JELASKAN BAGAIMANA KONSEP IT RISK MANAGEMENT PADA ITSM

BERIKAN CONTOH KASUS (JURNAL)

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

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

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

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

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

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

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

## I. PENDAHULUAN

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

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

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

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

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

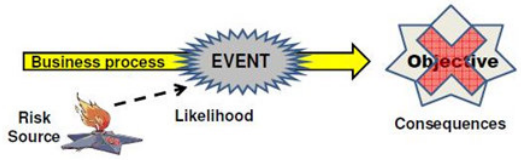
## II. METODE

### A. *Enterprise Risk Management (ERM)*

**Konsep Manajemen Risiko**

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

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




Gambar 1. Definisi Risiko[1]

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

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

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

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

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

**Konsep ERM**

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

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

***ISO 31000 Risk Management-Principle and Guidelines***

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

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

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

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

**Prinsip Manajemen Risiko**

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

***Framework* Manajemen Risiko**

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

Gambar 2. Komponen *framework* Manajemen Risiko

a. Mandat dan komitmen

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

b. Perencanaan *framework* manajemen risiko

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

c. Penerapan *framework* manajemen risiko

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

d. *Monitoring* dan *review*

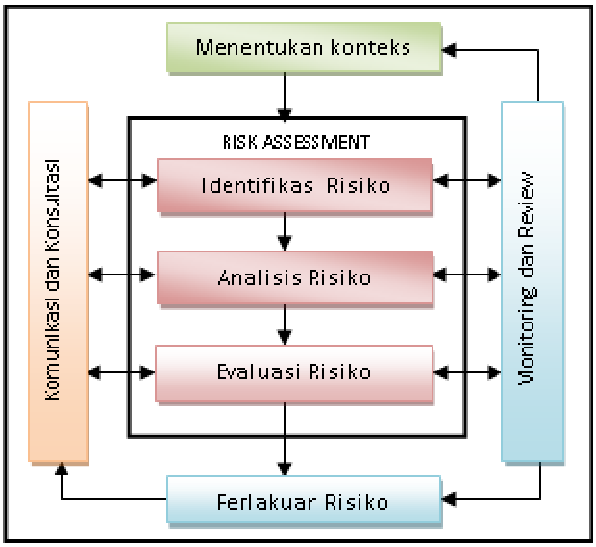
Menetapkan ukuran kinerja, meninjau secara berkala *framework* manajemen risiko, kebijakan risiko dan rencana penerapan risiko tetap sesuai dengan konteks internal dan eksternal organisasi.

e. Perbaikan kerangka kerja secara berkelanjutan.

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

**Proses Manajemen Risiko** (*Risk Management Process)*

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




Gambar 3. Proses Manajemen Risiko[1]

a. **Komunikasi dan konsultasi**

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

b. **Menetapkan konteks**

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

1) Menentukan Konteks Eksternal

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

2) Menentukan Konteks Internal

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

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

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

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

c. **Assessment Risiko**

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

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

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

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

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

## III. STUDI KASUS: PEMBOBOLAN ATM BCA

**Studi Kasus *event***

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

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

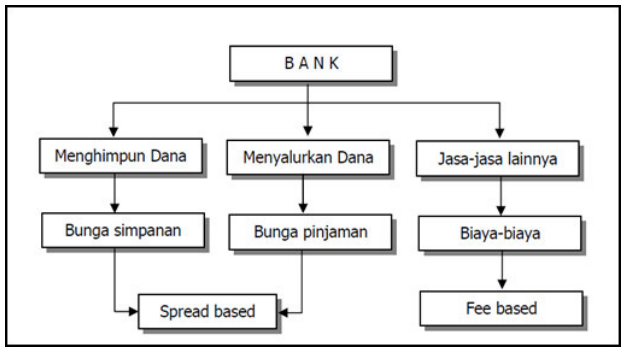
Sebagai Antisipasi, BCA menerapkan beberapa tindakan yaitu : 1) Memasang *anti-skiming,* penutup pin, dan kamera CCTV di bilik ATM, 2) Menganjurkan nasabah untuk mengganti PIN[a].

Rumusan Kasus :

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

**Unit Analisis**

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



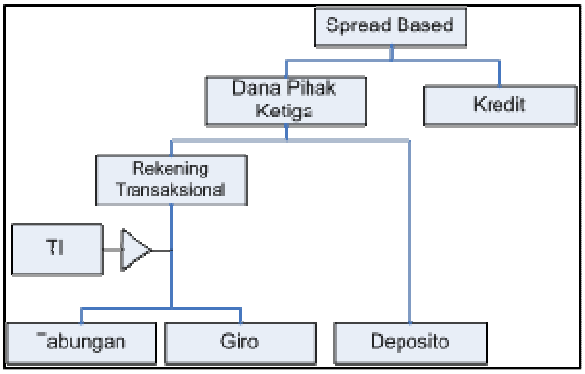

Gambar 4. Model Bisnis Bank[8]

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

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

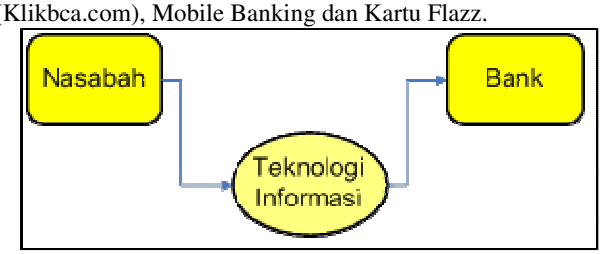
**Tujuan Penggunaan IT di BCA**

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




Gambar 5. TI dalam Strategi BCA

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




Gambar 6. Diagram Posisi TI dalam Strategi BCA

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

TABEL 1. JUMLAH JARINGAN LAYANAN (UNIT)

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

TABEL 2. JUMLAH TRANSAKSI MELALUI DELIVERY CHANEL

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

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

**Manajemen Risiko di BCA**

**Struktur Manajemen Risiko**

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

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

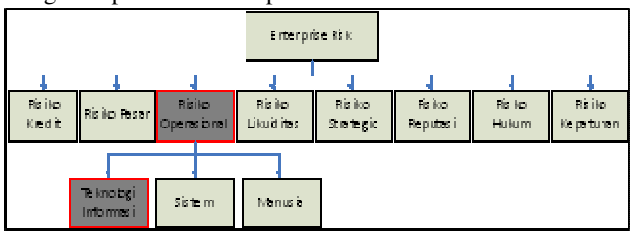
Bank juga memiliki Komite Manajemen Risiko yang berfungsi memberikan rekomendasi kebijakan dan membahas seluruh aspek risiko yang dihadapi Bank. Selain itu, Direksi telah membentuk komite-komite khusus yang bertugas untuk menangani risiko yang lebih spesifik, yaitu Komite Kebijakan Perkreditan, Komite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

**Kategori Risiko**

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

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

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




Gambar 7. Kategori Risiko BCA

## IV. HASIL ANALISIS

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

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

A. ***Menentukan Konteks***

**Konteks Internal**

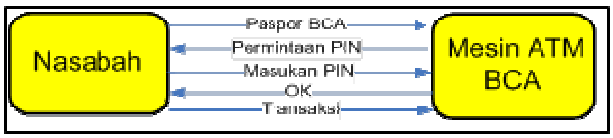
Dalam *Risk Event* Pembobolan ATM, Kategori Risiko yang terpengaruh adalah Risiko Operasional Teknologi Informasi dalam hal ini alat teknologi informasi ATM. Selain Risiko Operasional, Pembobolan ATM ini juga mengancam Kategori yang lain yaitu Risiko Reputasi, karena dapat mengakibatkan ketidakpercayaan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

**Proses Bisnis**

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

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

Gambar 8. Prosedur Permohonan Paspor BCA




Gambar 9. Prosedur Penggunaan Mesin ATM BCA

**Keamanan Transaksi**

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

**Kriteria Risiko**

**Kriteria Kemungkinan(*likelihood*)**

Dalam membentuk Kriteria kemungkinan, penulis menggunakan table Matrik probabilitas.

TABEL 3. MATRIKS PROBABILITAS[1]

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

**Kriteria Dampak(*consequence*)**

Dalam membentuk Kriteria Dampak, penulis menggunakan table Matrik Dampak.

TABEL 4. MATRIKS DAMPAK[1]

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

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

**Kriteria Pemeringkat Risiko(*Risk Level)***

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

TABEL 5 PENENTUAN PERINGKAT RISIKO[1]

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

## B. *Assesment Risiko*

### 1) *Identifikasi Risiko*

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

Nama Risiko : Pembobolan ATM

Uraian Risiko

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

Perkiraan Sumber Risiko

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

Uraian Dampak Risiko

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

Uraian Kemungkinan terjadinya Risiko

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

Status Risiko

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

### 2) *Analisis Risiko*

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

**Analisis Peluang**

Kriteria Kemungkinan:

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

Kriteria Dampak:

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

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

**Metode Sebab-Akibat**

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

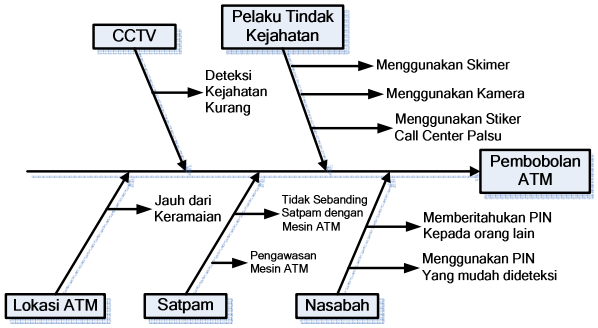
Langkah 1: Membuat Daftar Tanya Jawab Analisis Sebab-Akibat

TABEL 6. DAFTAR TANYA JAWAB ANALISIS SEBAB-AKIBAT

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

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

Langkah 2. Membuat Diagram Ishikawa




Gambar 10. Diagram Ishikawa untuk Risiko Pembobolan ATM

Langkah 3: Melakukan Analisis

Penyebab Dasar dari Risiko Pembobolan ATM.

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

*3) Evaluasi Risiko*

**Langkah BCA**

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

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

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

## C. *Perlakuan Risiko*

**Perlakuan Risiko oleh BCA**

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

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

**Analisis**

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

## V. KESIMPULAN

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

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

## DAFTAR PUSTAKA


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

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

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

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

**Online:**

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

Nama : Dhea Noranita Putri Tugas : ITSM

Nim : 182420112

---

**Soal :**

1. JELASKAN BAGAIMANA KONSEP IT RISK MANAGEMENT PADA ITSM BERIKAN CONTOH KASUS (JURNAL)

**Jawab :**

IT Risk Management didefinisikan sebagai proses mengidentifikasi, memantau dan mengelola risiko potensial untuk meminimalkan dampak negatif yang mungkin ditimbulkannya terhadap suatu organisasi. Setiap bidang dalam bisnis memiliki risikonya tersendiri. Contohnya di bidang sistem informasi, risiko potensialnya adalah seperti terjadinya pelanggaran keamanan data, kehilangan data, serangan dunia maya, kegagalan sistem, dan bencana alam. Sedangkan potensi risiko yang akan terjadi di perusahaan Manufaktur adalah gagal mencapai target produksi yang direncanakan, kerusakan mesin, hilangnya pesanan dari pelanggan, terjadinya masalah kualitas produk dan lain sebagainya. Proses manajemen risiko yang efektif akan membantu mengidentifikasi risiko mana yang menjadi ancaman terbesar bagi organisasi dan memberikan panduan untuk menanganinya.

**Proses Managemen Resiko IT**

1. Mengidentifikasi Resiko
   Perusahaan mengungkap, mengenali dan menggambarkan resiko yang mungkin mempengaruhi proyek.
2. Menganalisis Resiko
   Ketika resiko sudah di - identifikasi, perusahaan menentukan kemungkinan dan konsekuensi dari setiap resiko yang ada. Perusahaan lalu mengembangkan sebuah pemahaman tentang sifat resiko dan potensi untuk mempengaruhi tujuan dan sasaran proyek .
3. Mengevaluasi Resiko
   Perusahaan mengevalusi resiko dengan menentukan besarnya resiko, yang merupakan kombinasi dari kemungkinan dan konsekuensi. Lalu Perusahaan membuat keputusan apakah resiko itu diterima atau tidak.
4. Memantau dan Mempertimbangkan Resiko

Ini adalah tahap dimana perusahaan memantau setiap resiko yang ada untuk menghindari resiko yang lebih besar.

**Fungsi Manajemen Resiko IT**

1. Memberikan panduan untuk membantu para eksekutif dan manajemen mengajukan pertanyaan kunci, membuat lebih baik, keputusan risiko-disesuaikan lebih banyak informasi dan membimbing perusahaan mereka sehingga risiko dikelola secara efektif
2. Membantu menghemat waktu, biaya dan tenaga dengan alat untuk mengatasi risiko bisnis
3. Mengintegrasikan manajemen TI terkait risiko bisnis menjadi manajemen risiko perusahaan secara keseluruhan
4. Membantu kepemimpinan memahami risiko perusahaan dan toleransi risiko
5. Memberikan panduan praktis didorong oleh kebutuhan kepemimpinan perusahaan di seluruh dunia

**Contoh Kasus (Jurnal):**

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

**Penulis :** Anthon R. Tampubolon dan Suhardi, Sekolah Teknik Elektro dan Informatika Institut Teknologi Bandung Jalan Ganesha 10 Bandung

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

Nama : Caesario Rian Saputra

Nim : 182420131

# RISK MANAGEMENT

## IT Risk Management

Risk Management (Manajemen Resiko) merupakan suatu proses mengidentifikasi resiko, menilai resiko, dan mengambil langkah meminimalisir resiko untuk mengontrol dan menjamin resiko tetap pada level yang dapat diterima. IT Risk Management mencoba untuk melindungi *confidentiality*, *integrity*, dan *availability* (CIA). Yaitu dengan meminimalisir dampak yang mungkin muncul yang dapat berefek pada *confidentiality* dari informasi, *integrity* dari data pada sistem, dan *availability* dari infrastruktur sistem.

## fokus Utama IT Risk Management

Alasan utama mengapa suatu organisasi perlu untuk menerapkan proses manajemen resiko adalah untuk mendukung misi organisasi dan melindungi aset dari organisasi tersebut. Pada IT Risk Management, erat kaitannya dengan bagaimana implementasi security pada suatu organisasi sehingga diperlukan pemahaman tentang proses bisnis organisasi dan kemungkinan resiko yang berdampak pada proses bisnis tersebut. Risk Management akan sangat membantu manajemen organisasi untuk menyeimbangkan antara dampak dari *risk* dan *cost* yang dibutuhkan untuk meminimalisir resiko tersebut.

Ketika membahas tentang Risk Management, kita tentu berbicara tentang sebuah kemungkinan yang tidak tentu (*uncertainty*). Kita bisa ambil contoh kasus pada sebuah server website. Sebuah server yang belum dipatch dan belum diproteksi pada network, tentu berpotensi untuk *compromised*. Jika itu mungkin tidak terjadi hari ini atau mungkin tidak terjadi besok, tapi kita tahu kemungkinan tersebut pasti ada dan dapat terjadi. Maka dari itu pemahaman kita tentang adanya *threat* dan *vulnerability*, sebarapa bahayanya, dan seberapa efektif langkah yang digunakan untuk mengamankannya, harus ditentukan ketika melakukan *assessment* terhadap kemungkinan *threat* dan *vulnerability* tersebut.

## Step-by-step IT Risk Management

Proses dari manajemen risiko berfungsi membantu dalam melakukan pengambilan keputusan yang lebih baik dan meningkatkan efisiensi. Meskipun banyak cara dalam menggambarkan proses manajemen risiko, langkah-langkah dasar yang terdapat dalam proses ini hampir serupa dan biasanya mencakup tiga langkah utama yaitu: risk identification, risk assessment, dan risk treatment

1. Risk Identification

Risk identification merupakan proses dalam menentukan apa, bagaimana, dan mengapa suatu kondisi atau kejadian dapat terjadi. Proses identifikasi risiko harus dilakukan secara komprehensif, harus terstruktur berdasarkan faktor-faktor utama agar nantinya risiko dapat dinilai secara sistematis [4]. Risiko dapat diidentifikasi melalui beberapa metode seperti; checklist, interview atau focused group discussion dan questionnaries. Checklist digunakan untuk menyederhanakan proses identtifikasi risiko. Checklist juga dirancang untuk

menghindari atau meminimalkan risiko, seringkali checklist merupakan bagian dari prosedur dokumentasi dan jaminan kualitas organisasi. Questionnaries atau kuesioner merupakan instrumen penelitian yang terdiri dari serangkaian pertanyaan dan petunjuk lainnya dengan tujuan untuk mengumpulkan informasi tertentu dari responden.

2. Risk Assesment

Risk assesment merupakan keseluruhan proses dari risk analysis dan risk evaluation. Risk analysis adalah proses sistematis dalam menggunakan informasi yang ada untuk menentukan seberapa sering risiko dapat terjadi dan seberapa besar dampak yang dihasilkan bila risiko tersebut terjadi

3. Risk Treatment

Risk treatment bertujuan untuk menentukan tindakan yang dilakukan dalam mengatasi risiko yang telah teridentifikasi, guna mengurangi pengaruh risiko secara keseluruhan . Risk treatment merubah analisis sebelumnya, risk identification dan risk assessment, menjadi tindakan substantif untuk mengurangi risiko.

