Penerapan Manajemen Risiko IT pada Bank X dengan Menggunakan *Framework COBIT* 2019

William Jordy, Leo Willyanto Santoso, Yulia
Program Studi Sistem Informasi Bisnis
Jl. Siwalankerto 121 – 131 Surabaya 60236
Telp. (031) – 2983455, Fax. (031) - 8417658
Email : c14170073@john.petra.ac.id, leow@petra.ac.id, yulia@petra.ac.id

ABSTRAK

Pada perusahaan Bank X terjadi berbagai permasalahan pada proses bisnis yang melibatkan IT. terjadi permasalahan seperti kondisi jaringan server yang tidak stabil dan mengalami masalah ketika melakukan proses bisnis penginputan data. Tujuan dari penelitian ini adalah mencari tahu faktor atau penyebab apa saja yang paling berpengaruh dalam penggunaan IT pada proses bisnis Bank X dan memberikan response terhadap risiko yang ada berdasarkan panduan CobiT 2019 dengan domain Align, Plan and Organize (APO) pada proses APO 11 Managed Quality dan APO 12 Managed Risk. Metodologi Penelitian akan dilakukan dengan meneliti capability level dan melakukan penilaian risiko menggunakan standar OWASP pada domain APO11 dan APO12 sesuai dengan hasil yang ada pada Mapping Alignment Goal (AG) dan Enterprise Goal (EG) serta dimensi BSC. Berdasarkan hasil penelitian yang dilakukan, penulis mendapati beberapa risiko yang berdampak pada proses bisnis IT perusahaan beserta dengan respon dan solusi yang diberikan. Solusi yang diberikan adalah dengan melakukan Mitigate atau Avoid tergantung dari risk severity risiko - risiko tersebut. Kesimpulan dari penelitian ini adalah Divisi IT memiliki peran penting dalam menjalankan proses bisnis perusahaan. Selain berperan sebagai support, divisi IT juga memiliki peran dalam melakukan software development dalam aplikasi - aplikasi perbankan customer, keterbukaan responden dan divisi IT sebagai support system perusahaan menjadi faktor penting dalam membantu penelitian ini.

Kata Kunci: Risk Assessment, Risk Management, Quality Management dan solusi.

ABSTRACT

At Bank X, various problems occurred in business processes involving IT. problems occur such as unstable server network conditions and experiencing problems when carrying out business processes inputting data. The purpose of this thesis is to find out what factors or causes are the most influential in the use of IT in Bank X's business processes and provide a response to existing risks based on the 2019 CobiT guidelines with the Align, Plan and Organize (APO) domain in the APO 11 Managed Quality process. and APO 12 Managed Risk. Methodology The research will be conducted by examining the capability level and conducting a risk assessment using the OWASP standard in the APO11 and APO12 domains in accordance with the results in the Mapping Alignment Goal (AG) and Enterprise Goal (EG) as well as the BSC dimensions. Based on the results of research conducted, the authors found several risks that have an impact on the company's IT business processes along with the responses and solutions provided. The solution given is to Mitigate or Avoid depending on the risk severity of the risks. The conclusion of this research is that the IT Division has an important role in running the company's business processes. In addition to acting as support, the IT division also has a role in software development in customer banking applications, respondent transparency and the IT division as the company's support system are important factors in assisting this research.

Keywords: Risk Assessment, Risk Management, Quality Management and Solutions.

1. PENDAHULUAN

PT Bank X Tbk. didirikan pada 18 Agustus 1989 berdasarkan Akta No. 52 tanggal 18 Agustus 1989, Bank memperoleh status sebagai Bank Umum Devisa tahun 1995. Pada 13 Desember 2010, Bank X melakukan Penawaran Saham Umum Perdana (*Initial Public Offering*/IPO) dengan struktur permodalan sebesar Rp728 miliar dan dengan mengeluarkan Waran Seri I. Pada Bank X terjadi permasalahan seperti kondisi jaringan server yang tidak stabil dan mengalami masalah ketika melakukan proses bisnis penginputan data. Hal ini dikarenakan setiap data nasabah yang ada akan selalu dimasukkan kedalam server, dan mengakibatkan kapasitas memory yang ada pada server Bank X menjadi tidak cukup untuk menampung data yang ada. Selain itu terjadi kerusakan *hardware* yang diakibatkan oleh kelalaian user. Untuk mengetahui kebutuhan (*requirement*) perusahaan serta mengukur kinerja dan mengintegrasikan tata kelola I&T dengan tata kelola dan strategi bisnis secara keseluruhan melalui pemetaan tujuan kontrol ke proses COBIT diperlukan adanya Mapping terkait Alignment Goal (AG) dan Enterprise Goal (EG). Mapping ini dibuat untuk mengetahui domain dan objective perusahaan apa saja yang menjadi kebutuhan utama dan sekunder dari perusahaan. Pada penelitian ini akan dilakukan proses risk assessment terhadap quality management dan risk management dalam layanan IT untuk mengetahui risiko apa saja yang akan terjadi, seberapa besar risiko tersebut, intensitas frekuensi (seberapa sering risiko terjadi). Dari hasil analisa akan ditunjukkan risiko mana yang memiliki nilai (score) yang paling tinggi agar dapat dilakukan penanganan. Perusahaan dapat menggunakan risk assessment sebagai suatu pertimbangan untuk pengambilan keputusan yang dapat bermanfaat bagi perusahaan untuk meningkatkan proses bisnis yang terjadi.

