan ke tahap berikutnya.

3.1.2 Identifikasi Risiko

Proses pertama pada tahap penilaian risiko yakni proses identifikasi risiko atau aset pada Bank BTPN, kemungkinan risiko serta dampak yang terjadi.

3.1.3 Identifikasi Kemungkinan Risiko

Pada tahap kedua, identifikasi risiko aplikasi m-Banking mempertimbangkan tiga faktor pemicu risiko: alam, manusia, dan sistem. Hasilnya, ditemukan 10 risiko terkait aplikasi tersebut, dengan rincian pada Tabel 1.

Tabel 1. Identifikasi Kemungkinan Risiko

Kode	Jenis Risiko	Aspek
R1	Gempa bumi	Alam
R2	Kebakaran	
R3	Peretasan database	Manusia
R4	Penyalahgunaan hak akses oleh pihak lain	
R5	Pencurian hardware	
R6	Kelalaian atau keteledoran nasabah	
R7	Keamanan sistem yang lemah	Sistem
R8	Ketidakstabilan Aplikasi atau Bug	
R9	Gangguan jaringan atau koneksi	
R10	Tampilan pengguna sulit dipahami	

3.1.3 Identifikasi Dampak Risiko

Tahap ketiga melibatkan identifikasi dampak risiko dengan fokus pada dampak yang mungkin terjadi dari risiko yang telah diidentifikasi pada aplikasi m-Banking. Detail dampak risiko dapat dilihat pada tabel berikut.

Tabel 2. Identifikasi Dampak Risiko

Kode	Jenis Risiko	Faktor
R1	Gempa bumi	Kerusakan infrastruktur dan aktivitas bisnis terhenti
R2	Kebakaran	Kerusakan infrastruktur dan aktivitas bisnis terhenti
R3	Peretasan database	Merusak sistem, terjadinya memanipulasi dan mencuri data
R4	Penyalahgunaan hak akses oleh pihak lain	Akses mudah diretas oleh pihak lain sehingga terjadinya pembobolan data
R5	Pencurian hardware	Kurangnya sistem pemantauan keamanan yang dapat rentan terhadap pencurian hardware
R6	Kelalaian atau keteledoran nasabah	kurangnya pemahaman fitur keamanan produk yang menyebabkan uang nasabah hilang
R7	Keamanan sistem yang lemah	Hanya menggunakan sistem keamanan yang standar untuk transaksi maupun login pada m-Banking
R8	Ketidakstabilan Aplikasi atau Bug	Ketidakstabilan pada aplikasi m-banking dapat menyebabkan kesalahan transasi atau kebocoran informasi
R9	Gangguan jaringan atau koneksi	Adanya gangguan jaringan saat data sedang ditransfer dapat menyebabkan kesalahan atau korupsi data
R10	Tampilan pengguna sulit dipahami	Tampilan website dan url yang simple membuat pihak tidak

		berwenang mudah dalam menduplikasi

3.2 Analisis Risiko

Langkah berikutnya adalah analisis risiko, di mana peneliti mengevaluasi potensi risiko yang telah diidentifikasi. Tahap ini fokus pada dua faktor utama, yaitu kemungkinan dan dampak dari setiap risiko [10]. Tabel hasil menunjukkan penilaian risiko pada aplikasi Jenius, dengan rincian nilai risiko, kemungkinan, dan dampak terlampir pada tabel.

Tabel 3. Penilaian Risiko

Kode	Jenis Risiko	Nilai Kemungkinan	Nilai Dampak
R1	Gempa bumi	2	5
R2	Kebakaran	1	5
R3	Peretasan database	3	4
R4	Penyalahgunaan hak akses oleh pihak lain	2	3
R5	Pencurian hardware	1	3
R6	Kelalaian atau keteledoran nasabah	4	4
R7	Keamanan sistem yang lemah	4	5
R8	Ketidakstabilan Aplikasi atau Bug	2	1
R9	Gangguan jaringan atau koneksi	2	4
R10	Tampilan pengguna sulit dipahami	3	1

3.3 Evaluasi Risiko

Tabel 4. Evaluasi Risiko

	Tidak Signifikan	Kecil	Sedang	Serius	Besar
Jarang			R5		R2
Tidak Mungkin	R8		R4	R9	R1
Mungkin	R10			R3	
Kemungkinan Besar				R6	R7
Hampir Pasti					

Tabel 5. Skala Risiko

Kode	Jenis Risiko	Kemungkinan	Dampak	Level
R1	Gempa bumi	2	5	Medium
R2	Kebakaran	1	5	Low
R3	Peretasan database	3	4	Medium
R4	Penyalahgunaan hak akses oleh pihak lain	2	3	Low
R5	Pencurian hardware	1	3	Low
R6	Kelalaian atau keteledoran nasabah	4	4	High
R7	Keamanan sistem yang lemah	4	5	High
R8	Ketidakstabilan Aplikasi atau Bug	2	1	Low

R9	Gangguan jaringan atau koneksi	2	4	Medium
R10	Tampilan pengguna sulit dipahami	3	1	Low

3.4 Penanganan Risiko

Tahapan terakhir yang dilakukan untuk memanajemen risiko merupakan penanganan risiko yang diberikan untuk semua kemungkinan risiko yang ada. Pada proses ini, penulis memberikan penanganan risiko pada berbagai kemungkinan risiko yang ada. Detail penanganan risiko ditampilkan pada Tabel 6.