**Contoh kasus jurnal :**

Analisis Manajemen Resiko Teknologi Informasi Penerapan Pada *Document Management System* di PT. Jabar Telematika (JATEL)

**A. Risk Identification**

Pada proses identifikasi risiko dilakukan pengelompokan risiko berdasarkan sumber daya TI, yang didefinisikan oleh COBIT, yang berhubungan dengan document management system arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL.

Identifikasi yang dilakukan menghasilkan beberapa risiko yang mungkin terjadi pada setiap sumber daya TI yang dimiliki oleh PT. Jabar Telematika (JATEL) antara lain:

1. Application

- External Attacks
- Malicious Code
- Network Congestion
- System Crash

2. Information

- Database Failure
- Data/Document Fraud

3. Infrastructure

- Physical Damage

- Hardware Failure

- Power Outages

- Force Majure

4.People

- Inappropriate Access

- Abuse of Position of Trus

- Disgruntled Employees

**B. Risk Assessment**

Pada proses ini dilakukan penilaian terhadap risiko yang terjadi document management system arsip elektronikADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL. Penilaian terhadap risiko merupakan gabungan proses yang terdiri dari risk analysis (analisis risiko) dan risk evaluation (evaluasi risiko). Penilaian risiko terhadap risiko yang terjadi pada document management system arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL dilakukan untuk mengevaluasi dan mengestimasi level of risk (tingkatan risiko) dari masing-masing risiko yang telah diidentifikasi pada proses identifikasi risiko dan menetapkan acceptable level of risk (tingkatan risiko yang dapat diterima) organisasi.

Risk Analysis

Analisis risiko dilakukan untuk menentukan seberapa sering risiko pada document management system arsipelektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL dapat terjadi dan seberapa besar dampak yang dihasilkan apabila risiko tersebut terjadi. o Bow-tie Analysis Bow-tie Analysis dilakukan agar proses analisis terhadap risiko menghasilkan recovery (pemulihan) dan control (kontrol).

**C. Risk Treatment**

Pada tahap ini dapat dilihat tindakan yang dilakukan oleh PT. Jabar Telematika (JATEL) dalam mengatasi risiko yang telah teridentifikasi pada aplikasi document management system arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) dan memiliki medium level of risk. Pada tahap ini juga ditentukan usulan strategi perlakuan risiko yang tepat dalam mengatasi permasalahan yang sesuai dengan pembahasan ini yaitu dengan risk prevention (pencegahan risiko).

**NAMA** **: DINI RAHMADIA**

**NIM** **: 182420134**

**KELAS** **: MTI REG B**

SOAL

JELASKAN BAGAIMANA KONSEP IT RISK MANAGEMENT PADA ITSM

BERIKAN CONTOH KASUS (JURNAL)

JAWABAN:

*IT Risk Management* (Manajemen Resiko Teknologi Informasi) adalah suatu proses identifikasi kerentanan dan ancaman terhadap sumber daya informasi yang digunakan oleh sebuah organisasi dan dilakukan oleh manajer IT untuk mencapai tujuan bisnis,mengurangi resiko, dan menyeimbangkan pengeluaran dalam mencapai keuntungan dan melindungi IT.

Ada dua hal didalam definisi ini yang mungkin membutuhkan penjelasan. Pertama, proses manajemen resiko yang merupakan proses berulang yang berlangsung. Ini adalah proses yang yang harus diulang tanpa batas, disebabkan lingkungan bisnis yang fleksibel atau terus berubah yang menyebabkan munculnya ancaman baru. Kedua, pilihan penanggulangan (kontrol)yang digunakan untuk mengelola resiko harus menjaga keseimbangan antara produktivitas, biaya, efektivitas penanggulangan, dan nilai aset informasi yang harus dilindungi.

**Konsep dan prosesManagemen Resiko IT**

- Mengidentifikasi Resiko. Perusahaan mengungkap, mengenali dan menggambarkan resiko yang mungkin mempengaruhi proyek.
- Menganalisis Resiko. Ketika resiko sudah di - identifikasi, perusahaan menentukan kemungkinan dan konsekuensi dari setiap resiko yang ada. Perusahaan lalu mengembangkan sebuah pemahaman tentang sifat resiko dan potensi untuk mempengaruhi tujuan dan sasaran proyek .

- Mengevaluasi Resiko. Perusahaan mengevalusi resiko dengan menentukan besarnya resiko, yang merupakan kombinasi dari kemungkinan dan konsekuensi. Lalu Perusahaan membuat keputusan apakah resiko itu diterima atau tidak.
- Memantau dan Mempertimbangkan Resiko. Ini adalah tahap dimana perusahaan memantau setiap resiko yang ada untuk menghindari resiko yang lebih besar.

**Fungsi Manajemen Resiko IT**

1. Memberikan panduan untuk membantu para eksekutif dan manajemen mengajukan pertanyaan kunci, membuat lebih baik, keputusan risiko-disesuaikan lebih banyak informasi dan membimbing perusahaan mereka sehingga risiko dikelola secara efektif
2. Membantu menghemat waktu, biaya dan tenaga dengan alat untuk mengatasi risiko bisnis
3. Mengintegrasikan manajemen TI terkait risiko bisnis menjadi manajemen risiko perusahaan secara keseluruhan
4. Membantu kepemimpinan memahami risiko perusahaan dan toleransi risiko
5. Memberikan panduan praktis didorong oleh kebutuhan kepemimpinan perusahaan di seluruh dunia

ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/319392414

# Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Petrokimia Gresik)

**Article** · January 2018

CITATION
1

READS
3,976

**2 authors**, including:

Suprapto Suprapto
Brawijaya University
**4** PUBLICATIONS **4** CITATIONS

SEE PROFILE

All content following this page was uploaded by Suprapto Suprapto on 31 August 2017.

The user has requested enhancement of the downloaded file.

**Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer** e-ISSN: 2548-964X
Vol. 1, No. 1, Juni 2017, hlm. x-x http://j-ptiik.ub.ac.id

# Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Petrokimia Gresik)

**Nurfitri Zukhrufatul Firdaus[1], Suprapto[2]**

Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]fitri.firdaus0@gmail.com, [2]praptomlg@yahoo.com

**Abstrak**

SAP (*System Application and Product in Data Processing*) merupakan jenis software ERP yang digunakan oleh PT. Petrokimia Gresik untuk menunjang otomatisasi proses bisnis perusahaan dan mendukung proses pengambilan keputusan agar lebih efektif dan efisien. Untuk mengantisipasi timbulnya risiko yang dapat mengganggu jalannya proses bisnis perusahaan, PT. Petrokimia Gresik menerapkan manajemen risiko berdasarkan standart ISO 31000:2009. Dalam hal ini perlu dilakukan evaluasi untuk mnegetahui pencapaian penerapan manajemen risiko teknologi informasi pada PT. Petrokimia Gresik dengan menggunakan kerangka kerja COBIT 5 khususnya pada domain proses APO12 (Risk Management) dan EDM03 (Ensure Risk Optimation). Untuk memperoleh data yang akurat, maka teknik pengumpulan data yang digunakan adalah dengan melakukan penyebaran kuesioner, obeservasi langsung dan wawancara dengan pihak yang berwenang. Proses evaluasi tersebut terdiri dari beberapa tahapan, antara lain melakukan analisis *capability level*, analisis *gap* dan analisis *risk assessment* untuk mengidentifikasi risiko – risiko potensial serta menilai sejauh mana dampak yang dapat ditimbulkan. Berdasarkan hasil analisis tersebut, maka didapatkan nilai *capability level* untuk domain proses EDM03 berada pada level 2 dan domain proses APO12 berada pada level 3 serta menghasilkan 16 buah strategi mitigasi dan 9 buah rekomendasi yang dapat digunakan untuk membantu perbaikan penerapan manajemen risiko teknologi informasi di PT. Petrokimia Gresik.

**Kata kunci**: *COBIT 5, capability level, manajemen risiko, analisis gap, risk assessment, mitigasi risiko*

**Abstract**

*SAP (System Application and Product in Data Processing) is a type of ERP Software that used by PT. Petrokimia Gresik to support business process automation and support decision-making process to be more effective and efficient. To anticipate the potential problems that might obstruct business processes at the company, so PT. Petrokimia Gresik managed to use risk management based on the standards of ISO 31000:2009. An evaluation on the implementation of IT risk management was done to measure its capability level accomplishment. COBIT 5 Framework, especially in process domain APO12 (Risk Management) dan EDM03 (Ensure Risk Optimation), was used as the basis of the evaluation. To collect accurate data, the data were obtained by distributing questionnaire, conducting a direct observation and an interview to the people in charge. The process of evaluating the implementation of IT risk management consists of several stages, including capability level analysis, gap analysis and risk assessment analysis to identify potential risks and assess the extent of the impacts of each risk. From the evaluation result, it turned out that capability level for process domain EDM03 was on level 2 and on level 3 for process domain APO12 and 16 mitigation strategy and 9 recommendation were made to support the improvement for the implementation of risk management information and technology at PT. Petrokimia Gresik.*

**Keywords**: *COBIT 5, capability level, risk management, gap analysis, risk assessment, risk mitigation*

## 1. PENDAHULUAN

Salah satu perusahaan yang telah memanfaatkan teknologi informasi dan menerapkan manajemen risiko teknologi informasi sebagai sarana pendukung untuk mencapai tujuan perusahaan adalah PT. Petrokimia Gresik. Untuk meningkatkan kualitas perusahaan dibidang teknologi

informasi, PT. Petrokimia Gresik menerapkan sistem ERP – SAP yang terdiri dari sepuluh modul. Disamping itu PT. Petrokimia Gresik juga menerapkan beberapa aplikasi Non ERP untuk menunjang jalannya Sistem ERP-SAP. Dengan diterapkannya Sistem tersebut diharapkan mampu menunjang otomatisasi proses bisnis perusahaan dan mendukung proses pengambilan keputusan secara efektif dan efisien. Namun pada kenyatannya, penerapan Teknologi Informasi (TI) pada perusahaan tidak selalu berjalan sesuai dengan yang diharapkan, sehingga menimbulkan risiko – risiko yang dapat merugikan perusahaan. Oleh karena itu untuk mengelola segala macam risiko yang dapat mengganggu jalannya proses bisnis dan menimbulkan kerugian, maka PT. Petrokimia Gresik telah menerapkan manajemen risiko berdasarkan pada Standart ISO 31000 : 2009 sejak tahun 2003.

Padatnya proses bisnis yang berjalan di PT. Petrokimia Gresik, mengakibatkan risiko – risiko yang terjadi menjadi sangat kritis dan fatal. Risiko – risiko tersebut diantaranya berupa gangguan jaringan internet, gangguan arus listrik, kurang optimalnya dukungan teknis operasional ERP, gangguan komunikasi data antara user dengan server ERP dan lain sebagainya. Oleh karena itu perlu adanya evaluasi manajemen risiko Teknologi Informasi (TI) untuk mengetahui tingkat kapabilitas yang telah dicapai sehingga dapat meningkatkan kemampuan perusahaan dalam menerapkan manajemen risiko Teknologi Informasi (TI). Dari evaluasi tersebut menghasilkan rekomendasi berupa saran maupun usulan yang dapat digunakan oleh perusahaan untuk meminimalisir terjadinya risiko – risiko yang tidak diinginkan. Salah satu *framework* yang dapat digunakan untuk mengevaluasi manajemen risiko Teknologi Informasi (TI) pada PT. Petrokimia Gresik adalah COBIT 5 khususnya pada domain proses APO12 (*Manage Risk*) dan EDM03 (*Ensure Risk Optimisatin*). Digunakannya domain tersebut karena dalam COBIT 5, hanya ada dua domain yang membahas secara terperinci mengenai manajemen risiko Teknologi Informasi (TI).

## 2. LANDASAN KEPUSTAKAAN

### 2.1 Kajian Pustaka

Adapun penelitian – penelitian terdahulu yang relevan dengan penelitian ini adalah sebagai berikut :

1. Penelitian yang dilakukan oleh Astri Dyahaloka yang berjudul "Evaluasi Manajemen Risikio *E-Procurement* Menggunakan COBIT 5 *IT Risk* (Studi Kasus : PT. Pertamina (Persero))". Penelitian tersebut menggunakan kerangka kerja COBIT 5 dengan domain EDM03 dan APO12. Dalam melakukan evaluasi, penelitian tersebut menggunakan analisis *capability level*, analisis *gap* dan analisis SWOT, sehingga menghasilkan nilai *capability level* yang telah dicapai dan rekomendasi untuk perbaikan penerapan manajemen risiko.
2. Penelitian yang dilakukan oleh Diaz Mahardika yang berjudul "Pengukuran Tingkat Kapabilitas Proses Pengelolaan Risiko Teknologi Informasi Pada Direktorat Sistem Informasi Universitas Airlangga Berdasarkan Cobit 5 Proses APO12 *Manage Risk".* Penelitian tersebut menggunakan kerangka kerja COBIT 5 dengan domain APO12. Dalam melakukan evaluasi, penelitian tersebut menggunakan analisis *capability level* dan analisis *capability level* dan analisis *management awareness*, sehingga menghasilkan nilai *capability level* yang telah dicapai dan usulan model tata kelola TI.

### 2.2 Manajemen Risiko

Manajemen risiko merupakan proses menjalankan aktivitas manajemen untuk menanggulangi munculnya risiko, baik yang dihadapi perusahaan maupun yang dihadapi oleh masyarakat. Sehingga dapat disimpulkan bahwa fungsi – fungsi manajemen yang dijalankan untuk menanggulangi risiko mencakup proses pengelolaan, pengukuran dan penilaian risiko. Dalam hal ini manajemen risiko dimaksudkan untuk mengurangi dampak negatif dari suatu risiko, menghindari terjadinya risiko, menampung sebagian atau keseluruhan dari konsekuensi risiko atau mengalihkan risiko kepada pihak lain.

### 2.3 COBIT 5

C*ontrol Objective for Information and Related Technology* (COBIT) merupakan seperangkat pedoman dan hasil dokumentasi yang berfungsi untuk membantu auditor, pemangku kepentingan atau pengguna (*user*) dalam menghubungkan antara model kendali bisnis dan model kendali TI. COBIT

dikembangkan untuk menerapkan *Governance of Enterprise IT*. Versi terbaru yang dikeluarkan oleh *IT Governance Institute* dikenal sebagai COBIT 5. COBIT 5 terbentuk dengan mengintegrasikan Risk IT *framework*, VAL IT 2.0 dan COBIT 4.1. Selain itu COBIT 5 juga menyesuaikan antara *best practices* yang ada seperti ITIL V3, TOGAF dan standart relevan dari ISO.

ISACA (2012) menjelaskan bahwa terdapat tujuh buah tahapan yang harus dilakukan menurut siklus implementasi COBIT 5, antara lain :

a. *Initiate Programme*, yaitu proses identifikasi pemicu perubahan seperti kondisi trend, kinerja, implementasi perangkat lunak, isu penting dan tujuan organisasi yang mampu memberikan dorongan untuk berubah.
b. *Define Problems and Opportunities*, yaitu proses penyelarasan antara tujuan penerapan TI dengan risiko maupun strategi organisasi, serta mengutamakan tujuan penerapan TI, tujuan organisasi dan proses penerapan TI yang paling utama.
c. *Define Road Map*, yaitu proses penetapan target untuk meningkatkan upaya perbaikan dan diikuti dengan analisis *gap* untuk menentukan beberapa solusi potensial.
d. *Plan Programme*, yaitu proses perencanaan solusi yang dianggap layak untuk dijalankan.
e. *Execute Plan*, yaitu proses penerapan solusi yang telah disarankan ke dalam aktivitas keseharian serta melakukan pemantauan untuk memastikan bahwa keselarasan bisnis dapat dicapai dan kinerja dapat diukur.
f. *Realise Benefits*, yaitu proses transisi secara berkelanjutan dengan menerapkan praktik tata kelola atau manajemen yang telah ditingkatkan ke dalam proses bisnis dan memantau perkembangannya dengan memetakannya pada matriks berdasarkan kinerja dan manfaat yang ingin diperoleh.
g. *Review Effectiveness*, yaitu proses evaluasi keberhasilan yang telah dicapai secara umum, kemudian melakukan identifikasi segala kebutuhan perbaikan secara berkala untuk lebih meningkatkan praktik tata kelola atau manajemen.