2. TINJAUAN PUSTAKA

2.1 Bank X

PT Bank X Tbk. didirikan pada 18 Agustus 1989 berdasarkan Akta No. 52 tanggal 18 Agustus 1989, Bank memperoleh status sebagai Bank Umum Devisa tahun 1995. Pada 13 Desember 2010, Bank X melakukan Penawaran Saham Umum Perdana (*Initial Public Offering*/IPO) dengan struktur permodalan sebesar Rp728 miliar dan dengan mengeluarkan Waran Seri I. Bank X telah membuka cabang salah satunya berlokasi di kota Ende.

2.2 ISO 31000:2018 (versi 2018)

Secara umum, ISO 31000:2018 menyederhanakan versi 2009.Hal itu langsung terlihat antara lain dari nama yang berubah dari "principles and guidelines" menjadi hanya "guidelines" serta dari jumlah halaman yang menyusut dari 24 halaman menjadi 16 halaman. Diagram yang menggambarkan hubungan prinsip, kerangka kerja, dan proses manajemen proses pun berubah. Selain itu, jumlah "principles" pada versi yang lama terdapat 11 prinsip [6]. Dapat dikatakan bahwa ISO versi 2009 memiliki beberapa kerangka kerja yang tertutup [13]. Pada versi 2009, prinsip, kerangka kerja, dan proses digambarkan sebagai rangkaian unsur yang berurutan, sedangkan pada versi 2018 ketiga bagian ini digambarkan sebagai sistem terbuka yang saling berkaitan.[11]. Menurut BSI ISO 31000:2018 diatur berdasarkan 8 prinsip risiko, yaitu : [7]

- Terintegrasi
- Terstruktur dan komprehensif
- Disesuaikan
- Inklusif
- Dinamis
- Informasi terbaik yang tersedia
- Faktor manusia dan budaya
- Perbaikan berkelanjutan

ISO 31000:2018 juga akan digunakan sebagai panduan dalam penilaian risiko berdasarkan *severity* [16]

2.3 CobiT 2019

Pengertian Cobit COBIT (*Control Objectives for Information and Related Technology*) adalah sekumpulan dokumentasi *best practices* untuk IT Governance yang dapat membantu auditor, pengguna (user), dan manajemen, untuk menjembatani gap antara risiko bisnis, kebutuhan control dan masalah-masalah teknis IT. Dalam CobiT terdapat 5 domain yaitu: (1). Evaluate, Direct and Monitor (EDM), (1). Align, Plan and Organize (APO), (2). Build, Acquire and Implement (BAI), (3). Delivery, Service and Support (DSS), (4). Monitoring, Evaluate and Assess (MEA). Penelitian ini akan berfokus pada domain Align, Plan and Organize (APO) [1]. Cobit 2019 adalah evolusi dari versi sebelumnya, COBIT 5.

2.3.1 Alignment Goal (AG) Mapping to CobiT 2019

Hasil Mapping *AG* digunakan untuk mengetahui penyelarasan antara tujuan perusahaan terhadap *CobiT 2019* [4]. Dari Mapping yang telah dibuat diketahui jumlah hubungan Primary (P) pada APO11 dan APO12 yang paling mendominasi. Pada APO11 terdapat 3 hubungan Primary pada AG5, AG9, dan AG10. Lalu, pada APO12 terdapat 2 hubungan Primary (P) pada AG02 dan AG07.

2.3.2 Enterprise Goal (AG) Mapping to CobiT 2019

Hasil Mapping *EG* digunakan untuk mengetahui antara tujuan perusahaan dari 4 persepktif, yaitu : *financial, internal, customer,* dan *learning & growth* terhadap *CobiT 2019* [4]. Pada Mapping EG diketahui bahwa hubungan Primary paling banyak dijumpai pada perspektif Financial dan Internal pada dimensi Balance Scorecard (BSC). karena hubungan primary yang paling banyak pada perspektif Financial dan Internal, maka penerapan CobiT 2019 akan dilakukan pada kedua dimensi BSC tersebut.

2.3.3 Align Plan and Organize (APO)

APO membahas keseluruhan organisasi, strategi dan aktivitas pendukung untuk I&T [12]

1. APO 11 (Managed quality)

Tujuan dari APO11 adalah untuk memastikan pengiriman solusi dan layanan teknologi yang konsisten untuk memenuhi persyaratan kualitas perusahaan dan memenuhi kebutuhan pemangku kepentingan (stakeholders). Terdapat 5 control objective pada APO11 [2], yaitu :

- APO11.01 Establish a quality management system (QMS).
- APO11.02 Focus quality management on customers.
- APO11.03 Manage quality standards, practices and procedures and integrate quality management into key processes and solutions.
- APO11.04 Perform quality monitoring, control and reviews.
- APO11.05 Maintain continuous improvement.