Tabel 6. Penanganan Risiko

Kode	Risiko	Level Risiko	Penanganan Risiko
R7	Keamanan sistem yang lemah	High	Menggunakan teknologi keamanan dan enkripsi data yang memenuhi standar dunia
R6	Kelalaian atau keteledoran nasabah	High	Melakukan pembuatan fitur untuk mengedukasi nasabah dalam pentingnya menjaga kerahasiaan data
R3	Peretasan database	Medium	Memperbarui sistem patch keamanan yang terbaru, dan melakukan pemantauan kemanan yang intensif
R1	Gempa Bumi	Medium	Menyediakan lokasi yang aman untuk menyimpan data dan server pada mbanking
R9	Gangguan jaringan atau koneksi	Medium	Menyediakan infrastruktur jaringan yang memiliki tingkat redundansi yang tinggi
R4	Penyalahgunaan hak akses oleh	Low	Menerapkan prinsip kebutuhan dasar dalam pemberian hak

	pihak lain		akses sesuai tugas dan tanggung jawab
R10	Tampilan pengguna sulit dipahami	Low	Melakukan audit pada *user research* guna untuk memahami kebutuhan dan tingkat pemahaman pengguna terhadap aplikasi
R8	Ketidakstabilan Aplikasi atau Bug	Low	Melakukan monitoring dalam pemantauan aplikasi secara terus menerus
R2	Kebakaran	Low	Melakukan langkah-langkah pencegahan kebakaran di pusat data atau server, termasuk sistem deteksi asam, peralatan tahan api, dll
R5	Pencurian hardware	Low	Melakukan sistem pemantauan keamanan lokal pada perangkat keras guna mendeteksi pergerakan dalam potensi pencurian

4. KESIMPULAN

Berdasarkan hasil riset analisis risiko teknologi informasi di Bank BTPN dengan menggunakan kerangka kerja ISO 31000 untuk m-banking Jenius terdapat 10 potensi risiko. Terdapat 2 potensi risiko yang high, yaitu keamanan sistem yang lemah dan juga kelalaian atau keteledoran pada nasabah. 3 potensi risiko dengan tingkat level medium yang meliputi peretasan database, gempa bumi, dan gangguan jaringan atau koneksi. Dan adapun 5 potensi risiko di tingkat low, yaitu penyalahgunaan hak akses oleh pihak lain, tampilan pengguna sulit dipahami, ketidakstabilan aplikasi atau bug, kebakaran, dan pencurian hardware.

REFERENSI

[1] "Laporan Tahunan PT.Bank BTPN Tbk 2022." Dec. 31, 2022. [Online]. Available: https://www.btpn.com/pdf/investor/annual-report/2023/ar-2022--btpn_-ina-resize.pdf

[2] Z. Putra, S. Chan, and M. Iha, "Desain Manajemen Risiko Berbasis Iso 31000 pada PDAM Tirta Meulaboh," vol. 1, 2017.

[3] A. Sukmawijaya, "3 Kasus Pembobolan Jenius dalam Waktu Berdekatan," Jul. 27, 2021. [Online]. Available: https://kumparan.com/kumparanbisnis/3-kasus-pembobolan-nasabah-jenius-dalam-waktu-berdekatan-1wDEvNTttcg/3

[4] M. Miftakhatun, "Analisis Manajemen Risiko Teknologi Informasi pada Website Ecofo Menggunakan ISO 31000," *J. Comput. Sci. Eng. JCSE*, vol. 1, no. 2, pp. 128–146, Aug. 2020, doi: 10.36596/jcse.v1i2.76.

[5] J. Ecleas, "Analisis Manajemen Risiko Teknologi Informasi Software PEGA Menggunakan ISO 31000," *JATISI J. Tek. Inform. Dan Sist. Inf.*, vol. 8, no. 1, pp. 209–224, Mar. 2021, doi: 10.35957/jatisi.v8i1.601.

[6] F. Wati, S. Sari, and J. N. Utamajaya, "Manajemen Risiko TI Berbasis ISO 31000 Untuk Aplikasi BRImo (BRI Mobile) Sebagai Sistem Informasi Pemrosesan Transaksi," vol. 2, 2021.

[7] C. Vorst R., D. S. Priyarsono, and A. Budiman, *Manajemen Risiko Berbasis SNI ISO 31000*, 1st ed. Jakarta: Badan Standardisasi Nasional, 2018.

[8] "Framework SNI ISO:31000 2011."

[9] D. L. Ramadhan, R. Febriansyah, and R. S. Dewi, "Analisis Manajemen Risiko Menggunakan ISO 31000 pada Smart Canteen SMA XYZ," *JURIKOM J. Ris. Komput.*, vol. 7, no. 1, p. 91, Feb. 2020, doi: 10.30865/jurikom.v7i1.1791.

[10] H. C. Christian and M. N. N. Sitokdana, "Analisis Risiko Teknologi Informasi pada BANK ABC Menggunakan Framework ISO 31000," vol. 9, no. 1, 2022.