## 2.4 Fokus Area Manajemen Risiko

Menurut ISACA (2012), terdapat dua proses untuk manajemen risiko dari COBIT 5 antara lain :

1. EDM03 : *Ensure Risk Optimisation*
   Proses EDM03 bertujuan untuk memastikan apakah tingkat risiko dan besarnya toleransi yang dapat diterima oleh perusahaan telah dimengerti, diartikulasikan dan dikomunikasikan dengan baik, serta memastikan apakah risiko – risiko yang terkait dengan Teknologi Informasi (TI) telah diidentifikasi dan dikelola dengan baik. Proses EDM03 terbagi menjadi 3 atribut, yaitu antara lain :
   a. EDM03.01 : *Evaluate Risk Management*
   b. EDM03.02 : *Direct Risk Management*
   c. EDM03.03 : *Monitor Risk Management*
2. APO12 : *Manage Risk*
   Proses APO12 bertujuan untuk mengidentifikasi, menilai dan mengurangi risiko terkait dengan teknologi Informasi (TI) agar tidak melebihi batas toleransi yang telah ditentukan oleh manajemen eksekutif organisasi. Selain itu proses APO12 juga bertujuan untuk mengintegrasikan manajamen risiko Teknologi Informasi (TI) dengan manajemen risiko perusahaan (ERM). Proses APO12 terbagi menjadi enam subdomain, yaitu antara lain :
   a. APO12.01 : *Collect Data*
   b. APO12.02 : *Analyse Risk*
   c. APO12.03 : *Maintain A Risk Profile*
   d. APO12.04 : *Articulate Risk*
   e. APO12.05 : *Define a Risk Management Action Portofolio*
   f. APO12.06 : *Respond to Risk*

## 2.5 *Risk Assessment*

ISACA (2012) menjelaskan bahwa Secara umum Risk Assessment berfungsi untuk mengidentifikasi risiko potensial baik yang berasal dari internal maupun eksternal organisasi, selain itu juga menilai sejauh mana dampak yang ditimbulkan oleh risiko tersebut dapat mengganggu jalannya proses bisnis dan tujuan organisasi. Besarnya dampak dapat diukur melalui penilaian Inherent Risk dan Residual Risk, serta dianalisis melalui dua perspektif antara lain *Probability/Likelihood* dan *Impact/Consequence*.

## 2.6 *Risk Response*

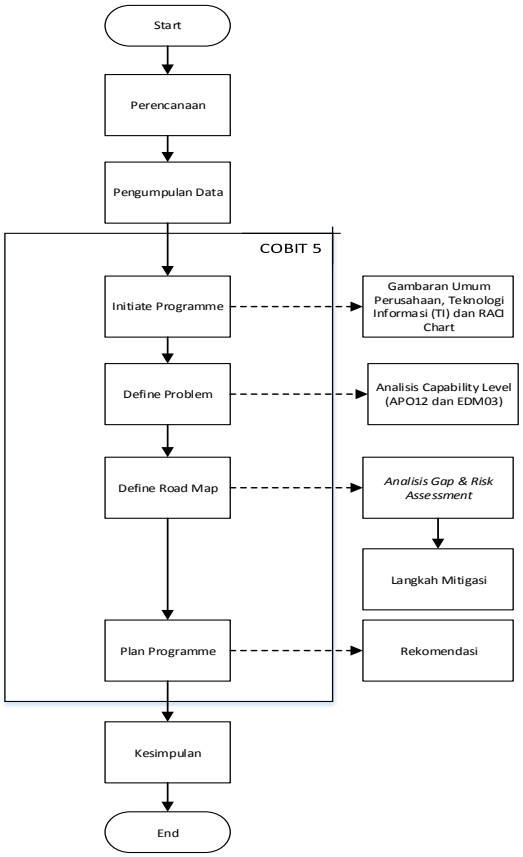
ISACA (2012) menjelaskan bahwa *Risk Response* atau Respon Risiko berfungsi untuk menyelaraskan antara risiko yang ditemukan dengan batas toleransi risiko yang telah ditentukan oleh organisasi. Dalam penelitian

ini, langkah yang diambil untuk merespon risiko adalah dengan melakukan *Risk Reduction* atau *Mitigation*, yaitu salah satu metode yang dilakukan dengan cara mengurangi besarnya *Probability* atau *Likelihood* (Peluang atau kecenderungan) dan *Impact* atau *Consequence* (Dampak) yang ditimbulkan dari risiko tersebut.

### 2.7 Sistem ERP – SAP

*System Application and Product in Data Processing* (SAP) merupakan *software* jenis *Enterprise Resources Planning* (ERP) yang dikembangkan untuk menunjang jalannya kegiatan operasional suatu organisasi agar lebih efektif dan efisien. Adapun modul – modul SAP yang diimplementasikan di PT. Petrokimia Gresik antara lain *Material Management (MM), Production Planning (PP), Plant Maintenance (PM), Sales Distribution (SD), Financial Accounting Controlling (FICO), Human Capital Management (HCM), Quality Management (QM), Fund Management (FM), Business Planning and Consolidation (BPC)* dan *Dashboard*.

## 3. METODOLOGI




Gambar 1 Diagram Alur Penelitian

1. Menentukan objek dan subjek penelitian, menentukan kerangka kerja yang tepat serta menggali informasi yang terkait**.**
2. Melakukan pengumpulan data, baik data primer maupun data sekunder dengan cara melakukan penyebaran kuesioner, melakukan observasi langsung, melakukan wawancara dengan pihak – pihak yang berwenang dan studi kepustakaan.
3. Mendeskripsikan gambaran umum mengenai kondisi umum organisasi, visi dan misi sebagai tujuan organisasi, gambaran umum sistem informasi atau teknologi informasi yang diterapkan dan pihak – pihak yang bertanggung jawab dalam penerapan manajemen risiko berdasarkan RACI *Chart*.
4. Melakukan analisis penilaian *Capability Level* berdasarkan kerangka kerja COBIT 5 khususnya domain proses EDM03 (*Ensure Risk Optimisation*) dan APO12 (*Manage Risk*).
5. Melakukan *Gap Analysis*, *Risk Assessment* dan menentukan langkah mitigasi untuk setiap risiko yang melebihi batas toleransi perusahaan berdasarkan data yang diperoleh dari hasil kuesioner, observasi dan wawancara.
6. Membuat rekomendasi untuk menentukan solusi potensial berdasarkan hasil analisis *Capability Level*, *Gap Analysis* dan *Risk Assessment*.
7. Menyusun kesimpulan yang berisi ringkasan tentang semua langkah - langkah yang telah dilalui dalam melakukan penelitian.

## 4. HASIL

### 4.1 Hasil Kuesioner

Berdasarkan hasil pembuatan RACI *Chart*, dapat diketahui bahwa pihak yang berhak menjadi responden untuk mengisi kuesioner adalah sejumlah tiga orang, antara lain Manager Dept. TEKINFO, Kabag. Infrastruktur TEKINFO dan Manager Dept. TKP & MR.

Tabel 1 Rekapitulasi Hasil Pengisian Kuesioner

| *Prosess Assesment Results* | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Nama Proses** | ***Proces Capability Level*** | | | | | | **Total Responden** |
| | **0** | **1** | **2** | **3** | **4** | **5** | |
| *Evaluate, Direct, and Monitoring* | | | | | | | |
| EDM03 | 0 | 0 | 3 | 0 | 0 | 0 | 3 |
| *Align, Plan, and Organise (APO)* | | | | | | | |
| APO12 | 0 | 0 | 0 | 3 | 0 | 0 | 3 |

. Dari Tabel 1 diatas, dapat diketahui bahwa hasil pengisian kuesioner yang dilakukan oleh tiga orang responden menunjukkan nilai *Capability Level* terkait proses EDM03 berada pada Level 2 dan nilai *Capability Level* terkait proses APO12 berada pada Level 3.

### 4.2 Hasil Observasi dan Wawancara

Dalam mengelola proses bisnis perusahaan, PT. Petrokimia Gresik telah mendukung penerapan sistem yang bernama ERP-SAP. Sistem tersebut diharapkan mampu mengintegrasikan seluruh proses bisnis yang ada pada perusahaan dan mensinergiskan proses bisnis dari masing – masing anggota Pupuk Indonesia *Holding Company* (PIHC). Dalam hal ini, pihak yang bertanggung jawab mendukung jalannya Sistem ERP-SAP, mengintegrasikan sistem atau aplikasi yang dibuat sendiri dengan Sistem ERP-SAP, serta meningkatkan kualitas SDM untuk mendukung penerapan Sistem ERP-SAP adalah Departemen TEKINFO.

Dalam penerapan Sistem ERP – SAP tersebut, tidak pernah lepas dari suatu risiko. Oleh karena itu untuk mengelola segala bentuk risiko perusahaan, Departemen TKP & MR telah menerapkan manajemen risiko berdasarkan standart dan kebijakan yang ditetapkan yaitu ISO 31000 : 2009. Standart dan kebijakan tersebut tertuang dalam dokumen Kebijakan Manajemen Risiko, Pedoman Penerapan Manajemen Risiko, Prosedeur Penerapan Manajeen Risiko, Panduan Penilaian Penerapan Manajemen Risiko dan Pedoman Manajemen Risiko PT. Pupuk Indonesia (Persero). Selama ini penerapan manajemen risiko pada PT. Petrokimia Gresik dimulai dengan melakukan identifikasi terhadap semua risiko yang muncul, menganalisis setiap risiko yang telah diidentifikasi, mengevaluasi setiap risiko, pengendalian dan penanganan risiko serta monitoring dan review terhadap pengendalian dan penanganan. Selanjutnya hasil dari aktivitas pengelolaan risiko tersebut disusun dalam sebuah dokumen yang bernama Profil Risiko PT. Petrokimia Gresik.

Dalam mengelola setiap risiko perusahaan, Departemen TKP & MR memiliki aplikasi yang bernama SIMAR (Sistem Informasi Manajemen Risiko) dan program kerja yang bernama Klinik Risiko. Dengan adanya aplikasi SIMAR dan program Klinik Risiko tersebut, dapat memudahkan Departemen TKP & MR dalam memantau penerapan manajemen risiko pada setiap unit kerja.

### 4.3 Hasil Temuan

Berdasarkan hasil analisis *capability level* yang diperoleh dari perhitungan hasil kuesioner dan proses wawancara dengan pihak Departemen TKP & MR dan Departemen TEKINFO PT. Petrokimia Gresik, didapatkan beberapa temuan berikut :

1. Adanya layanan Tata Kelola Perusahaan dan Manajemen Risiko pada PT. Petrokimia Gresik, namun belum adanya manajemen atau team yang dibentuk secara khusus untuk mengelola segala macam risiko terkait dengan teknologi informasi.
2. Pengelolaan risiko yang dilakukan oleh Departemen TKP & MR pada PT. Petrokimia Gresik masih secara umum yaitu dilakukan pada seluruh unit kerja perusahaan dan belum berfokus secara spesifik pada penerapan teknologi informasi.
3. Tidak semua risiko teknologi informasi telah didokumentasikan dan dikelola dengan baik.
4. Belum secara penuh memantau kesesuaian seluruh risiko yang dikelola dengan risk appetite.
5. Dalam melakukan analisis risiko tersebut, belum disertai dengan analisis *cost benefit* yaitu perkiraan frekuensi besarnya keuntungan dan kerugian yang berhubungan dengan penanganan setiap skenario risiko.

## 5 PEMBAHASAN

### 5.1 Analisis *Capability Level*

Berdasarkan hasil pengisian kuesioner yang dilakukan oleh 3 responden dari Departemen TKP & MR dan Departemen TEKINFO PT. Petrokimia Gresik dapat diketahui bahwa nilai *capability level* yang telah dicapai subdomain EDM03 berada pada Level 2 dan nilai *capability level* yang telah dicapai subdomain APO12 berada pada Level 3. Hal tersebut dapat dilihat pada Tabel 2 di bawah ini.

Tabel 2 Rekapitulasi Hasil Gap Analysis

| Nama Proses | Level Saat Ini | Level Target | *Gap* |
|---|---|---|---|
| EDM03 | 2 | 3 | 1 |
| APO12 | 3 | 4 | 1 |

### 5.2 Analisis *Gap*

Berdasarkan hasil wawancara, diperoleh informasi bahwa level target yang ingin dicapai oleh Departemen TKP & MR dan Departemen TEKINFO PT. Petrokimia Gresik adalah naik satu level untuk setiap domain prosesnya, yaitu domain proses EDM03 berada pada Level 3 dan domain proses APO12 berada pada Level 4. Sehingga besarnya *gap* yang terbentuk antara level yang terjadi saat ini dan level target yang ingin dicapai pada domain proses EDM03 dan APO12 adalah sebesar 1.

### 5.3 *Risk Assessment*

Proses *Risk Assessment* dilakukan berdasarkan dua tahapan, antara lain :

1. *Risk Analysis*

*Risk Analysis* bertujuan untuk menentukan seberapa sering risiko tersebut dapat terjadi dan seberapa besar dampak yang dihasilkan oleh risiko tersebut. *Risk Analysis* diawali dengan melakukan identifikasi risiko, menentukan parameter *probability*, menentukan parameter *impact*, menentukan parameter *rating* risiko, melakukan penilaian risiko terhadap *inherent risk* dan *residual risk*.

Adapun pengelompokan risiko berdasarkan skenario risiko dan aset dapat dilihat dalam Tabel 3 dan Tabel 4 berikut ini.

Tabel 3 Rekapitulasi Berdasarkan Skenario Risiko

| No | Skenario Risiko | Jumlah *Risk Issue* |
|---|---|---|
| 1 | New Technology | 1 |
| 2 | Software Implementation | 2 |
| 3 | Destruction of Infrastructure | 1 |
| 4 | IT Staff | 1 |
| 5 | IT Expertise and Skills | 2 |
| 6 | Software Integrity | 2 |
| 7 | Infrastructure (Hardware) | 3 |
| 8 | System Capacity | 2 |
| 9 | Malware | 1 |
| 10 | Logical Attacks | 1 |
| 11 | Utilities Performance | 1 |
| 12 | Data(base) Integrity | 2 |
| 13 | Logical Trespassing | 1 |
| 14 | Operational IT Errors | 2 |
| 15 | Acts of Nature | 1 |
| Total | | 23 |

Tabel 4 Rekapitulasi Berdasarkan Aset

| No | Kategori Aset | Jumlah *Risk Issue* | Persentase |
|---|---|---|---|
| 1 | Aplikasi | 5 | 21,74 % |
| 2 | Fasilitas | 1 | 4,35 % |
| 3 | Infrastruktur TI | 3 | 13,04 % |
| 4 | Informasi / Data | 7 | 30,43 % |
| 5 | Proses | 4 | 17,39 % |
| 6 | SDM | 3 | 13,04 % |
| Total | | 23 | 100 % |

Sebelum melakukan penilaian risiko terhadap *Inherent Risk* dan *Residual Risk*, terlebih dahulu menentukan standart penilaian berupa parameter *probability* (kecenderungan), parameter *impact* (dampak) dan parameter *Rating* Risiko. Dari hasil rekapitulasi risiko berdasarkan aset dan skenario risiko serta mempertimbangkan parameter *probability* dan *impact* yang telah dibuat, maka dapat diketahui kategori risiko dasar (*Inherent Risk*). *Inherent Risk* merupakan risiko yang dinilai tanpa memasukkan unsur pengendalian yang telah diterapkan. Adapun rekapitulasi hasil penilaian risiko terhadap *Inherent Risk* yang disusun berdasarkan aset dapat dilihat pada Tabel 5 berikut ini.

Tabel 5 Penilaian Inherent Risk Berdasarkan Aset

| No | Kategori Aset | Nilai Risiko Dasar | | | | |
|---|---|---|---|---|---|---|
| | | Rendah | Rendah Menengah | Menengah | Menengah Tinggi | Tinggi |
| 1 | Aplikasi | 0 | 0 | 4 | 0 | 1 |
| 2 | Fasilitas | 0 | 0 | 1 | 0 | 0 |
| 3 | Infrastruktur TI | 0 | 1 | 2 | 0 | 0 |
| 4 | Informasi / Data | 0 | 0 | 5 | 2 | 0 |
| 5 | Proses | 0 | 0 | 4 | 0 | 0 |
| 6 | SDM | 0 | 0 | 2 | 1 | 0 |
| Total | | 0 | 1 | 18 | 3 | 1 |

Berdasarkan hasil wawancara dengan beberapa perwakilan dari Dept. TEKINFO dan Dept. TKP & MR, dapat diketahui bahwa setiap risiko – risiko yang teridentifikasi telah memiliki pengendalian tersendiri. Pengendalian tersebut digunakan sebagai dasar untuk melakukan penilaian Residual Risk. Adapun rekapitulasi hasil penilaian risiko terhadap *Residual Risk* yang disusun berdasarkan aset dapat dilihat pada Tabel 6 berikut ini.

Tabel 6 Penilaian Residual Risk Berdasarkan Aset

| No | Kategori Aset | Nilai Risiko Dasar | | | | |
|---|---|---|---|---|---|---|
| | | Rendah | Rendah Menengah | Menengah | Menengah Tinggi | Tinggi |
| 1 | Aplikasi | 4 | 0 | 1 | 0 | 0 |
| 2 | Fasilitas | 1 | 0 | 0 | 0 | 0 |
| 3 | Infrastruktur TI | 3 | 0 | 0 | 0 | 0 |
| 4 | Informasi / Data | 5 | 0 | 2 | 0 | 0 |
| 5 | Proses | 3 | 1 | 0 | 0 | 0 |
| 6 | SDM | 1 | 0 | 2 | 0 | 0 |
| | Total | 0 | 17 | 1 | 5 | 0 |

2. *Risk Evaluation*

*Risk Evaluation* bertujuan untuk mengevaluasi apakah risiko – risiko tersebut dapat ditoleransi atau tidak oleh perusahaan. *Risk Evaluation* dilakukan dengan menggambarkan hubungan antara *probability* (kecenderungan) dan *impact* (dampak) ke dalam sebuah matriks yang disebut *Risk Map*. Dari *Risk Map* tersebut dapat diketahui risiko mana saja yang membutuhkan tindakan untuk mengatasinya. Adapun hasil pemetaan *Risk Map* dapat dilihat pada Tabel 7 berikut ini.