2. APO 12 (Managed Risk)

APO12 bertujuan untuk mengintegrasikan manajemen risiko perusahaan terkait I & T dengan manajemen risiko perusahaan (ERM) secara keseluruhan dan menyeimbangkan biaya dan manfaat dari pengelolaan risiko perusahaan terkait I & T. PO9 memiliki 6 control objective [3], yaitu :

- APO12.01 Collect data.
- APO12.02 Analyze risk.
- APO12.03 Maintain a risk profile.
- APO12.04 Articulate risk.
- APO12.05 Define a risk management action portfolio.
- APO12.06 Respond to risk.

2.4 Risk Rating Methodology by OWASP

Open Web Application Security Project (OWASP) memiliki metode untuk melakukan penilaian kriteria. Penilaian kriteria dalam OWASP dilaksanakan dengan mengukur Likelihood dan Impact [17]. Terdapat 2 faktor yang digunakan dalam mengestimasi Likelihood, yaitu: Threat Agent Factors dan Vulnerability Factors

2.4.1 Likelihood

a. Threat Agent Factors

Tujuannya adalah untuk memperkirakan kemungkinan serangan yang berhasil dilakukan oleh kelompok agen ancaman ini, Threat Agent Factors diperkirakan berdasarkan : Skill Level, Motive, Opportunity, dan Size.

b. Vulnerability Factors

Tujuan Vulnerability Factors di sini adalah untuk memperkirakan kemungkinan kerentanan tertentu yang terlibat ditemukan dan dieksploitasi. Vulnerability Factors terbagi menjadi 4, yaitu : Ease of Discovery, Ease of Exploit, Awareness, Intrusion Detection.

2.4.2 Impact

a. Technical Impact Factor

Tujuan dari Technical Impact Factors adalah untuk memperkirakan besarnya dampak pada sistem jika kerentanan akan dieksploitasi. Technical Impact Factors akan dinilai berdasarkan : Loss of Confidentiality, Loss of Integrity, Loss of Availability, Loss of Accountability

b. Business Impact Factors

Tujuan Business Impact Factors adalah memperkirakan dampak risiko terhadap proses bisnis perusahaan ketika kerentanan berhasil di eksploitasi. Business Impact

Factors, akan dinilai berdasarkan : Financial damage, Reputation Damage, Non-compliance, Privacy Violation.

3. METODE PENELITIAN

3.1 Analisa IT Perusahaan

Pada bagian ini akan dijelaskan analisa IT pada Bank X. Pada analisa ini peneliti akan memberikan gambaran mengenai IT pada Bank X dengan menjabarkannya menjadi 3 subbab. Ketiga subbab tersebut antara lain, adalah: Data Perusahaan, Aplikasi Perusahaan, dan Teknologi perusahaan. Berikut penjelasan yang ada :

3.1.1 Data Perusahaan

Bank X yang terletak pada cabang daerah Ende memiliki satu database server. Cabang pada daerah Ende ini merupakan cabang baru dengan wilayah yang lebih kecil dibandingkan di NTT. database server ini digunakan untuk menyimpan data yang digunakan untuk beberapa aplikasi yang ada. Database yang disimpan menggunakan *Database Management System* (DBMS) Oracle. Data yang terdapat di dalam database perusahaan Bank X adalah: data nasabah, data tabungan, data deposito, data giro, data reksadana, data bancassurance, data layanan & transaksi, dan data kartu kredit.

3.1.2 Aplikasi Perusahaan

3.1.2.1 Simobi Plus

SimobiPlus merupakan layanan Internet Banking Bank Sinarmas versi mobile yang dikembangkan untuk nasabah Bank Sinarmas melakukan transaksi perbankan dengan mudah melalui smartphone berbasis Android dan iOS. Aplikasi SimobiPlus dapat dibilang sebagai ujung tombak yang mendukung proses bisnis IT pada Bank X. Hal ini dikarenakan pada aplikasi SimobiPlus user dapat melakukan hampir semua proses bisnis seperti : Pembukaan Rekening, Deposito, Transaksi / Transfer antar sesama rekening Bank X ataupun rekening Bank lain, Mutasi Rekening, pembayaran berbagai macam tagihan, dan kegiatan internet/mobile banking lainnya.

3.1.2.2 PEGASYSTEMS

Pegasystems.Inc adalah Master software untuk keunggulan operasional dan Customer engagement. Pega merancang perangkat lunak untuk manajemen proses bisnis (BPM), otomatisasi proses digital dan manajemen hubungan pelanggan (Customer Relationship Management) [8]. Proses bisnis maintain nasabah merupakan bagian dari support system Bank X. Proses ini membuat rancangan software untuk customer relationship management dan business process management. Proses bisnis ini merupakan bagian dari internal pada perusahaan sehingga tidak terlibat secara langsung dengan nasabah yang ada.