Tabel 7 *Risk Map*

| *Impact* | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Sangat Besar (5) | 0 | 0 | 0 | 0 | 0 | 0 |
| | Besar (4) | 0 | 0 | 0 | 0 | 0 | 0 |
| | Sedang (3) | 1 | 0 | 0 | 0 | 0 | 1 |
| | Kecil (2) | 11 | 5 | 0 | 0 | 0 | 16 |
| | Sangat Kecil (1) | 3 | 3 | 0 | 0 | 0 | 6 |
| | Total | 15 | 8 | 0 | 0 | 0 | 23 |
| | | Sangat Jarang (1) | Jarang (2) | Kadang-kadang (3) | Sering (4) | Sangat Sering (5) | Total |
| | | *Probability* | | | | | |

Berdasarkan Tabel 7 di atas, dapat diketahui bahwa terdapat 5 buah risiko yang termasuk dalam kategori Menengah (M) dan 1 buah risiko yang termasuk dalam kategori Menengah Rendah (LM). Kedua kategori tersebut termasuk dalam jenis risiko yang tidak dapat diterima oleh perusahaan, sehingga untuk mengurangi dampak terjadinya risiko perlu dilakukan tindakan mitigasi.

### 5.4 Strategi dan Langkah Mitigasi

Langkah mitigasi dapat dirancang dengan melakukan pemetaan skenario risiko IT ke dalam kerangka kerja COBIT untuk mendapatkan risiko – risiko yang relevan. Skenario risiko TI yang dipetakan terdiri dari 1 *Risk Issue* yang termasuk dalam *New Technology*, 1 *Risk Issue* yang termasuk dalam *System Capacity*, 2 *Risk Issue* yang termasuk dalam *Data(base) Integrity* dan 2 *Risk Issue* yang termasuk dalam *IT Expertise and Skills.* Adapun langkah strategi mitigasi yang disarankan untuk PT. Petrokimia Gresik dalam menyikapi beberapa *Risk Issue* dapat dilihat pada Tabel 8 sampai Tabel 11 berikut ini.

Tabel 8 Langkah Mitigasi *New Technology*

| Risiko | Langkah Mitigasi |
|---|---|
| 1. Permintaan aplikasi diluar modul SAP tidak terpenuhi. | - Menyediakan Staff IT yang secara khusus bertanggung jawab dalam proses perancangan dan pembuatan aplikasi.<br>- Memberikan *training* dan pelatihan kepada seluruh Staff IT mengenai perkembangan teknologi informasi terkini.<br>- Melakukan *Outsourcing* untuk memenuhi banyaknya permintaan aplikasi.<br>- Melakukan analisis *cost-benefit* untuk menentukan investasi jangka panjang dan menentukan prioritas aplikasi yang harus dipenuhi terlebih dahulu. |

Tabel 9 Langkah Mitigasi *System Capacity*

| Risiko | Langkah Mitigasi |
|---|---|
| 1. Operasional SAP lambat dan kurang optimal | - Menyediakan Staff IT yang secara khusus bertanggung jawab dalam proses monitoring dan evaluasi terhadap operasional SAP.<br>- Mengadakan *User Licence* pada setiap unit kerja. |

Tabel 10 Langkah Mitigasi *Data(base) Integrity*

| Risiko | Langkah Mitigasi |
|---|---|
| 1. Gangguan komunikasi data antara PG dengan PIHC.<br>2. Gangguan transmisi data antar departemen. | - Menyediakan Staff IT yang secara khusus bertanggung jawab dalam menjaga integritas dan keamanan data.<br>- Menjalin kerja sama dengan Team IT dari PIHC.<br>- Menyediakan *helpdesk* untuk menampung segala keluhan terkait dengan integritas data, sehingga dapat ditindak lanjuti dengan segera.<br>- Menggunakan teknik *outomatic switch* jika terjadi *failure.* |

Tabel 11 Langkah Mitigasi *IT Expertise and Skills*

| Risiko | Langkah Mitigasi |
|---|---|
| 1. Dukungan teknis dari Team IT kurang optimal.<br>2. Adanya *gap* terkait kemampuan yang dimiliki Staff IT | - Meningkatkan kompetensi setiap Staff IT dengan menambah intensitas dalam mengadakan pelatihan atau training terkait dengan Sistem ERP - SAP.<br>- Memperbaiki pola rekruitmen dan pelatihan SDM.<br>- Mengasah kemampuan setiap Staff IT dengan memberikan penugasan atau pekerjaan yang berbeda – beda, agar Staff IT mampu menguasai segala bidang kompetensi yang berhubungan dengan IT.<br>- Mengadakan monitoring dan evaluasi terhadap kinerja seluruh Staff IT.<br>- Bekerja sama dengan Team IT dari PIHC untuk meningkatkan dukungan teknis operasional ERP – SAP.<br>- Menyediakan *helpdesk* tersendiri untuk memudahkan Staff IT dalam menangani setiap keluhan. |

### 5.5 Rekomendasi

Berdasarkan hasil evaluasi manajemen risiko teknologi informasi PT. Petrokimia Gresik dengan menggunakan analisis *capability level* dan *risk assessment* (Penilaian Risiko), disusunlah beberapa rekomendasi yang dapat digunakan untuk mengembangkan dan memperbaiki penerapan manajemen risiko teknologi informasi serta mengurangi terjadinya risiko teknologi informasi di PT. Petrokimia Gresik. Berikut ini adalah hasil rekomendasi yang telah dibuat berdasarkan domain proses EDM03 dan APO12. Berikut ini merupakan hasil rekomendasi yang diberikan kepada PT. Petrokimia Gresik :

1. Membentuk *team* atau manajemen khusus di bawah naungan Departemen TKP & MR yang bertugas untuk mengelola dan mengkoordinasikan penerapan manajemen risiko teknologi informasi, khususnya sistem ERP-SAP di PT. Petrokimia Gresik.
2. Melakukan evaluasi terhadap kinerja staff serta memberikan pelatihan terkait penerapan manajemen risiko teknologi informasi untuk meningkatkan kompetensi SDM.
3. Membuat dokumen tertulis yang fokus membahas mengenai pedoman dan prosedur penerapan manajemen risiko teknologi informasi, khususnya sistem ERP-SAP di PT. Petrokimia Gresik.
4. Menetapkan metode yang tepat untuk memonitoring penerapan manajemen risiko teknologi informasi di PT. Petrokimia Gresik sehingga dapat memantau kesesuaian antara risiko yang ditemukan dengan *Risk Appetite.*
5. Membuat dokumen tertulis yang membahas mengenai mitigasi risiko, *Business continuity Plan, Disaster Recovery Plan,* dan *risk respond* dari seluruh risiko terkait dengan penerapan teknologi informasi.
6. Membuat dokumen tertulis yang membahas mengenai *Cost Benefit Analysis* untuk memperkirakan frekuensi besarnya kerugian dan keuntungan yang harus ditanggung ketika melakukan penanganan pada setiap skenario risiko teknologi informasi.
7. Meningkatkan intensitas kegiatan pemantauan, review, pengendalian dan pengelolaan terhadap penerapan manajemen risiko teknologi informasi melalui program

Klinik Risiko dan Kajian Ulang Manajemen Risiko.
8. Membuat dokumen tertulis yang berbentuk seperti Profil Risiko namun secara khusus menampung hasil identifikasi risiko, analisis risiko (baik berupa analisis sumber, penyebab dan akibat dari risiko), evaluasi penilaian risiko dan pengendalian atau penanganan risiko terkait dengan risiko teknologi informasi.
9. Mengoptimalkan penggunaan Sistem Informasi Manajemen Risiko (SIMAR) dalam melakukan pengelolaan risiko teknologi informasi

## 6 KESIMPULAN DAN SARAN

### 6.1 Kesimpulan

Berdasarkan hasil pembahasan terkait penerapan manajemen risiko teknologi informasi pada PT. Petrokimia Gresik, maka dapat diperoleh kesimpulan sebagai berikut :

1. Proses evaluasi penerapan manajemen risiko teknologi informasi pada PT. Petrokimia Gresik menggunakan kerangka kerja COBIT 5 khususnya subdomain EDM03 *(Ensure Risk Optimation)* dan APO12 *(Manage Risk)* menghasilkan beberapa hal berikut ini :
   a. Nilai *Capability Level* untuk subdomain EDM03 berada pada Level 2 yaitu *Managed Process* yang artinya kegiatan perencanaan, monitoring dan penyelarasan pada domain proses EDM03 telah dikelola serta hasil kerjanya telah ditetapkan, dipantau dan dikelola dengan tepat. Sedangkan Nilai *Capability Level* untuk subdomain APO12 berada pada Level 3 yaitu *Established Process* yang artinya setiap proses yang diimplementasikan telah diidentifikasi terlebih dahulu pada prosedur standart formal dalam bentuk tertulis untuk mencapai hasil yang maksimal dari setiap proses tersebut.
   b. Besarnya *gap* yang terbentuk antara nilai *capability level* yang telah diperoleh dengan nilai *capability level* yang ingin dicapai untuk subdomain EDM03 dan APO12 masing – masing adalah sebesar 1.
   c. Ditemukannya 23 *risk issue* yang terbagi dalam 15 skenario risiko. Dan dari kelima belas skenario risiko tersebut, terdapat 4 skenario risiko yang membutuhkan strategi dan langkah mitigasi.
2. Hasil rekomendasi dan langkah mitigasi yang diberikan untuk perbaikan manajemen risiko teknologi informasi di PT. Petrokimia Gresik adalah sebagai berikut :
   a. Dibuatnya 9 buah rekomendasi agar nilai *Capability Level* pada subdomain EDM03 dapat mencapai Level 3 dan pada subdomain APO12 dapat mencapai Level 4.
   b. Dibuatnya 16 langkah mitigasi berdasarkan 6 buah *risk issue* yang termasuk dalam 4 buah skenario risiko, diantaranya *new technology, database integrity, system capacity* dan *IT expertise skills.* Langkah mitigasi tersebut dirancang untuk memenuhi permintaan aplikasi diluar modul SAP; untuk mengatasi gangguan transmisi data antara departemen dan departemen serta antara PG dengan pihak PIHC; untuk mengoptimalkan operasional SAP; untuk mengoptimalkan dukungan teknis dari team IT dan untuk mengurangi *gap* yang timbul akibat tidak meratanya kemampuan atau *skill* yang dimiliki oleh setiap staff IT.

### 6.2 Saran

Berikut ini terdapat beberapa saran yang akan diberikan oleh penulis untuk penelitian selanjutnya khususnya penelitian terkait manajemen risiko teknologi informasi :

1. Penelitian yang akan dilakukan selanjutnya disarankan untuk meneruskan tahap manajemen risiko dari COBIT 5 *For Risk* ke tahap *Execute Plan* atau bahkan hingga ke tahap *Review Effectiveness*.
2. Penelitian yang akan dilakukan selanjutnya disarankan untuk menggunakan metode atau kerangka kerja lain dalam mengukur *Capability Level* dari penerapan manajemen risiko teknologi informasi, seperti *COSO ERM Integrated Framework*, *Risk IT Framework*, OCTAVE (*Operationally Critical Threat, Asset and Vulnerability Evaluation*), ISO 31000 : 2009 *Risk Management*, NIST *Special Publication* 800-30 *Framework* dan lain – lain

## 7 DAFTAR PUSTAKA

Afifa, L. N., 2011. *Usulan Panduan Pelaksanaan Manajemen Risiko Tata*

*Kelola TIK Nasional. Konferensi Teknologi Informasi dan Komunikasi untuk Indonesia,* pp. 368–372.

Febriyanti, Aulia., and Bekti C.H, S.Si., M.Kom., 2012. *Manajemen Risiko pada Pengelolaan Data di Bagian Pengolahan Data PT. Petrokimia Gresik. Jurnal Teknik POMITS,* 1(1), pp 1-6.

Dyahaloka, Astri, 2016. *Evaluasi Manajemen Risiko E-Procurement Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Pertamina (Persero)).* Malang : Universitas Brawijaya.

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

Hayaty, M., Rosidi, A., and Arief, M.R., 2013. *Risk Assessment Dan Business Impact Analysis Sebagai Dasar Penyusunan Disaster Recovery Plan (Studi Kasus Di Stmik Amikom Yogyakarta). SEMNASTEKNOMEDIA ONLINE,* 1(1), pp.23-1.

ISACA., 2012. *COBIT 5 : A Bussiness Framework for the Governance and Management of Enterprise IT*. Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : Enabling Process.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : The Risk IT Practitioner Guide.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : For Risk.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : Self-Assessment Guide.* Rolling Meadows : ISACA.

Islamiah, Mega Putri., 2014. *Tata Kelola Teknologi Informasi (IT Governance) Menggunakan Framework Cobit 5: Studi Kasus Dewan Kehormatan Penyelenggara Pemilu* (DKPP). Jakarta : Universitas Islam Negeri Syarif Hidayatullah.

ITGI., 2003. *Broad Briefing on IT Governance 2nd Edition*. Rolling Meadows : IT Governance Institute.

Pratama, Enda E., and Suhardi., 2013. *Analisis Nilai & Manajemen Risiko Teknologi Informasi (Studi Kasus PT. Bank Tabungan Negara. Tbk).* Bandung : Institute Teknologi Bandung.

Pressman, Roger S., 2005. *Software engineering: a practitioner's approach*. United Kingdom : Palgrave Macmillan.

Kusumaningrum, Vika P., 2016. *Evaluasi Teknologi Informasi Menggunakan Framework COBIT 5 Pada Domain DSS (Delivery Service and Support) (Studi Kasus : PT. PLN (Persero) Rayon Ngawi).* Malang : Universitas Brawijaya.

Samaptoaji, Sigit, 2014. *Evaluasi Pengelolaan Risiko Teknologi Informasi (TI) pada Instansi Pemerintah : Studi Kasus Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementrian Dalam Negeri.* Jakarta : Universitas Indonesia.

Setiawan, Alexander, 2009. *Evaluasi Penerapan Teknologi Informasi Di Perguruan Tinggi Swasta Yogyakarta Dengan Menggunakan Model Cobit Framework. Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*. Vol. 1. No. 1.

Suwarno, Fajrin Rizkia P., 2014. *Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Pada Proses Manage Relationship (APO08) (Studi Kasus : PT. OTO Multiartha).* Jakarta : Universitas Islam Negeri Syarif Hidayatullah.

Teruri, Shabrina., 2016. *Evaluasi Manajemen Resiko Migrasi Sistem MES Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Krakatau Steel (Persero)Tbk).* Malang : Universitas Brawijaya.

Wibisono, Diaz Mahardika, 2015. *Pengukuran Tingkat Kapabilitas Proses Pengelolaan Risiko Teknologi Informasi Pada Direktorat Sistem Informasi Universitas Airlangga Berdasarkan COBIT 5 Proses APO12 Manage Risk.* Surabaya : Universitas Airlangga.



View publication stats

**Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer** e-ISSN: 2548-964X
Vol. 2, No. 1, Januari 2018, hlm. 91-100 http://j-ptiik.ub.ac.id

# Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Petrokimia Gresik)

**Nurfitri Zukhrufatul Firdaus[1], Suprapto[2]**

Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]fitri.firdaus0@gmail.com, [2]spttif@ub.ac.id

**Abstrak**

SAP (*System Application and Product in Data Processing*) merupakan jenis software ERP yang digunakan oleh PT. Petrokimia Gresik untuk menunjang otomatisasi proses bisnis perusahaan dan mendukung proses pengambilan keputusan agar lebih efektif dan efisien. Untuk mengantisipasi timbulnya risiko yang dapat mengganggu jalannya proses bisnis perusahaan, PT. Petrokimia Gresik menerapkan manajemen risiko berdasarkan standart ISO 31000:2009. Dalam hal ini perlu dilakukan evaluasi untuk mnegetahui pencapaian penerapan manajemen risiko teknologi informasi pada PT. Petrokimia Gresik dengan menggunakan kerangka kerja COBIT 5 khususnya pada domain proses APO12 (Risk Management) dan EDM03 (Ensure Risk Optimation). Untuk memperoleh data yang akurat, maka teknik pengumpulan data yang digunakan adalah dengan melakukan pengisian lembar kerja evaluasi, obeservasi langsung dan wawancara dengan pihak yang berwenang. Proses evaluasi tersebut terdiri dari beberapa tahapan, antara lain melakukan analisis *capability level*, analisis *gap* dan analisis *risk assessment* untuk mengidentifikasi risiko – risiko potensial serta menilai sejauh mana dampak yang dapat ditimbulkan. Berdasarkan hasil analisis tersebut, maka didapatkan nilai *capability level* untuk domain proses EDM03 berada pada level 2 dan domain proses APO12 berada pada level 3 serta menghasilkan 16 buah strategi mitigasi dan 9 buah rekomendasi yang dapat digunakan untuk membantu perbaikan penerapan manajemen risiko teknologi informasi di PT. Petrokimia Gresik.