3.1.3 Teknologi Perusahaan

Pada bagian ini akan dijelaskan mengenai teknologi yang ada pada Bank X. Bank X cabang Ende memiliki total komputer sebanyak 8 unit yang tersebar dalam kantor. Sebanyak 4 komputer berbasis windows 7 dan memiliki processor intel i5 dengan graphic card nvidia geforce 700m. Keempat komputer ini digunakan untuk keperluan dalam kantor dimana 2 diantaranya digunakan oleh cashier, 1 digunakan untuk customer service, dan 1 digunakan untuk mencatat detail rekening. Keempat komputer lainnya digunakan oleh Manajer kepala cabang, Manajer Divisi IT, dan Anggota Divisi IT. Keempat komputer ini menggunakan processor intel i7 dengan graphic card nvidia 800m.

3.2 Permasalahan IT pada Bank X

Pada bagian ini akan dijelaskan permasalahan umum yang sering terjadi pada perusahaan Bank X. Permasalahan yang ada pada aplikasi akan dipisahkan antara SimobiPlus dan PegaSystems. SimobiPlus mencakup hampir seluruh proses bisnis yang ada pada Bank X, sedangkan PEGA System hanya mencakup bagian proses bisnis IT internal perusahaan dalam hal maintain nasabah. Beberapa permasalahan tersebut, antara lain: Jaringan *Server* yang tidak stabil, *Single Device usage only*, *Changing Device Number*, *Log-in issues*, *Difficult Technical Setup*, *Filtering Problems*, *Drill-Down Problems*

3.3 Proses Bisnis IT pada Bank X

3.3.1 Pembukaan Rekening

Proses bisnis ini bertujuan untuk mendaftarkan seseorang menjadi bagian dari anggota nasabah Bank X, untuk mendaftarkan diri menjadi bagian dari nasabah seseorang perlu mengisi formulir pembukaan rekening, melampirkan fotokopi KTP dan NPWP dan mengunduh formulir pembukaan tabunganku. Minimal setoran untuk pembukaan rekening adalah Rp 20.000,00 dan memiliki suku bunga yang beragam mulai dari 0%, 0.25%, dan 1.00%. Proses bisnis pembukaan rekening sangat krusial dalam dunia perbankan begitu pula dengan Bank X. Hal ini dikarenakan nasabah adalah penanam modal dalam dunia perbankan dan instansi perbankan seperti Bank X memerlukan uang dari nasabah untuk pinjaman, dan lain sebagainya.

3.3.2 Deposito

Pengertian dari deposito adalah produk simpanan di bank yang penyetorannya maupun penarikannya hanya bisa dilakukan pada waktu tertentu saja. Apabila dana yang disimpan diambil sebelum waktunya, maka dapat dikenakan denda penalti. semakin besar dan semakin lama Anda menyimpan dana dalam bentuk deposito, maka semakin besar pula bunga yang ditawarkan. Agar dapat melakukan deposito pada Bank X, nasabah perlu memiliki rekening tabungan/giro Bank X dengan minimal nominal Rp 500.000,00. Deposito pada Bank X dapat dilakukan secara online dengan aplikasi *mobile*. Proses bisnis Deposito penting bagi Bank X, karena merupakan proses bisnis investasi dimana nasabah memasukkan jumlah nominal besar kepada Bank yang tidak boleh diambil dalam kurun waktu tertentu.

3.3.3 Transaksi / Transfer

Bank X memiliki aplikasi yang dapat digunakan untuk melakukan transaksi perbankan secara online antar sesama rekening Bank X misalnya rekening sendiri ataupun orang lain, juga dapat bertransaksi dengan rekening Bank lain akan tetapi memiliki batas (*limit*) nominal transaksi. Transaksi ≤ Rp. 5 Juta menggunakan Easy PIN, Transaksi > Rp. 5 Juta menggunakan SMS OTP, dan transfer ke rekening sendiri dan pembukaan deposito online selalu menggunakan Easy PIN. Proses Transaksi adalah bagian utama (*core*) dari proses bisnis perbankan sehingga sangat penting bagi perusahaan dan nasabah.

3.3.4 Maintain Nasabah

Untuk mengatur dan melakukan *maintain* pada nasabah, Bank X menggunakan aplikasi bernama PEGA. Pegasystems.Inc adalah Master software untuk keunggulan operasional dan Customer engagement. Pega merancang perangkat lunak untuk manajemen proses bisnis (BPM), otomatisasi proses digital dan manajemen hubungan pelanggan (Customer Relationship Management) (Ham, H., 2019). Proses bisnis maintain nasabah merupakan bagian dari *support system* Bank X. Proses ini membuat rancangan *software*

untuk *customer relationship management* dan *business process management*.

3.3.5 Internet Banking / Mobile Banking

Internet banking adalah kegiatan yang melakukan transaksi, pembayaran, dan transaksi lainnya melalui internet dengan website milik bank yang dilengkapi sistem keamanan. Berbeda dengan mobile banking yang harus menggunakan aplikasi, internet banking dapat diakses langsung melalui browser kamu. Untuk menggunakan fitur dari internet banking ini, nasabah membutuhkan user id, password, token atau one time password (OTP) terlebih dahulu. Untuk mendapatkan user id, password, dan token, nasabah bisa mendatangi bank terlebih dahulu untuk melakukan pendaftaran. Setelah itu, nasabah bisa menggunakan internet banking dengan leluasa. Proses Mobile Banking / Internet Banking penting karena merupakan bentuk digitalisasi dan *support system* bagi proses bisnis yang ada pada Bank X. Karena memudahkan nasabah dalam melakukan proses transaksi, proses bisnis ini penting bagi perusahaan dan nasabah.[14]

3.4 Persiapan Pengumpulan Data

3.4.1 Responden

Tabel 3.1 Tabel Responden

Peran / Posisi / jenis responden	***No / Jumlah***
Kepala Cabang	1
Manajer Divisi IT	1
Anggota Divisi IT	2
Customer Service / Pegawai	4

Tabel 3.1 menampilkan data responden yang akan diwawancarai untuk Analisa risiko berdasarkan domain *APO11* dan *APO12*.

3.4.2 Cara Mendesain atau merancang Pertanyaan

Pertanyaan dirancang dengan menjabarkan setiap management practices yang ada pada suatu subdomain. Langkah ini bertujuan untuk membagi subdomain menjadi beberapa segmen untuk memudahkan pembuatan pertanyaan pada kuesioner. Penjabaran subdomain menjadi management practices ini dapat dilihat pada panduan CobiT 2019. Poin - poin pada subdomain CobiT dapat digali menjadi berbagai pertanyaan.

3.4.3 Desain / Rancangan Pertanyaan

Pertanyaan yang akan diajukan kepada responden akan menggunakan standar CobiT 2019 sesuai dengan domain Align, Plan and Organize (APO) pada subdomain APO11 Managed Quality dan APO12 Managed Risk. Pertanyaan akan diberikan untuk melakukan assesment pada Capability Level kedua domain tersebut pada Bank X. Cara memberikan assessment pada capability level adalah dengan memberikan sebuah rating berupa nilai dari angka 1-5. Setiap angka yang ada memiliki nilainya masing- masing antara lain :

- Initial—Proses tak terduga yang tidak terkontrol dengan baik dan reaktif
- Managed—Proses direncanakan, didokumentasikan, dan dipantau di tingkat proyek dan seringkali bersifat reaktif
- Defined—Proses proaktif dimaksudkan untuk organisasi
- Quantitatively Managed—Proses yang terukur dan terkendali
- Optimizing—Fokus pada proses dan peningkatan berkelanjutan

4. ANALISA RISIKO

Pada Bagian sebelumnya (Bagian 3) penulis telah membahas kondisi perusahaan seperti proses bisnis apa saja yang melibatkan IT dalam perusahaan, analisa IT pada perusahaan, hardware dan software yang digunakan pada perusahaan, dan permasalahan IT / Teknologi Informasi yang terdapat dalam perusahaan Bank X. Pada Bagian Bab 4 penulis akan membahas mengenai wawancara bersama para responden yang detailnya dapat dilihat pada Bab 3.4.2 Responden. Wawancara akan dilakukan dengan menggunakan data sekunder secara deskriptif [9]. Hasil wawancara akan dilakukan secara naratif sesuai dengan referensi Kurniati [10]. Hasil wawancara ini nantinya akan dianalisis dan digolongkan berdasarkan kategori mulai dari *low* hingga *high* [15].

4.1 Analisa Risiko berdasarkan Domain APO11 (Managed Quality)

4.1.1 Analisa Risiko berdasarkan APO11.01 (Establish a quality management system (QMS))

Berdasarkan wawancara yang dilakukan peneliti mendapati beberapa poin / faktor yang dapat menyebabkan risiko terhadap perusahaan, seperti:

- Tidak terdapat pedoman QMS untuk kinerja divisi IT
- Kondisi stagnant pada perkembangan divisi IT, karena belum ada perencanaan lebih lanjut terhadap pengembangan teknologi informasi dan SOP pada perusahaan
- Jadwal kegiatan pekerjaan yang kadang tidak selesai tepat waktu karena tidak adanya QMS.
- Beberapa proses bisnis yang terganggu karena divisi IT tidak on time.

4.1.2 Analisa Risiko berdasarkan APO11.02 (Focus quality management on customers)

Berdasarkan hasil wawancara APO11.02 peneliti menemukan beberapa poin/faktor yang dapat mengakibatkan risiko pada perusahaan, seperti:

- Divisi IT tidak begitu memahami kebutuhan customer
- Customer kurang memahami software yang sebenarnya mereka butuhkan sehingga feedback terkesan kurang maksimal
- Jumlah anggota divisi IT yang lebih sedikit mengakibatkan banyak review / feedback yang tidak diberikan secara berkala, dan kewalahan yang terjadi dalam menangani masalah.