**Kata kunci**: *COBIT 5, capability level, manajemen risiko, analisis gap, risk assessment, mitigasi risiko*

**Abstract**

*SAP (System Application and Product in Data Processing) is a type of ERP Software that used by PT. Petrokimia Gresik to support business process automation and support decision-making process to be more effective and efficient. To anticipate the potential problems that might obstruct business processes at the company, so PT. Petrokimia Gresik managed to use risk management based on the standards of ISO 31000:2009. An evaluation on the implementation of IT risk management was done to measure its capability level accomplishment. COBIT 5 Framework, especially in process domain APO12 (Risk Management) dan EDM03 (Ensure Risk Optimation), was used as the basis of the evaluation. To collect accurate data, the data were obtained by filling evaluation worksheet, conducting a direct observation and an interview to the people in charge. The process of evaluating the implementation of IT risk management consists of several stages, including capability level analysis, gap analysis and risk assessment analysis to identify potential risks and assess the extent of the impacts of each risk. From the evaluation result, it turned out that capability level for process domain EDM03 was on level 2 and on level 3 for process domain APO12 and 16 mitigation strategy and 9 recommendation were made to support the improvement for the implementation of risk management information and technology at PT. Petrokimia Gresik.*

**Keywords**: *COBIT 5, capability level, risk management, gap analysis, risk assessment, risk mitigation*

## 1. PENDAHULUAN

Salah satu perusahaan yang telah memanfaatkan teknologi informasi dan menerapkan manajemen risiko teknologi informasi sebagai sarana pendukung untuk mencapai tujuan perusahaan adalah PT. Petrokimia Gresik. Untuk meningkatkan kualitas perusahaan dibidang teknologi informasi, PT. Petrokimia Gresik menerapkan sistem ERP – SAP yang terdiri dari sepuluh

modul. Disamping itu PT. Petrokimia Gresik juga menerapkan beberapa aplikasi Non ERP untuk menunjang jalannya Sistem ERP-SAP. Dengan diterapkannya Sistem tersebut diharapkan mampu menunjang otomatisasi proses bisnis perusahaan dan mendukung proses pengambilan keputusan secara efektif dan efisien. Namun pada kenyatannya, penerapan Teknologi Informasi (TI) pada perusahaan tidak selalu berjalan sesuai dengan yang diharapkan, sehingga menimbulkan risiko – risiko yang dapat merugikan perusahaan. Oleh karena itu untuk mengelola segala macam risiko yang dapat mengganggu jalannya proses bisnis dan menimbulkan kerugian, maka PT. Petrokimia Gresik telah menerapkan manajemen risiko berdasarkan pada Standart ISO 31000 : 2009 sejak tahun 2003.

Padatnya proses bisnis yang berjalan di PT. Petrokimia Gresik, mengakibatkan aktivitas pengelolaan risiko menjadi kurang optimal, sehingga masih ditemukan risiko yang dapat menghambat jalannya proses bisnis perusahaan. Risiko – risiko tersebut diantaranya berupa gangguan jaringan internet, gangguan arus listrik, kurang optimalnya dukungan teknis operasional ERP, gangguan komunikasi data antara user dengan server ERP dan lain sebagainya. Oleh karena itu perlu adanya evaluasi manajemen risiko Teknologi Informasi (TI) untuk mengetahui tingkat kapabilitas pengelolaan risiko yang telah dicapai, sehingga dapat meningkatkan kemampuan perusahaan dalam mengelola setiap risiko terkait penerapan sistem ERP-SAP pada PT. Petrokimia Gresik. Dari evaluasi tersebut menghasilkan rekomendasi berupa saran maupun usulan yang dapat digunakan oleh perusahaan untuk meminimalisir terjadinya risiko – risiko yang tidak diinginkan. Salah satu *framework* yang dapat digunakan untuk mengevaluasi manajemen risiko Teknologi Informasi (TI) pada PT. Petrokimia Gresik adalah COBIT 5 khususnya pada domain proses APO12 (*Manage Risk*) dan EDM03 (*Ensure Risk Optimisatin*). Digunakannya domain tersebut karena dalam COBIT 5, hanya ada dua domain yang membahas secara terperinci mengenai manajemen risiko Teknologi Informasi (TI).

## 2. LANDASAN KEPUSTAKAAN

### 2.1. Kajian Pustaka

Adapun penelitian – penelitian terdahulu yang relevan dengan penelitian ini adalah sebagai berikut:

1. Penelitian yang dilakukan oleh Astri Dyahaloka yang berjudul "Evaluasi Manajemen Risikio *E-Procurement* Menggunakan COBIT 5 *IT Risk* (Studi Kasus : PT. Pertamina (Persero))". Penelitian tersebut menggunakan kerangka kerja COBIT 5 dengan domain EDM03 dan APO12. Dalam melakukan evaluasi, penelitian tersebut menggunakan analisis *capability level*, analisis *gap* dan analisis SWOT, sehingga menghasilkan nilai *capability level* yang telah dicapai dan rekomendasi untuk perbaikan penerapan manajemen risiko.
2. Penelitian yang dilakukan oleh Sigit Samaptoaji yang berjudul "Evaluasi Pengelolaan Risiko Teknologi Informasi (TI) pada Instansi Pemerintah : Studi Kasus Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementerian Dalam Negeri". Dalam melakukan evaluasi, penelitian tersebut menggunakan analisis *risk assessment* dan penentuan strategi atau langkah mitigasi, sehingga menghasilkan dokumen profil risiko teknologi informasi yang dapat dijadikan sebagai masukan atau pertimbangan dalam proses pengambilan keputusan.

### 2.2 Manajemen Risiko

Djojosoedarso (2003) menjelaskan bahwa manajemen risiko merupakan proses menjalankan aktivitas manajemen untuk menanggulangi munculnya risiko, baik yang dihadapi perusahaan maupun yang dihadapi oleh masyarakat. Sehingga dapat disimpulkan bahwa fungsi – fungsi manajemen yang dijalankan untuk menanggulangi risiko mencakup proses pengelolaan, pengukuran dan penilaian risiko. Dalam hal ini manajemen risiko dimaksudkan untuk mengurangi dampak negatif dari suatu risiko, menghindari terjadinya risiko, menampung sebagian atau keseluruhan dari konsekuensi risiko atau mengalihkan risiko kepada pihak lain.

### 2.3. COBIT 5

*Control Objective for Information and Related Technology* (COBIT) merupakan seperangkat pedoman dan hasil dokumentasi yang berfungsi untuk membantu auditor, pemangku kepentingan atau pengguna (*user*) dalam menghubungkan antara model kendali bisnis dan model kendali TI. COBIT

dikembangkan untuk menerapkan *Governance of Enterprise IT*. Versi terbaru yang dikeluarkan oleh *IT Governance Institute* dikenal sebagai COBIT 5. COBIT 5 terbentuk dengan mengintegrasikan Risk IT *framework*, VAL IT 2.0 dan COBIT 4.1. Selain itu COBIT 5 juga menyesuaikan antara *best practices* yang ada seperti ITIL V3, TOGAF dan standart relevan dari ISO.

Dalam melakukan evaluasi, ISACA (2012) menjelaskan bahwa terdapat tujuh buah tahapan yang harus diterapkan menurut siklus implementasi COBIT 5, antara lain:

1. *Initiate Programme*, yaitu proses identifikasi pemicu perubahan seperti kondisi trend, kinerja, implementasi perangkat lunak, isu penting dan tujuan organisasi yang mampu memberikan dorongan untuk berubah.
2. *Define Problems and Opportunities*, yaitu proses penyelarasan antara tujuan penerapan TI dengan risiko maupun strategi organisasi, serta mengutamakan tujuan penerapan TI, tujuan organisasi dan proses penerapan TI yang paling utama.
3. *Define Road Map*, yaitu proses penetapan target untuk meningkatkan upaya perbaikan dan diikuti dengan analisis *gap* untuk menentukan beberapa solusi potensial.
4. *Plan Programme*, yaitu proses perencanaan solusi yang dianggap layak untuk dijalankan.
5. *Execute Plan*, yaitu proses penerapan solusi yang telah disarankan ke dalam aktivitas keseharian serta melakukan pemantauan untuk memastikan bahwa keselarasan bisnis dapat dicapai dan kinerja dapat diukur.
6. *Realise Benefits*, yaitu proses transisi secara berkelanjutan dengan menerapkan praktik tata kelola atau manajemen yang telah ditingkatkan ke dalam proses bisnis dan memantau perkembangannya dengan memetakannya pada matriks berdasarkan kinerja dan manfaat yang ingin diperoleh.
7. *Review Effectiveness*, yaitu proses evaluasi keberhasilan yang telah dicapai secara umum, kemudian melakukan identifikasi segala kebutuhan perbaikan secara berkala untuk lebih meningkatkan praktik tata kelola atau manajemen.

Menurut ISACA (2012), COBIT 5 telah menyediakan dua proses yang berkaitan dengan penerapan manajemen risiko, antara lain:

1. EDM03 : *Ensure Risk Optimisation*
   Proses EDM03 bertujuan untuk memastikan apakah tingkat risiko dan besarnya toleransi yang dapat diterima oleh perusahaan telah dimengerti, diartikulasikan dan dikomunikasikan dengan baik, serta memastikan apakah risiko – risiko yang terkait dengan Teknologi Informasi (TI) telah diidentifikasi dan dikelola dengan baik. Proses EDM03 terbagi menjadi 3 atribut, yaitu *Evaluate Risk Management*, *Direct Risk Management* dan *Monitor Risk Management.*
2. APO12 : *Manage Risk*
   Proses APO12 bertujuan untuk mengidentifikasi, menilai dan mengurangi risiko terkait dengan teknologi Informasi (TI) agar tidak melebihi batas toleransi yang telah ditentukan oleh manajemen eksekutif organisasi. Selain itu proses APO12 juga bertujuan untuk mengintegrasikan manajamen risiko Teknologi Informasi (TI) dengan manajemen risiko perusahaan (ERM). Proses APO12 terbagi menjadi enam subdomain, yaitu *Collect Data*, *Analyse Risk*, *Maintain A Risk Profile*, *Articulate Risk*, *Define a Risk Management Action Portofolio* dan *Respond to Risk*

Penilaian *Capability Level* untuk setiap proses tersebut digolongkan menjadi enam tingkatan, yaitu Level 0 (*Incomplete Process*), Level 1 (*Performed Process*), Level 2 (*Managed process*), Level 3 (*Established Process*), Level 4 (*Predictable process*) dan Level 5 (*Optimized process*).

### 2.4. *Risk Assessment*

ISACA (2012) menjelaskan bahwa Secara umum *Risk Assessment* berfungsi untuk mengidentifikasi risiko potensial baik yang berasal dari *internal* maupun *eksternal* organisasi, selain itu juga menilai sejauh mana dampak yang ditimbulkan oleh risiko tersebut dapat mengganggu jalannya proses bisnis dan tujuan organisasi. Besarnya dampak dapat diukur melalui penilaian *Inherent Risk* dan *Residual Risk*, serta dianalisis melalui dua perspektif antara lain *Probability/Likelihood* dan *Impact/Consequence*.

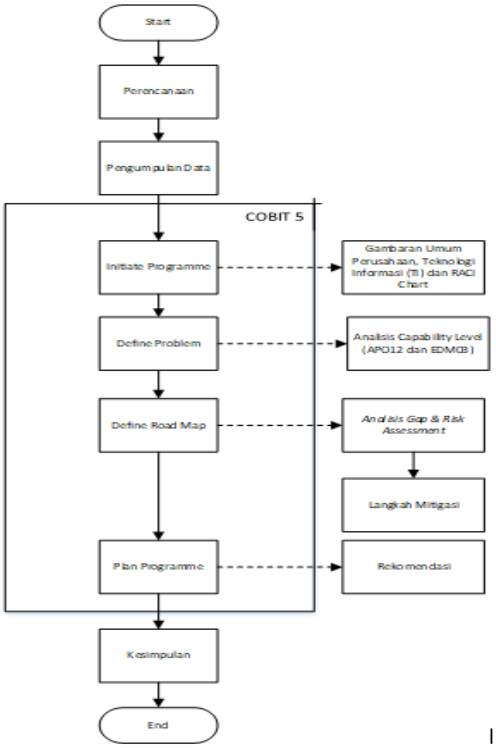
Untuk menyelaraskan antara risiko - risiko yang ditemukan dengan batas toleransi risiko yang telah ditentukan oleh organisasi, maka diperlukan adanya *Risk Response* atau Respon Risiko. Dalam penelitian ini, langkah yang diambil untuk merespon risiko adalah dengan melakukan *Risk Reduction* atau *Mitigation*, yaitu salah satu metode yang dilakukan dengan cara mengurangi besarnya *Probability* atau

*Likelihood* (Peluang atau kecenderungan) dan *Impact* atau *Consequence* (Dampak) yang ditimbulkan dari risiko tersebut.

### 2.5. Sistem ERP – SAP

*System Application and Product in Data Processing* (SAP) merupakan *software* jenis *Enterprise Resources Planning* (ERP) yang dikembangkan untuk menunjang jalannya kegiatan operasional suatu organisasi agar lebih efektif dan efisien. Adapun modul – modul SAP yang diimplementasikan di PT. Petrokimia Gresik antara lain *Material Management, Production Planning, Plant Maintenance, Sales Distribution, Financial Accounting Controlling, Human Capital Management, Quality Management, Fund Management, Business Planning and Consolidation* dan *Dashboard*.

## 3. METODOLOGI




Gambar 1. Diagram Alur Penelitian

1. Menentukan objek penelitian dan kerangka kerja yang tepat serta menggali informasi yang terkait**.**
2. Melakukan pengumpulan data, baik data primer maupun data sekunder dengan cara melakukan pengisian lembar kerja evaluasi, melakukan observasi langsung, melakukan wawancara dengan pihak – pihak yang berwenang dan studi kepustakaan.
3. Mendeskripsikan gambaran umum mengenai kondisi umum organisasi, visi dan misi sebagai tujuan organisasi, gambaran umum sistem informasi atau teknologi informasi yang diterapkan dan pihak – pihak yang bertanggung jawab dalam penerapan manajemen risiko berdasarkan RACI *Chart*.
4. Melakukan analisis penilaian *Capability Level* berdasarkan kerangka kerja COBIT 5 khususnya domain proses EDM03 (*Ensure Risk Optimisation*) dan APO12 (*Manage Risk*).
5. Melakukan *Gap Analysis*, *Risk Assessment* dan menentukan langkah mitigasi untuk setiap risiko yang melebihi batas toleransi perusahaan berdasarkan data yang diperoleh dari hasil lembar kerja evaluasi, observasi dan wawancara.
6. Membuat rekomendasi untuk menentukan solusi potensial berdasarkan hasil analisis *Capability Level*, *Gap Analysis* dan *Risk Assessment*.
7. Menyusun kesimpulan yang berisi ringkasan tentang semua langkah - langkah yang telah dilalui dalam melakukan penelitian.

## 4. HASIL

### 4.1. Hasil Lembar Kerja Evaluasi

Berdasarkan hasil pembuatan RACI *Chart*, dapat diketahui bahwa pihak yang berhak menjadi responden untuk mengisi lembar kerja evaluasi adalah sejumlah tiga orang, antara lain Manager Dept. TEKINFO, Kabag. Infrastruktur TEKINFO dan Manager Dept. TKP & MR.

Tabel 1. Rekapitulasi Hasil Lembar Kerja Evaluasi

| *Prosess Assesment Results* | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Nama Proses** | ***Proces Capability Level*** | | | | | | **Total Responden** |
| | **0** | **1** | **2** | **3** | **4** | **5** | |
| *Evaluate, Direct, and Monitoring* | | | | | | | |
| EDM03 | 0 | 0 | 3 | 0 | 0 | 0 | 3 |
| *Align, Plan, and Organise (APO)* | | | | | | | |
| APO12 | 0 | 0 | 0 | 3 | 0 | 0 | 3 |

Dari Tabel 1 diatas, dapat diketahui bahwa hasil pengisian lembar kerja evaluasi yang dilakukan oleh tiga orang responden menunjukkan nilai *Capability Level* terkait proses EDM03 berada pada Level 2 dan nilai *Capability Level* terkait proses APO12 berada pada Level 3.

### 4.2. Hasil Observasi dan Wawancara

Dalam mengelola proses bisnis perusahaan, PT. Petrokimia Gresik telah mendukung penerapan sistem yang bernama ERP-SAP. Sistem tersebut diharapkan mampu

mengintegrasikan seluruh proses bisnis yang ada pada perusahaan dan mensinergiskan proses bisnis dari masing – masing anggota Pupuk Indonesia *Holding Company* (PIHC). Dalam hal ini, pihak yang bertanggung jawab mendukung jalannya Sistem ERP-SAP, mengintegrasikan sistem atau aplikasi yang dibuat sendiri dengan Sistem ERP-SAP, serta meningkatkan kualitas SDM untuk mendukung penerapan Sistem ERP-SAP adalah Departemen TEKINFO.

Dalam penerapan Sistem ERP – SAP tersebut, tidak pernah lepas dari suatu risiko. Oleh karena itu untuk mengelola segala bentuk risiko perusahaan, Departemen TKP & MR telah menerapkan manajemen risiko berdasarkan standart dan kebijakan yang ditetapkan yaitu ISO 31000 : 2009. Standart dan kebijakan tersebut tertuang dalam dokumen Kebijakan Manajemen Risiko, Pedoman Penerapan Manajemen Risiko, Prosedeur Penerapan Manajeen Risiko, Panduan Penilaian Penerapan Manajemen Risiko dan Pedoman Manajemen Risiko PT. Pupuk Indonesia (Persero). Selama ini penerapan manajemen risiko pada PT. Petrokimia Gresik dimulai dengan melakukan identifikasi terhadap semua risiko yang muncul, menganalisis setiap risiko yang telah diidentifikasi, mengevaluasi setiap risiko, melakukan pengendalian dan penanganan risiko serta melakukan monitoring dan review terhadap pengendalian dan penanganan. Selanjutnya hasil dari aktivitas pengelolaan risiko tersebut disusun dalam sebuah dokumen yang bernama Profil Risiko PT. Petrokimia Gresik.