4.1.3 Analisa Risiko berdasarkan APO11.03 (Manage quality standards, practices and procedures

and integrate quality management into key processes and solutions)

Berdasarkan wawancara yang dilakukan peneliti mendapati beberapa poin / faktor yang dapat menyebabkan risiko terhadap perusahaan, seperti:

- Alur bug resolving yang dapat dibilang panjang pada software yang dibuat oleh pihak eksternal, karena membutuhkan bantuan pihak eksternal untuk menyelesaikkannya
- Proses bisnis dapat terganggu karena bug resolving yang memakan waktu
- Tidak adanya proses testing yang menyeluruh, hal ini menyebabkan proses kerja divisi IT hanya mengandalkan feedback dari user yang ada.

4.1.4 Analisa Risiko berdasarkan APO11.04 (Perform quality monitoring, control and reviews)

Berdasarkan wawancara yang dilakukan peneliti mendapati beberapa poin / faktor yang dapat menyebabkan risiko terhadap perusahaan, seperti:

- Perusahaan memiliki alur resolving yang lebih lambat dikarenakan harus melapor pada kantor pusat di NTT terlebih dahulu.
- Perusahaan tidak mengetahui apakah metode untuk melakukan penilaian sudah sesuai dengan tuntutan zaman.

4.1.5 Analisa Risiko berdasarkan APO11.05 (Maintain continuous improvement)

Berdasarkan wawancara yang dilakukan peneliti mendapati beberapa poin/faktor yang dapat menyebabkan risiko terhadap perusahaan, seperti:

- Divisi IT tidak memiliki arahan / panduan yang jelas untuk menyelesaikan pekerjaannya.
- SOP saat ini beresiko tidak dapat mengcover dan mengimbangi tujuan perusahaan.

4.2 Hasil Pengujian

4.2.1 Analisa Risiko berdasarkan APO12.01 (Collect data)

Berdasarkan wawancara yang dilakukan peneliti mendapati beberapa poin/faktor yang dapat menyebabkan risiko terhadap perusahaan, seperti:

- Divisi IT tidak bisa memprediksi risiko - risiko yang akan dihadapi perusahaan dimasa mendatang.
- Pencegahan dinilai kurang dikarenakan penanganan akan dilakukan ketika risiko sudah terkena pada perusahaan.

4.2.2 Analisa Risiko berdasarkan APO12.02 (Analyze risk)

Berdasarkan wawancara yang dilakukan peneliti mendapati beberapa poin/faktor yang dapat menyebabkan risiko terhadap perusahaan, seperti:

- Perusahaan tidak dapat menentukan tingkat prioritas risiko secara akurat
- Perusahaan tidak dapat mengetahui dampak risiko kepada proses bisnis

4.2.3 Analisa Risiko berdasarkan APO12.03 (Maintain a risk profile)

Berdasarkan wawancara yang dilakukan peneliti mendapati beberapa poin/faktor yang dapat menyebabkan risiko terhadap perusahaan, seperti:

- Perusahaan tidak dapat memiliki dokumentasi khusus untuk profil risiko yang ada
- Aktivitas perusahaan terhambat karena tanpa adanya laporan / dokumentasi khusus maka proses penanganan risiko akan menjadi lebih lama.

4.2.4 Analisa Risiko berdasarkan APO12.04 (Articulate risk)

Berdasarkan wawancara yang dilakukan peneliti mendapati beberapa poin/faktor yang dapat menyebabkan risiko terhadap perusahaan, seperti:

- Terdapat berbagai risiko yang berdampak bagi perusahaan
- Perusahaan tidak mengetahui secara pasti dampak risiko baik secara bisnis maupun materil.

4.2.5 Analisa Risiko berdasarkan APO12.05 (Define a risk management action portfolio)

Berdasarkan wawancara yang dilakukan peneliti mendapati beberapa poin/faktor yang dapat menyebabkan risiko terhadap perusahaan, seperti:

- Jika terjadi kejadian yang berulang - ulang (repeatable), divisi IT dan perusahaan tidak dapat menentukan langkah yang optimal, karena tidak ada pencatatan khusus.

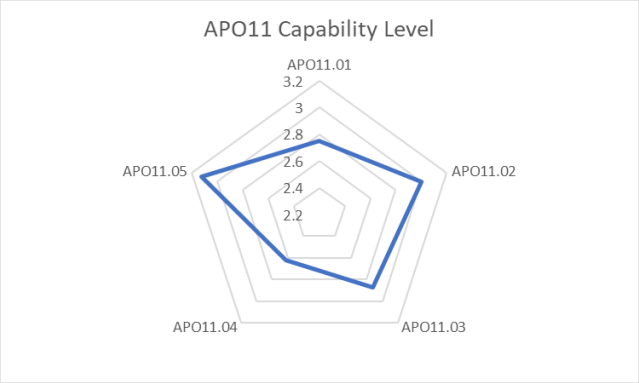
4.2.6 Analisa Risiko berdasarkan APO12.06 (Respond to risk)

Berdasarkan wawancara yang dilakukan peneliti mendapati bahwa perusahaan telah memiliki respon terhadap risiko - risiko yang ada. Selain itu, divisi IT juga sudah melakukan komunikasi 2 arah dengan perusahaan terhadap risiko - risiko tersebut.