Dalam mengelola setiap risiko perusahaan, Departemen TKP & MR memiliki aplikasi yang bernama SIMAR (Sistem Informasi Manajemen Risiko) dan program kerja yang bernama Klinik Risiko. Dengan adanya aplikasi SIMAR dan program Klinik Risiko tersebut, dapat memudahkan Departemen TKP & MR dalam memantau penerapan manajemen risiko pada setiap unit kerja.

### 4.3. Hasil Temuan

Berdasarkan hasil lembar kerja evaluasi, observasi dan proses wawancara dengan pihak Departemen TKP & MR dan Departemen TEKINFO PT. Petrokimia Gresik, didapatkan beberapa temuan berikut:

1. Adanya layanan Tata Kelola Perusahaan dan Manajemen Risiko pada PT. Petrokimia Gresik, namun belum adanya manajemen atau team yang dibentuk secara khusus untuk mengelola segala macam risiko terkait dengan teknologi informasi.
2. Pengelolaan risiko yang dilakukan oleh Departemen TKP & MR pada PT. Petrokimia Gresik masih secara umum yaitu dilakukan pada seluruh unit kerja perusahaan dan belum berfokus secara spesifik pada penerapan teknologi informasi.
3. Tidak semua risiko teknologi informasi telah didokumentasikan dan dikelola dengan baik.
4. Belum secara penuh memantau kesesuaian seluruh risiko yang dikelola dengan risk appetite.
5. Dalam melakukan analisis risiko tersebut, belum disertai dengan analisis *cost benefit* yaitu perkiraan frekuensi besarnya keuntungan dan kerugian yang berhubungan dengan penanganan setiap skenario risiko.

## 5. PEMBAHASAN

### 5.1. Analisis *Capability Level*

Berdasarkan hasil pengisian lembar kerja evaluasi yang dilakukan oleh 3 responden dari Departemen TKP & MR dan Departemen TEKINFO PT. Petrokimia Gresik dapat diketahui bahwa nilai *capability level* yang telah dicapai subdomain EDM03 berada pada Level 2 dan nilai *capability level* yang telah dicapai subdomain APO12 berada pada Level 3. Hal tersebut dapat dilihat pada Tabel 2 di bawah ini.

Tabel 2. Rekapitulasi Hasil Gap Analysis

| Nama Proses | Level Saat Ini | Level Target | *Gap* |
|---|---|---|---|
| EDM03 | 2 | 3 | 1 |
| APO12 | 3 | 4 | 1 |

### 5.2. Analisis *Gap*

Berdasarkan hasil wawancara, diperoleh informasi bahwa level target yang ingin dicapai oleh Departemen TKP & MR dan Departemen TEKINFO PT. Petrokimia Gresik adalah naik satu level untuk setiap domain prosesnya, yaitu domain proses EDM03 berada pada Level 3 dan domain proses APO12 berada pada Level 4. Sehingga besarnya *gap* yang terbentuk antara level yang terjadi saat ini dan level target yang ingin dicapai pada domain proses EDM03 dan APO12 adalah sebesar 1.

### 5.3. *Risk Assessment*

Proses *Risk Assessment* dilakukan berdasarkan dua tahapan, antara lain:

1. *Risk Analysis*

*Risk Analysis* bertujuan untuk menentukan seberapa sering risiko tersebut dapat terjadi dan seberapa besar dampak yang dihasilkan oleh risiko tersebut. *Risk Analysis* diawali dengan melakukan identifikasi risiko, menentukan parameter *probability*, menentukan parameter *impact*, menentukan parameter *rating* risiko, melakukan penilaian risiko terhadap *inherent risk* dan *residual risk*.

Adapun pengelompokan risiko berdasarkan skenario risiko dapat dilihat dalam Tabel 3 berikut ini.

Tabel 3. Rekapitulasi Berdasarkan Skenario Risiko

| No | Skenario Risiko | Jumlah *Risk Issue* |
|---|---|---|
| 1 | *New Technology* | 1 |
| 2 | *Software Implementation* | 2 |
| 3 | *Destruction of Infrastructure* | 1 |
| 4 | *IT Staff* | 1 |
| 5 | *IT Expertise and Skills* | 2 |
| 6 | *Software Integrity* | 2 |
| 7 | *Infrastructure (Hardware)* | 3 |
| 8 | *System Capacity* | 2 |
| 9 | *Malware* | 1 |
| 10 | *Logical Attacks* | 1 |
| 11 | *Utilities Performance* | 1 |
| 12 | *Data(base) Integrity* | 2 |
| 13 | *Logical Trespassing* | 1 |
| 14 | *Operational IT Errors* | 2 |
| 15 | *Acts of Nature* | 1 |
| | Total | 23 |

Sedangkan untuk pengelompokan risiko berdasarkan aset dapat dilihat dalam Tabel 4 berikut ini.

Tabel 4. Rekapitulasi Berdasarkan Aset

| No | Kategori Aset | Jumlah *Risk Issue* | Persentase |
|---|---|---|---|
| 1 | Aplikasi | 5 | 21,74 % |
| 2 | Fasilitas | 1 | 4,35 % |
| 3 | Infrastruktur TI | 3 | 13,04 % |
| 4 | Informasi / Data | 7 | 30,43 % |
| 5 | Proses | 4 | 17,39 % |
| 6 | SDM | 3 | 13,04 % |
| | Total | 23 | 100 % |

Sebelum melakukan penilaian risiko terhadap *Inherent Risk* dan *Residual Risk*, terlebih dahulu menentukan standart penilaian berupa parameter *probability* (kecenderungan), parameter *impact* (dampak) dan parameter *Rating* Risiko. Dari hasil rekapitulasi risiko berdasarkan aset dan skenario risiko serta mempertimbangkan parameter *probability* dan *impact* yang telah dibuat, maka dapat diketahui kategori risiko dasar (*Inherent Risk*). *Inherent Risk* merupakan risiko yang dinilai tanpa memasukkan unsur pengendalian yang telah diterapkan. Adapun rekapitulasi hasil penilaian risiko terhadap *Inherent Risk* yang disusun berdasarkan aset dapat dilihat pada Tabel 5 berikut ini.

Tabel 5. Penilaian *Inherent Risk* Berdasarkan Aset

| No | Kategori Aset | Nilai Risiko Dasar | | | | |
|---|---|---|---|---|---|---|
| | | Rendah | Rendah Menengah | Menengah | Menengah Tinggi | Tinggi |
| 1 | Aplikasi | 0 | 0 | 4 | 0 | 1 |
| 2 | Fasilitas | 0 | 0 | 1 | 0 | 0 |
| 3 | Infrastruktur TI | 0 | 1 | 2 | 0 | 0 |
| 4 | Informasi / Data | 0 | 0 | 5 | 2 | 0 |
| 5 | Proses | 0 | 0 | 4 | 0 | 0 |
| 6 | SDM | 0 | 0 | 2 | 1 | 0 |
| | Total | 0 | 1 | 18 | 3 | 1 |

Berdasarkan hasil wawancara dengan beberapa perwakilan dari Dept. TEKINFO dan Dept. TKP & MR, dapat diketahui bahwa setiap risiko – risiko yang teridentifikasi telah memiliki pengendalian tersendiri. Pengendalian tersebut digunakan sebagai dasar untuk melakukan penilaian Residual Risk. Adapun rekapitulasi hasil penilaian risiko terhadap *Residual Risk* yang disusun berdasarkan aset dapat dilihat pada Tabel 6 berikut ini.

Tabel 6. Penilaian *Residual Risk* Berdasarkan Aset

| No | Kategori Aset | Nilai Risiko Dasar | | | | |
|---|---|---|---|---|---|---|
| | | Rendah | Rendah Menengah | Menengah | Menengah Tinggi | Tinggi |
| 1 | Aplikasi | 4 | 0 | 1 | 0 | 0 |
| 2 | Fasilitas | 1 | 0 | 0 | 0 | 0 |
| 3 | Infrastruktur TI | 3 | 0 | 0 | 0 | 0 |
| 4 | Informasi / Data | 5 | 0 | 2 | 0 | 0 |
| 5 | Proses | 3 | 1 | 0 | 0 | 0 |
| 6 | SDM | 1 | 0 | 2 | 0 | 0 |
| | Total | 17 | 1 | 5 | 0 | 0 |

2. *Risk Evaluation*

*Risk Evaluation* bertujuan untuk mengevaluasi apakah risiko – risiko tersebut dapat ditoleransi atau tidak oleh perusahaan. *Risk Evaluation* dilakukan dengan menggambarkan hubungan antara *probability* (kecenderungan) dan *impact* (dampak) ke dalam sebuah matriks yang disebut *Risk Map*. Dari *Risk Map* tersebut dapat diketahui risiko mana saja yang membutuhkan tindakan untuk

mengatasinya. Adapun hasil pemetaan *Risk Map* dapat dilihat pada Tabel 7 berikut ini.

Tabel 7. *Risk Map*

| *Impact* | | | | | | | |
|---|---|---|---|---|---|---|---|
| | **Sangat Besar (5)** | 0 | 0 | 0 | 0 | 0 | 0 |
| | **Besar (4)** | 0 | 0 | 0 | 0 | 0 | 0 |
| | **Sedang (3)** | 1 | 0 | 0 | 0 | 0 | 1 |
| | **Kecil (2)** | 11 | 5 | 0 | 0 | 0 | 16 |
| | **Sangat Kecil (1)** | 3 | 3 | 0 | 0 | 0 | 6 |
| | **Total** | 15 | 8 | 0 | 0 | 0 | 23 |
| | | **Sangat Jarang (1)** | **Jarang (2)** | **Kadang-kadang (3)** | **Sering (4)** | **Sangat Sering (5)** | **Total** |
| | | ***Probability*** | | | | | |

Berdasarkan Tabel 7 di atas, dapat diketahui bahwa terdapat 5 buah risiko yang termasuk dalam kategori Menengah (M) dan 1 buah risiko yang termasuk dalam kategori Menengah Rendah (LM). Kedua kategori tersebut termasuk dalam jenis risiko yang tidak dapat diterima oleh perusahaan, sehingga untuk mengurangi dampak terjadinya risiko perlu dilakukan tindakan mitigasi.

## 5.4. Strategi dan Langkah Mitigasi

Langkah mitigasi dapat dirancang dengan melakukan pemetaan skenario risiko IT ke dalam kerangka kerja COBIT untuk mendapatkan risiko – risiko yang relevan. Skenario risiko TI yang dipetakan terdiri dari 1 *Risk Issue* yang termasuk dalam *New Technology*, 1 *Risk Issue* yang termasuk dalam *System Capacity*, 2 *Risk Issue* yang termasuk dalam *Data(base) Integrity* dan 2 *Risk Issue* yang termasuk dalam *IT Expertise and Skills.* Adapun langkah strategi mitigasi yang disarankan untuk PT. Petrokimia Gresik dalam menyikapi beberapa *Risk Issue* dapat dilihat pada Tabel 8 sampai Tabel 11 berikut ini.

Tabel 8. Langkah Mitigasi *New Technology*

| Risiko | Langkah Mitigasi |
|---|---|
| 1. Permintaan aplikasi diluar modul SAP tidak terpenuhi. | - Menyediakan Staff IT yang secara khusus bertanggung jawab dalam proses perancangan dan pembuatan aplikasi.<br>- Memberikan *training* dan pelatihan kepada seluruh Staff IT mengenai perkembangan teknologi informasi terkini.<br>- Melakukan *Outsourcing* untuk memenuhi banyaknya permintaan aplikasi.<br>- Melakukan analisis *cost-benefit* untuk menentukan investasi jangka panjang dan menentukan prioritas aplikasi yang harus dipenuhi terlebih dahulu. |

Tabel 9. Langkah Mitigasi *System Capacity*

| Risiko | Langkah Mitigasi |
|---|---|
| 1. Operasional SAP lambat dan kurang optimal | - Menyediakan Staff IT yang secara khusus bertanggung jawab dalam proses monitoring dan evaluasi terhadap operasional SAP.<br>- Mengadakan *User Licence* pada setiap unit kerja. |

Tabel 10. Langkah Mitigasi *Data(base) Integrity*

| Risiko | Langkah Mitigasi |
|---|---|
| 1. Gangguan komunikasi data antara PG dengan PIHC.<br>2. Gangguan transmisi data antar departemen. | - Menyediakan Staff IT yang secara khusus bertanggung jawab dalam menjaga integritas dan keamanan data.<br>- Menjalin kerja sama dengan Team IT dari PIHC.<br>- Menyediakan *helpdesk* untuk menampung segala keluhan terkait dengan integritas data, sehingga dapat ditindak lanjuti dengan segera.<br>- Menggunakan teknik *outomatic switch* jika terjadi *failure.* |

Tabel 11. Langkah Mitigasi *IT Expertise and Skills*

| Risiko | Langkah Mitigasi |
|---|---|
| 1. Dukungan teknis dari Team IT kurang optimal.<br>2. Adanya *gap* terkait kemampuan yang dimiliki Staff IT | - Meningkatkan kompetensi setiap Staff IT dengan menambah intensitas dalam mengadakan pelatihan atau training terkait dengan Sistem ERP - SAP.<br>- Memperbaiki pola rekruitmen dan pelatihan SDM.<br>- Mengasah kemampuan setiap Staff IT dengan memberikan penugasan atau pekerjaan yang berbeda – beda, agar Staff IT mampu menguasai segala bidang kompetensi yang berhubungan dengan IT.<br>- Mengadakan monitoring dan evaluasi terhadap kinerja seluruh Staff IT.<br>- Bekerja sama dengan Team IT dari PIHC untuk meningkatkan dukungan teknis operasional ERP – SAP.<br>- Menyediakan *helpdesk* tersendiri untuk memudahkan Staff IT dalam menangani setiap keluhan. |

### 5.5.Rekomendasi

Berdasarkan hasil evaluasi manajemen risiko teknologi informasi PT. Petrokimia Gresik dengan menggunakan analisis *capability level* dan *risk assessment* (Penilaian Risiko), disusunlah beberapa rekomendasi yang dapat digunakan untuk mengembangkan dan memperbaiki penerapan manajemen risiko teknologi informasi serta mengurangi terjadinya risiko teknologi informasi di PT. Petrokimia Gresik. Berikut ini adalah hasil rekomendasi yang telah dibuat berdasarkan domain proses EDM03 dan APO12. Berikut ini merupakan hasil rekomendasi yang diberikan kepada PT. Petrokimia Gresik:

1. Membentuk *team* atau manajemen khusus di bawah naungan Departemen TKP & MR yang bertugas untuk mengelola dan mengkoordinasikan penerapan manajemen risiko teknologi informasi, khususnya sistem ERP-SAP di PT. Petrokimia Gresik.
2. Melakukan evaluasi terhadap kinerja staff serta memberikan pelatihan terkait penerapan manajemen risiko teknologi informasi untuk meningkatkan kompetensi SDM.
3. Membuat dokumen tertulis yang fokus membahas mengenai pedoman dan prosedur penerapan manajemen risiko teknologi informasi, khususnya sistem ERP-SAP di PT. Petrokimia Gresik.
4. Menetapkan metode yang tepat untuk memonitoring penerapan manajemen risiko teknologi informasi di PT. Petrokimia Gresik sehingga dapat memantau kesesuaian antara risiko yang ditemukan dengan *Risk Appetite.*
5. Membuat dokumen tertulis yang membahas mengenai mitigasi risiko, *Business continuity Plan*, *Disaster Recovery Plan*, dan *risk respond* dari seluruh risiko terkait dengan penerapan teknologi informasi.
6. Membuat dokumen tertulis yang membahas mengenai *Cost Benefit Analysis* untuk memperkirakan frekuensi besarnya kerugian dan keuntungan yang harus ditanggung ketika melakukan penanganan pada setiap skenario risiko teknologi informasi.
7. Meningkatkan intensitas kegiatan pemantauan, review, pengendalian dan pengelolaan terhadap penerapan manajemen risiko teknologi informasi melalui program Klinik Risiko dan Kajian Ulang Manajemen Risiko.
8. Membuat dokumen tertulis yang berbentuk seperti Profil Risiko namun secara khusus menampung hasil identifikasi risiko, analisis risiko (baik berupa analisis sumber, penyebab dan akibat dari risiko), evaluasi penilaian risiko dan pengendalian atau penanganan risiko terkait dengan risiko teknologi informasi.
9. Mengoptimalkan penggunaan Sistem Informasi Manajemen Risiko (SIMAR) dalam melakukan pengelolaan risiko teknologi informasi

## 6. KESIMPULAN

Berdasarkan hasil pembahasan terkait penerapan manajemen risiko teknologi informasi pada PT. Petrokimia Gresik, maka dapat diperoleh kesimpulan sebagai berikut:

1. Proses evaluasi penerapan manajemen risiko teknologi informasi pada PT. Petrokimia Gresik menggunakan kerangka kerja COBIT 5 khususnya subdomain EDM03 *(Ensure Risk Optimation)* dan APO12 *(Manage Risk)* menghasilkan beberapa hal berikut ini:
   a. Nilai *Capability Level* untuk subdomain EDM03 berada pada Level 2 yaitu *Managed Process*. Sedangkan Nilai *Capability Level* untuk subdomain APO12 berada pada Level 3 yaitu *Established Process.*
   b. Besarnya *gap* yang terbentuk antara nilai *capability level* yang telah diperoleh dengan nilai *capability level* yang ingin dicapai untuk subdomain EDM03 dan APO12 masing – masing adalah sebesar 1.
   c. Ditemukannya 23 *risk issue* yang terbagi dalam 15 skenario risiko. Dan dari kelima belas skenario risiko tersebut, terdapat 4 skenario risiko yang membutuhkan strategi dan langkah mitigasi.
2. Hasil rekomendasi dan langkah mitigasi yang diberikan untuk perbaikan manajemen risiko teknologi informasi di PT. Petrokimia Gresik adalah sebagai berikut:
   a. Dibuatnya 9 buah rekomendasi agar nilai *Capability Level* pada subdomain EDM03 dapat mencapai Level 3 dan pada subdomain APO12 dapat mencapai Level 4.
   b. Dibuatnya 16 langkah mitigasi berdasarkan 6 buah *risk issue* yang termasuk dalam 4 buah skenario risiko,

diantaranya *new technology, database integrity, system capacity* dan *IT expertise skills.* Langkah mitigasi tersebut dirancang untuk memenuhi permintaan aplikasi diluar modul SAP; untuk mengatasi gangguan transmisi data antara departemen dan departemen serta antara PG dengan pihak PIHC; untuk mengoptimalkan operasional SAP; untuk mengoptimalkan dukungan teknis dari team IT dan untuk mengurangi *gap* yang timbul akibat tidak meratanya kemampuan atau *skill* yang dimiliki oleh setiap staff IT.

## 7. DAFTAR PUSTAKA


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

Dyahaloka, Astri, 2016. *Evaluasi Manajemen Risiko E-Procurement Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Pertamina (Persero)).* Malang : Universitas Brawijaya.

Febriyanti, Aulia., and Bekti C.H, S.Si., M.Kom., 2012. *Manajemen Risiko pada Pengelolaan Data di Bagian Pengolahan Data PT. Petrokimia Gresik. Jurnal Teknik POMITS,* 1(1), pp 1-6. Tersedia di: <http://digilib.its.ac.id> [Diakses 26 Januari 2017]

*Menggunakan Framework Cobit 5: Studi Kasus Dewan Kehormatan Penyelenggara Pemilu* (DKPP). Jakarta : Universitas Islam Negeri Syarif Hidayatullah. Tersedia di : <http://repository.uinjkt.ac.id> [Diakses 24 September 2016]

ITGI., 2003. *Broad Briefing on IT Governance 2nd Edition*. [e-book]. Rolling Meadows : IT Governance Institute.

Petrokimia Gresik, 2012. *Profil.* [Online] Tersedia di : <http://www.petrokimia-gresik.com/> [Diakses 11 Juli 2016].

Pratama, Enda E., and Suhardi., 2013. *Analisis Nilai & Manajemen Risiko Teknologi Informasi (Studi Kasus PT. Bank Tabungan Negara. Tbk).* Bandung : Institute Teknologi Bandung. Tersedia di : <http://www.academia.edu/> [Diakses 6 Oktober 2016].

Pressman, Roger S., 2005. *Software*

Hayaty, M., Rosidi, A., and Arief, M.R., 2013. *Risk Assessment Dan Business Impact Analysis Sebagai Dasar Penyusunan Disaster Recovery Plan (Studi Kasus Di Stmik Amikom Yogyakarta). SEMNASTEKNOMEDIA ONLINE*, 1(1), pp.23-1.

Husein, G.M. and Imbar, R.V., 2015. *Analisis Manajemen Risiko Teknologi Informasi Penerapan Pada Document Management System di PT. JABAR TELEMATIKA (JATEL). Jurnal Teknik Informatika dan Sistem Informasi*, *1*(2). Tersedia di: <http:// http://jutisi.maranatha.edu/index.php/jutisi> [Diakses 6 Oktober 2016]

ISACA., 2012. *COBIT 5 : A Bussiness Framework for the Governance and Management of Enterprise IT.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : Enabling Process.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : The Risk IT Practitioner Guide.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : For Risk.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : Self-Assessment Guide.* Rolling Meadows : ISACA.

Islamiah, Mega Putri., 2014. *Tata Kelola Teknologi Informasi (IT Governance) engineering: a practitioner's approach*. United Kingdom : Palgrave Macmillan.

Samaptoaji, Sigit, 2014. *Evaluasi Pengelolaan Risiko Teknologi Informasi (TI) pada Instansi Pemerintah : Studi Kasus Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementrian Dalam Negeri.* Jakarta : Universitas Indonesia. Tersedia di: <http://lib.ui.ac.id> [Diakses 29 Maret 2017]

Setiawan, Alexander, 2009. *Evaluasi Penerapan Teknologi Informasi Di Perguruan Tinggi Swasta Yogyakarta Dengan Menggunakan Model Cobit Framework. Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*. Vol. 1. No. 1. Tersedia di: <http:// http://www.jurnal.uii.ac.id/index.php> [Diakses 24 September 2016]

Suwarno, Fajrin Rizkia P., 2014. *Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Pada Proses Manage Relationship (APO08) (Studi Kasus : PT. OTO Multiartha).* Jakarta : Universitas Islam Negeri Syarif Hidayatullah. Tersedia di : <http://repository.uinjkt.ac.id> [Diakses 24 September 2016]

Teruri, Shabrina., 2016. *Evaluasi Manajemen Resiko Migrasi Sistem MES Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Krakatau Steel (Persero)Tbk).* Malang : Universitas Brawijaya.

Wibisono, Diaz Mahardika, 2015. *Pengukuran Tingkat Kapabilitas Proses Pengelolaan Risiko Teknologi Informasi Pada Direktorat Sistem Informasi Universitas Airlangga Berdasarkan COBIT 5 Proses APO12 Manage Risk.* Surabaya : Universitas Airlangga.

# Analisis Manajemen Resiko Teknologi Informasi Penerapan Pada *Document Management System* di PT. Jabar Telematika (JATEL)

Gilang M. Husein[#1], Radiant Victor Imbar[*2]

[#]*Jurusan Sistem Informasi, Universitas Kristen Maranatha Bandung*

[1]mchmd.hussein@gmail.com

[2]radiantv@gmail.com

*Abstract* — **ADEL (Aplikasi Dokumen Elektronik) and NADINE (Naskah Dinas Elektronik) are the use of information technology (IT) document management system (DMS) electronic archive product that used by JATEL to enhance information quality and to establish an information dan document workflow so it becomes easier, faster, and well-maintained. Electronic archive IT systems are designed to increase the value and benefits of information and able to control the documents distribution and disposition simultaneously that can increase JATEL business value and support business process automation. Information technology can assist organization but also present risks that need to be managed properly. To anticipate or reduce the likelihood of risk, information technology risk management is required. The implementation of information technology risk management involve risk identification, risk assessment, including risk analysis using bow-tie analysis, qualitative analysis also semi-quantitative analysis, and risk treatment so that risks can be identified, assess, and risk treatment strategy can be planned. With the implementation of information technology risk management at document management system in JATEL risks can be managed and prevented by eliminating sources of risk or reducing susbstantially the likelihood of occurrence.**

*Keywords* — ***risk identification, risk assessment, risk treatment, bow-tie analysis, qualitative analysis and semi-quantitative analysis.***

## I. PENDAHULUAN

### A. Latar Belakang

PT. Jabar Telematika (JATEL) merupakan anak perusahaan dari PT. Jasa Sarana, Badan Usaha Milik Daerah (BUMD) Pemerintah Provinsi Jawa Barat yang bergerak dibidang Infrastruktur. Melalui PT Jabar Telematika, PT Jasa Sarana mengembangkan 3 (tiga) layanan, yaitu: layanan akses internet kecepatan tinggi, layanan jaringan komunikasi data terintegrasi dan layanan *payment switching*. JATEL, sebagai perusahaan yang bergerak dibidang telematika, memiliki beberapa produk teknologi informasi yang digunakan untuk menunjang peningkatan kualitas informasi. Dalam membangun alur kerja informasi dan dokumen sehingga proses atau alur informasi dokumen menjadi lebih mudah, cepat, dan terkelola dengan baik JATEL menerapkan *Document Management System* arsip elektronik yaitu Aplikasi Dokumen Elektronik (ADEL) dan Naskah Dinas Elektronik (NADINE). Sistem arsip eletronik ini dirancang untuk meningkatkan nilai dan manfaat informasi serta mampu mengawasi distribusi dan disposisi dokumen dalam waktu bersamaan sehingga berdampak pada peningkatan *business value* JATEL.

Melalui Teknologi Informasi (TI), berupa sistem arsip elektronik, JATEL dapat melakukan proses bisnis yang lebih efisien. Sistem TI juga mendukung otomatisasi proses bisnis dan penyediaan informasi untuk pengambilan keputusan. Namun dalam penerapannya, TI tidak selalu berjalan sesuai dengan yang diharapkan oleh perusahaan, sehingga akan menimbulkan risiko yang merugikan perusahaan. Untuk mengantisipasi atau mengurangi kemungkinan terjadinya risiko tersebut maka diperlukan analisis manajemen risiko teknologi informasi. Penerapan dari analisis manajemen risiko teknologi informasi meliputi *risk identification, risk assessment* serta *risk treatment*.

### B. Rumusan Masalah

Berdasarkan latar belakang masalah yang telah dijelaskan pada bagian sebelumnya, maka perumusan masalah yang akan dibahas adalah sebagai berikut:

1. Bagaimana proses analisis manajemen risiko teknologi informasi pada *document management system* arsip elektronik Aplikasi Dokumen Elektronik (ADEL) dan Naskah Dinas Elektronik (NADINE) di JATEL?
2. Apa sajakah risiko yang terjadi pada *document management system* Aplikasi Dokumen Elektronik (ADEL) dan Naskah Dinas Elektronik (NADINE) arsip elektronik di JATEL?
3. Bagaimana hasil dari analisis manajemen risiko teknologi informasi pada *document management system* Aplikasi Dokumen Elektronik (ADEL) dan Naskah Dinas Elektronik (NADINE) arsip elektronik di JATEL?

### *C. Tujuan Pembahasan*

Tujuan yang ingin dicapai dari pembahasan penelitian ini adalah dengan melakukan analisis menjemen risiko teknologi informasi maka dapat diidentifikasi risiko *(risk identification*) yang terjadi dalam penerapan *document menegement* sistem arsip elektronik Aplikasi Dokumen Elektronik (ADEL) dan Naskah Dinas Elektronik (NADINE) di JATEL. Melakukan penilaian risiko (*risk assessment*) serta perlakuan terhadapan risiko (*risk treatment*). Nantinya, hasil analisis manajemen risiko teknologi informasi pada *document management system* arsip elektronik Aplikasi Dokumen Elektronik (ADEL) dan Naskah Dinas Elektronik (NADINE) di JATEL diharapkan dapat mengantisipasi dan mencegah kemungkinan terjadinya risiko (*risk prevention*). Tujuan pembahasan dapat dirumuskan sebagai berikut:

1. Melakukan proses analisis manajemen risiko teknologi informasi pada *document management system* arsip elektronik Aplikasi Dokumen Elektronik (ADEL) dan Naskah Dinas Elektronik (NADINE) di JATEL.
2. Menganalisis risiko yang terjadi pada *document management system* Aplikasi Dokumen Elektronik (ADEL) dan Naskah Dinas Elektronik (NADINE) arsip elektronik di JATEL.
3. Menghasilkan analisis manajemen risiko teknologi informasi pada *document management system* Aplikasi Dokumen Elektronik (ADEL) dan Naskah Dinas Elektronik (NADINE) arsip elektronik di JATEL.

## II. KAJIAN TEORI

### *A. Pengertian Risiko*

Definisi *risk* atau risiko pada *The Oxford English Dictionary* adalah *'A chance or possibility of danger, loss, injury, or other adverse consequences'* [1]. Dan definisi *at risk* atau berisiko dari sumber yang sama adalah *'exposed to danger'* [1]. Dalam konteks ini risiko selalu dikaitkan dengan konsekuensi negatif namun menghadapi atau mengambil risiko juga dapat menghasilkan dampak positif. Kemungkinan lainnya risiko bisa berujung pada konsekuensi yang tidak dapat dipastikan.

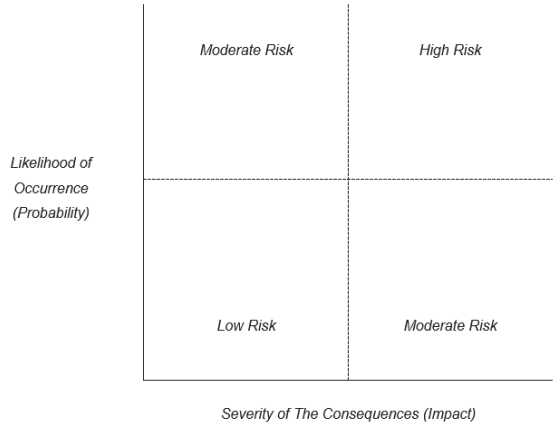
TABEL I
*DEFINITION OF RISK*[2]

| Organization | Definition of risk |
|---|---|
| ISO Guide 73<br>ISO 31000 | Effect of uncertainty on objectives. Note that an effect may be positive, negative, or a deviation from the expected. Also, risk is often described by an event, a change in circumstances or a consequence. |
| Institute of Risk Management (IRM) | Risk is the combination of the probability of an event and its consequence. Consequences can range from positive to negative. |
| "Orange Book" from HM Treasury | Uncertainty of outcome, within a range of exposure, arising from a combination of the impact and the probability of potential events. |
| Institute of Internal Auditors | The uncertainty of an event occurring that could have an impact on the achievement of the objectives. Risk is measured in terms of consequences and likelihood. |
| Alternative Definition by the author | Event with the ability to impact (inhibit, enhance or cause doubt about) the mission, strategy, projects, routine operations, objectives, core processes, key dependencies and / or the delivery of stakeholder expectations. |

Sedangkan risiko menurut ISO Guide 73 ISO 31000 adalah pengaruh ketidakpastian pada tujuan. Pengaruh bisa saja positif, negatif, atau penyimpangan dari yang diharapkan. Risiko juga sering digambarkan sebagai sebuah peristiwa, perubahan dalam keadaan atau konsekuensi. Menurut *Institute of Risk Management* (IRM) risiko merupakan gabungan antara kemungkinan sebuah kejadian beserta konsekuensinya. Konsekuensinya berkisar dari konsekuensi positif hingga konsekuensi negatif. *"Orange Book"* dari *HM Treasury* mendefinisikan risiko sebagai ketidakpastian hasil, dalam berbabagi paparan, timbul dari kombinasi antara dampak dan kemungkinan dari peristiwa. *Institute of Internal Auditors* menjelaskan bahwa risiko adalah ketidakpastian suatu peristiwa yang terjadi yang berdampak pada pencapaian sebuah tujuan. Risiko diukur dengan konsekuensi dan kemungkinan. Sedangkan menurut Paul Hopkins, risiko merupakan suatu peristiwa dengan kemampuan untuk mempengaruhi (menghambat, meningkatkan, atau menyebabkan keraguan) misi, strategi, proyek, operasi rutin, tujuan, proses inti, kunci dependensi dan/atau harapan dari *stakeholder* [2].

### *B. Konsep Risiko*

Risiko, seperti telah dijelaskan pada bagian sebelumnya, suatu kondisi atau kejadian yang tidak pasti yang bila terjadi dapat memberikan dampak negatif maupun positif. Risiko terjadi secara kumulatif dan dapat mempengaruhi sebuah objektif [2].




Gambar 2 *Concept of Risk* [3]

Berdasarkan Gambar 1 tentang konsep Risiko maka dapat diketahui *level of risk* (tingkatan risiko). Berdasarkan variabel yang digunakan, *probability* dan *impact*, maka *level of risk* dapat diklasifikasikan sebagai berikut [3]:

1. *Low Probability Low Impact = Low Risk*.
   Risiko ini adalah risiko dengan tingkat pengaruh yang paling kecil dibandingkan dengan risiko lainya sehingga, dengan kebijakan tertentu, risiko ini dapat diabaikan.

2. *Low Probability High Impact = Moderate Risk*.
   Risiko dengan tingkat pengaruh menengah, meskipun begitu risko ini harus dimonitor dan membutuhkan penanganan yang berkelanjutan tergantung dari dampak yang diberikan.
3. *High Probability Low Impact = Moderate Risk*.
   Risiko dengan tingkat pengaruh menengah. Berbeda dengan *low probability high impact* risiko ini hanya perlu dimonitor.
4. *High Probability High Impact = High Risk.*
   Risiko dengan pengaruh yang paling tinggi dibandingkan dengan lainnya. Merupakan risiko berbahaya yang harus diatasi secepatnya.

### C. Pengertian Manajemen Risiko

Manajemen risiko mengacu pada budaya, proses dan struktur yang diarahkan pada pengelolaan ketidakpastian [4]. Proses pada manajemen risiko terjadi secara sistematis, terus menerus dan diterapkan dalam segala aspek [2]. Dalam konteks organisasi, manajemen risiko diterapkan dalam seluruh bidang yang terdapat dalam organisasi tersebut.