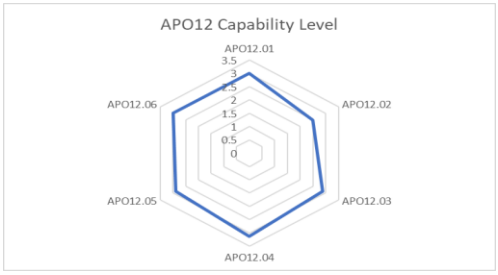
5. PENILAIAN RISIKO

5.1 Penilaian Capability Level

Penilaian *Capability Level* akan menggunakan referensi dari penelitian Atrinawati [5]



Gambar 5.1 Diagram Capability Level APO11



Gambar 5.2 Diagram Capabilty Level APO12

Gambar 5.1 dan Gambar 5.2 menampilkan hasil wawancara Diagram *Capability Level* yang diberikan kepada 3 responden, yaitu : 1 orang Manajer divisi IT, dan 2 orang anggota divisi IT.

5.2 Penilaian Risk Identification

Terdapat 11 faktor Risiko berserta dampaknya pada aktivitas proses bisnis perusahaan. Dari 11 faktor risiko tersebut terdapat berbagai penilaian Likelihood, yaitu : 2 Low, 8 Medium, dan 1 High. Dari 11 faktor risiko tersebut terdapat berbagai Penilaian Impact yaitu : 2 Technical Impact Low, 9 Technical Impact Medium, 3 Business Impact Low, dan 8 Business Impact High. Berdasarkan hasil penilaian Risk Severity terdapat 1 risiko dengan nilai Note, 3 risiko dengan nilai Low, 6 risiko dengan nilai Medium, dan 1 risiko dengan nilai High.

5.3 Penilaian Risk Response

Tabel 5.1 Penilaian Risk Response

Peringkat	No	Risiko	Risk Severity	Response
1	12	Belum ada pengembangan lebih lanjut terhadap respon dan asesmen risiko yang ada	High	Avoid
2	10	Tidak ada analisa terhadap risiko residual	Medium	Mitigate
3	4	Proses pemecahan masalah / *resolving* ketika terjadi error atau bug menjadi lebih lama, dikarenakan harus mengontak kantor pusat di NTT.	Medium	Mitigate
4	8	Tidak ada perhitungan khusus dalam menghitung dampak dan frekuensi terjadinya risiko	Medium	Avoid
5	6	Belum ada perencanaan untuk mengembangkan SOP dan QMS pada perusahaan	Medium	Mitigate

Tabel 5.2 Lanjutan Penilaian Risk Response

Peringkat	No	Risiko	Risk Severity	Response
6	5	Tidak ada standar / pedoman khusus yang mengatur jalannya proses IT secara keseluruhan pada perusahaan	Medium	Mitigate
7	1	Divisi IT tidak memiliki pedoman QMS untuk menjalankan pekerjaannya	Medium	Mitigate
8	11	Tidak ada respon yang terstruktur berdasarkan faktor biaya, manfaat, dan waktu	Medium	Mitigate

Tabel 5.3 Lanjutan Penilaian Risk Response

Peringkat	No	Risiko	Risk Severity	Response
9	9	Tidak ada dokumentasi atau pencatatan secara khusus terkait event / risiko yang mengganggu proses bisnis perusahaan	Low	Mitigate
10	7	Tidak ada dokumentasi atau laporan khusus pada risiko yang dialami oleh perusahaan	Low	Mitigate
11	2	SOP yang sederhana tidak mengcover seluruh pekerjaan divisi IT	Note	Mitigate

Tabel 5.1, Tabel 5.2, dan Tabel 5.3 menampilkan hasil dari penilaian *Risk Response* oleh kesebelas risiko yang ditemukan oleh peneliti. Kategori *risk severity* memiliki nilai mulai dari low hingga high dan *response* memiliki nilai *avoid, mitigate*, dan *share.*

6. KESIMPULAN DAN SARAN

6.1 Kesimpulan

Dari proses penelitian yang telah dilakukan oleh peneliti pada perusahaan Bank X dapat disimpulkan beberapa poin, antara lain:

- Divisi IT memiliki peran penting dalam menjalankan proses bisnis perusahaan. Selain berperan sebagai support, divisi IT juga memiliki peran dalam melakukan software development dalam aplikasi - aplikasi perbankan customer. Komunikasi antara divisi IT dan

customer memiliki peranan penting dalam kelancaran proses bisnis perusahaan.

- Pada Wawancara yang dilakukan bersama dengan responden dari perusahaan Bank X, didapati 11 risiko yang telah diurutkan berdasarkan prioritas dan diberikan respon / solusi yang diberikan oleh penulis sebagai masukan bagi perusahaan.

6.2 Saran

Dalam penelitian ini, informasi dari responden merupakan peran penting dalam mengetahui kondisi dalam perusahaan. Informasi yang diberikan oleh responden juga berguna dalam penulisan penelitian ini. Perusahaan juga disarankan menggunakan standar dalam menjalankan pekerjaan divisi IT. Respon yang diberikan untuk perusahaan terkait risiko - risiko yang ada juga dapat membantu mengurangi dampak yang diberikan oleh risiko pada perusahaan.

7. DAFTAR PUSTAKA

[1] Admin. 2019 June 2. Align, Plan and Organise (COBIT 2019). URI=https://wiki.process-symphony.com.au/framework/lifecycle/align-plan-and-organise-cobit/

[2] Admin. 2019 June. Quality Management – APO11 (COBIT2019). URI= https://wiki.process-symphony.com.au/framework/lifecycle/process/quality-management-apo11-cobit2019/

[3] Admin. 2019 June 2. Risk Management-APO12 (COBIT2019). URI= https://wiki.process-symphony.com.au/framework/lifecycle/process/risk-management-apo12-cobit2019/

[4] Anoruo, C. 2019 October 28. Employing COBIT 2019 for Enterprise Governance Strategy. URI= https://www.isaca.org/resources/news-and-trends/industry-news/2019/employing-cobit-2019-for-enterprise-governance-strategy

[5] Atrinawati, I., et.al. 2020. Assessment of Process Capability Level in University XYZ Based on COBIT 2019 (Yogyakarta, Indonesia October 08 - 09, 2020). 1 – 11. DOI= 10.1088/1742-6596/1803/1/012033

[6] businessaustralia. 2009. Best Practice Principles for undertaking risk management. URI= https://www.businessaustralia.com/how-we-help/be-a-better-employer/managing-risk/best-practice-principles-for-undertaking-risk-management-on-your-business

[7] BSI. 2018 February 28. BS ISO 31000:2018. URI= http://lpm.uin-suka.ac.id/media/dokumen_akademik/011_20191007_ISO%2031000.2018%20-%20Risk%20Management%20-%20Guidelines.pdf

[8] Ham, H. 2019. PEGA SYSTEM. URI= https://socs.binus.ac.id/2019/12/23/pega-system/

[9] Kiky, A. 2020 March. Manajemen risiko terhadap black swan event maret 2020 di Indonesia. Studi Kasus efek covid-19 terhadap pasar modal Indonesia (Tangerang, Banten March 2020). 90 – 105. DOI= https://doi.org/10.52859/jbm.v8i2.89

[10] Kurniati, A., et.al. 2020, December 14. Information Technology Risk Management on e-Government: Systematic Literature Review (Yogyakarta, Indonesia December 2020). 207 – 222. DOI= http://dx.doi.org/10.33164/iptekkom.22.2.2020.207-222

[11] Lanin, I. 2018. Standar Baru Manajemen Risiko ISO 31000:2018. URI= https://grc-indonesia.com/standar-baru-manajemen-risiko-iso-310002018/#:~:text=Pada%20Februari%202018%2C%20organisasi%20standar,%3A2018%20Risk%20management%20%E2%80%94%20Guidelines.&text=ISO%2031000%20adalah%20panduan%20penerapan,%2C%20dan%20proses%20(process).

[12] Lanter, D.D. 2018. COBIT 2019. URI= https://community.-mis.temple.edu/mis5203sec001sp2019/files/2019/01/COBIT-2019-Framework-Introduction-and-Methodology_res_eng_1118.pdf

[13] Mahendra, R. 2016 April 4. ISO 31000, Standar Manajemen Risiko. URI= https://isoindonesiacenter.com/iso-31000-standar-manajemen-risiko.

[14] Oktriwina, A.S. 2021 March 15. Mobile Banking dan Internet Banking, Apa Bedanya?. URI= https://glints.com/id/lowongan/mobile-banking-internet-banking/#:~:text=Internet%20banking%20adalah%20kegiatan%20yang,bank%20yang%20dilengkapi%20sistem%20keamanan.&text=Berbeda%20dengan%20mobile%20banking%20yang,diakses%20langsung%20melalui%20browser%20kamu.

[15] Rohman, A.F., et.al. 2020 December 20. Analisis Manajemen Risiko IT dan Keamanan Aset Menggunakan Metode Octave-S (Surabaya, Indonesia December 2020). 298 – 310. DOI = https://doi.org/https://doi.org/10.31539/intecoms.v3i2.1854

[16] Syahputri, H.Y. 2020 September 2020. Enterprise Risk Management Analysis of Group XYZ Based on ISO31000:2018 Framework (Bandung, Indonesia September 30 2020). 1 - 12. DOI= https://doi.org/https://doi.org/10.31521/1854

[17] Williams, J. 2016. OWASP Risk Rating Methodology. URI= https://owasp.org/www-community/OWASP_Risk_Rating_Methodology