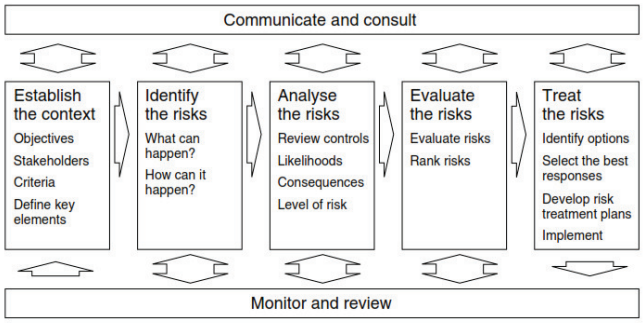
TABEL II
*DEFINITION OF RISK MANAGEMENT* [2]

| Organization | Definition of risk management |
|---|---|
| ISO Guide 73<br>BS 31100 | Coordinated activities to direct and control an organization with regard to risk |
| Institute of Risk Management (IRM) | Process which aims to help organizations understand, evaluate and take action on all their risks with a view to increasing the probability of success and reducing the likelihood of failure |
| HM Treasury | All the processes involved in identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress |
| London School of Economics | Selection of those risks a business should take and those which should be avoided or mitigated, followed by action to avoid or reduce risk |
| Business Continuity Institute | Culture, processes and structures that are put in place to effectively manage potential opportunities and adverse effects |

Menurut ISO Guide 73 BS31100 manajemen risiko adalah aktivitas yang terkoordinasi untuk mengarahkan dan mengendalikan organisasi dari hal-hal yang berkaitan dengan risiko. *Institute of Risk Management* (IRM) mendefinisikan manajemen risiko sebagai proses yang bertujuan untuk membantu organisasi memahami, menilai dan mengambil tindakan pada semua risiko dengan maksud untuk meningkatkan kemungkinan keberhasilan dan mengurangi kemungkinan kegagalan. *HM Treasury* menjelaskan manajemen risiko sebagai semua proses yang terlibat dalam mengidentifikasi, menilai, dan mempertimbangkan risiko, menetapkan kepemilikan, mengambil tindakan untuk mengurangi atau mengantisipasi risiko, dan pemantauan dan peninjauan kemajuan. Sedangkan menurut *London School of Economics* risiko bisnis harus diambil dan dipilah yang harus dihindari dan dikurangi diikuti oleh tindakan menghindar atau mengurangi risiko. Sedangkan menurut *Business Continuity Institute* manajemen risiko merupakan budaya, proses dan struktur yang diletakan untuk mengelola potensi peluang dan efek merugikan secara efektif [2].

### D. Proses Manajemen Risiko

Proses pada manajemen risiko melibatkan pengaplikasian secara sistematis dari pengelolaan kebijakan, proses dan prosedur hingga proses dalam penentuan konteks, mengidentifikasi, menilai, memperlakukan, mengamati, dan mengkomunikasikan risiko [4].




Gambar 3 *Risk Management Process* [4]

Proses dari manajemen risiko berfungsi membantu dalam melakukan pengambilan keputusan yang lebih baik dan meningkatkan efisiensi. Meskipun banyak cara dalam menggambarkan proses manajemen risiko, langkah-langkah dasar yang terdapat dalam proses ini hampir serupa dan biasanya mencakup tiga langkah utama yaitu: *risk identification, risk assessment,* dan *risk treatment*

1. *Risk Identification*
   *Risk identification* merupakan proses dalam menentukan apa, bagaimana, dan mengapa suatu kondisi atau kejadian dapat terjadi. Proses identifikasi risiko harus dilakukan secara komprehensif, harus terstruktur berdasarkan faktor-faktor utama agar nantinya risiko dapat dinilai secara sistematis [4]. Risiko dapat diidentifikasi melalui beberapa metode seperti; *checklist, interview* atau *focused group discussion* dan *questionnaries.*
   *Checklist* digunakan untuk menyederhanakan proses identtifikasi risiko. *Checklist* juga dirancang untuk menghindari atau meminimalkan risiko, seringkali *checklist* merupakan bagian dari prosedur dokumentasi dan jaminan kualitas organisasi.
   *Questionnaries* atau kuesioner merupakan instrumen penelitian yang terdiri dari serangkaian pertanyaan dan petunjuk lainnya dengan tujuan untuk mengumpulkan informasi tertentu dari responden.
2. *Risk Assesment*
   *Risk assesment* merupakan keseluruhan proses dari *risk analysis* dan *risk evaluation. Risk analysis* adalah

proses sistematis dalam menggunakan informasi yang ada untuk menentukan seberapa sering risiko dapat terjadi dan seberapa besar dampak yang dihasilkan bila risiko tersebut terjadi [4]. Proses penilaian risiko pada *risk analysis* dapat dilakukan dengan metode seperti; *bow-tie analysis, qualitative analysis,* dan *semi-quantitative analysis.* Sedangkan *risk evaluation* adalah proses dalam membandingkan risiko yang telah diperkirakan dengan kriteria risiko yang telah ditentukan [4]. Evaluasi risiko memperhitungkan apakah risiko dapat ditoleransi atau tidak didasarkan pada *level of risk* (tingkatan risiko) pada matriks risiko.
*Bow-tie analysis* pada *risk analysis* merupakan metode analisis yang digunakan untuk menggambarkan kegiatan manajemen risiko agar lebih mudah dimengerti dan diakses.

Gambar 4 *Bow-tie Analysis*

Sisi kiri dari dasi kupu-kupu merupakan sumber bahaya (*hazard*) tertentu dan menunjukan sistem klasifikasi yang digunakan oleh organisasi untuk sumber risiko. Sisi kanan dari dasi kupu-kupu menetapkan konsekuensi (*consequences*) dari peristiwa yang terjadi. Di bagian pusat, adalah *risk event* (kejadian risiko). Tujuan menggunakan ilustrasi dasi kupu-kupu adalah untuk menunjukan sistem klasifikasi risiko yang digunakan oleh organisasi. Kontrol (*control*) dapat diletakan untuk mencegah peristiwa yang terjadi dan diwakili oleh garis vertikal di sisi kiri dasi kupu-kupu. Pemulihan (*recovery*) dapat direpresentasikan dengan cara yang sama di sisi kanan dasi kupu-kupu [2]
*Qualitative Analysis* atau analisis kualitatif pada *risk analysis* didasarkan pada nominal atau skala deskriptif untuk menggambarkan *likelihood* dan *consequences* dari risiko, sedangkan *semi-quantitative analysis* atau analisis semi-kuantitatif pada *risk analysis* memperluas proses analisis kualitatif dengan mengalokasikan nilai numerik pada skala deskriptif.

3. *Risk Treatment*
   *Risk treatment* bertujuan untuk menentukan tindakan yang dilakukan dalam mengatasi risiko yang telah teridentifikasi, guna mengurangi pengaruh risiko secara keseluruhan [4]. *Risk treatment* merubah analisis sebelumnya, *risk identification* dan *risk assessment*, menjadi tindakan substantif untuk mengurangi risiko.

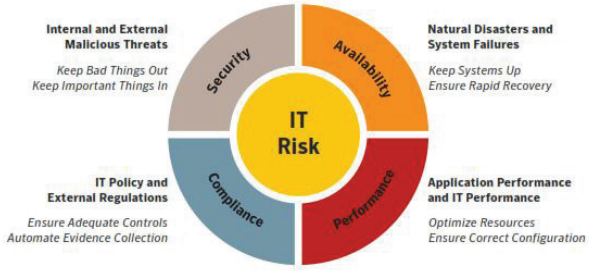
Terdapat beberapa *risk treatment* yang umumnya digunakan, yaitu; *risk prevention* (pencegahan risiko) dengan tujuan untuk mengurangi secara substansial kemungkinan terjadinya risiko, *risk mitigation* (mitigasi risiko) dengan tujuan untuk meminimalkan konsekuansi dari risiko, *risk sharing* (berbagi risiko) dengan tujuan untuk memindahkan risiko tidak hanya ke organisasi lain namun juga ke entitas bisnis ataupin individu, dan *risk retention* (retensi risiko) atau dikenal juga sebagai penyerapan, toleransi, atau penerimaan risiko.

## *E. Risk Management Framework*

Secara umum diakui bahwa *risk management framework* (kerangka kerja manajemen risiko) merupakan dokumen yang menghasilkan informasi pada proses manajemen risiko. Dalam banyak kerangka kerja manajemen risiko, aktivitas manajemen risiko harus dilakukan dalam konteks lingkungan bisnis, organisasi dan risiko yang dihadapi oleh organiasi. Agar konteks dapat dijelaskan dan didefinisikan, kerangka kerja diperlukan dalam mendukung prosesnya [2].

Berikut merupakan *risk management framework* yang digunakan dalam penelitian:

1. *Symantec: Risk Management Report*
   Teknologi Informasi (TI) secara luas dan mendalam telah menjadi saling berhubungan dengan operasi bisnis, risiko TI sendiri pun telah tumbuh menjadi bagian dari keseluruhan komponen operasional [7].




Gambar 5 *IT Risk Classification* [7]

Untuk membantu organisasi dalam memahami dan menganalisa risiko TI dan mengatur strategi mitigasi, maka dibuat *framework* (kerangka kerja) klasifikasi risiko berdasarkan dampaknya terhadap organisasi. Kerangka kerja tersebut mengklasifikasikan risiko TI sebagai [7]:

- *Security Risk* atau risiko keamanan – bahwa informasi dapat dirubah, diakses atau digunakan oleh pihak yang tidak bertanggung jawab.
- *Availability Risk* atau risiko ketersediaan – bahwa informasi atau aplikasi tidak dapat diakses karena *system failure* (kegagalan sistem) atau bencana alam, termasuk masa pemulihan (*recovery*).
- *Performance Risk* atau risiko kinerja – bahwa kinerja yang kurang dari system, aplikasi, personil, atau TI

secara keselruhan, dapat mengurangi produktivitas atau nilai bisnis.

- *Compliance Risk* atau risiko pemenuhan – bahwa penanganan atau pengolahan informasi gagal memenuhi peraturan, TI atau persyaratan kebijakan bisnis (*business policy requirements*).

2. COBIT 5 *for Risk*

COBIT adalah kerangka kerja (*framework)* yang dibuat oleh ISACA untuk manajemen teknologi informasi (TI) dan tata kelola IT. COBIT adalah *toolset* yang memungkinkan penggunanya untuk menjembatani kesenjangan antara kebutuhan kontrol, masalah teknis dan risiko bisnis [8].

Sumber daya TI yang diidentifikasikan dalam COBIT dapat dijelaskan secara singkat sebagai berikut [9]:

- Aplikasi (*Application*), merupakan suatu sarana atau *tool* yang digunakan untuk mengolah dan menyimpulkan atau meringkas, baik prosedur manual maupun yang terprogram.
- Informasi (*Information*), adalah data-data yang telah diolah untuk kepentingan manajemen dalam membantu mengambil keputusan dalam menjalankan roda bisnisnya. Data-data terdiri obyek-obyek dalam pengertian yang lebih luas (yakni internal dan eksternal), terstruktur dan tidak terstruktur, grafik, suara dan sebagainya.
- Infrastruktur (*infrastructure*), mencakup *hardware, software,* sistem operasi, sistem manajemen database, jaringan (*networking*), multimedia, dan fasilitas-fasilitas lainnya.
- Sumber Daya Manusia/SDM (*People*), merupakan sumber daya yang paling penting bagi organisasi dalam pengelolaan dan operasionalisasi bisnis organisasi. Kesadaran dan produktivitasnya dibutuhkan untuk merencanakan, mengorganisasikan, melaksanakan, memperoleh, menyampaikan, mendukung, dan memantau layanan TI organisasi.

### *F. Document Management System*

Manajemen dokumen, sering disebut sistem manajemen dokumen atau *Document Management System* (DMS), adalah penggunaan sistem komputer dan perangkat lunak untuk menyimpan, mengelola, dan untuk melacak dokumen elektronik dan gambar elektronik dari informasi berbasis kertas.

TABEL III
KOMPONEN *DOCUMENT MANAGEMENT SYSTEM*

| Komponen | Deskripsi |
|---|---|
| *Metadata* | Metadata biasanya tersimpan dalam tiap dokumen. Salah satu contoh dari metadata adalah tanggal dokumen itu disimpan dan identitas pengguna yang menyimpannya. DMS juga dapat mengekstrak metadata dari dokumen secara otomatis atau meminta pengguna untuk menambahkan metadata. Beberapa sistem bahkan menggunakan *optical charater recogniton* pada gambar, atau melakukan *text extraction* pada dokumen elektronik. Hasil dari teks yang telah diekstraksi dapat digunakan untuk membantu pengguna dalam menemukan dokumen dengan mengidentifikasi kata kunci. Teks yang terekstraksi juga dapat disimpan sebagai komponen dari metadata, disimpan dengan gambar, atau disimpan secara terpisah sebagai sumber untuk mencari dokumen. |
| *Integration* | Banyak *document management system* berusaha untuk mengintegrasikan sistemnya langsung ke aplikasi lain, sehingga pengguna dapat mengambil dokumen yang ada secara langsung dari repositorinya, membuat perubahan, dan menyimpan dokumen yang telah dirubah kembali ke repositori sebagai versi yang baru tanpa meninggalkan aplikasi *document management system*. Integrasi tersebut umumnya tersedia untuk aplikasi perkantoran dan e-mail atau perangkat lunak kolaborasi atau *groupware*. |
| *Capture* | *Capture* melibatkan penerimaan dan pemrosesan gambar dari dokumen kertas ke pemindai (*scanner*) atau printer multifungsi. *Optical character recognition software* (OCR) sering digunakan, baik diintegrasikan dengan perangkat keras atau perangkat lunak yang berdiri sendiri (*stand-alone software*), untuk mengkonversi gambar digital ke dalam mesin teks yang dapat dibaca. *Optical mark recognition software* (OMR) kadang-kadang digunakan untuk mengekstrak isian kotak centang (*checkbox*) atau gelembung (*bubbles*) |
| *Validation* | *Visual validation registration system*. Contohnya kesalahan dokumen, tanda tangan yang hilang, kesalahan ejaan dapat dicetak pada dokumen atau gambar pada dokumen. |
| *Indexing* | *Indexing* dapat melacak dokumen elektronik. Meskipun hanya sesederhana melacak indeks dokumen yang unik tetapi *indexing* seringkali memiliki bentuk yang lebih kompleks seperti memberikan klasifikasi melalui metadata atau bahkan melalui indeks kata yang diekstrak dari isi dokumen. Fungsi utama *indexing* adalah untuk mendukung pengambilan (*retrieval*). Pembuatan index *topology* diperlukan untuk melakukan pengambilan cepat (*rapid retrieval*). |
| *Storage* | Menyimpan dokumen elektronik. Penyimpanan dokumen mencakup pengelolaan dokumen seperti: Di mana mereka disimpan, untuk berapa lama dokumen disimpan, migrasi dokumen dari satu media penyimpanan ke media penyimpanan lainnya dan pemusnahan dokumen akhir (*eventual document destruction*) |
| *Retrieval* | Mengambil dokumen dari storage. Meskipun gagasan mengambil dokumen tertentu sederhana, namun dalam pengambilan (*retrieval*) dalam konteks dokumen elektronik dapat menjadi sangat kompleks. Pengambilan dokumen tunggal secara sederhana dapat didukung dengan memungkinkan pengguna untuk menentukan indeks yang unik, |

| Komponen | Deskripsi |
|---|---|
| | memiliki sistem yang menggunakan indeks dasar (atau *non-indexed query* pada data store) untuk mengambil dokumen. Proses pengambilan dokumen yang lebih fleksibel memungkinkan pengguna untuk menentukan istilah pencarian parsial (*partial search terms*) yang melibatkan indeks dokumen dan/atau bagian dari metadata yang diharapkan. Dengan cara seperti ini, sistem akan memberikan daftar dokumen yang cocok dengan istilah pencarian (*search term*) pengguna. |
| *Distribution* | Dokumen yang diterbitkan untuk didistribusi harus memiliki format yang tidak dengan mudah diubah. Dokumen, dalam industri yang diatur oleh hukum, salinan asli dokumen tidak pernah digunakan untuk distribusi selain pengarsipan. Dokumen yang akan didistribusikan secara elektronik terlebih dulu harus divalidasi demikian pula sistem yang digunakan. |
| *Security* | Dalam *document management system* keamanan merupakan bagian penting. *Complience requirements* untuk dokumen-dokumen tertentu bisa saja sangat kompleks. Beberapa *document management system* memiliki modul manajemen hak yang memungkinkan administrator untuk memberikan akses ke dokumen berdasarkan kelompok orang tertentu atau *user group*. *Marking* (penandaan) pada dokumen saat pencetakan atau penciptaan PDF merupakan elemen penting untuk mencegah perubahan atau penggunaan yang tidak diinginkan. |
| *Workflow* | *Workflow* adalah proses yang kompleks dan *document management system* memiliki model alur kerja tersendiri (*built-in workflow module*). Ada berbagai jenis alur kerja. Penggunaannya tergantung pada lingkungan dimana *document management system* diterapkan. Panduan alur kerja mengharuskan pengguna untuk melihat dokumen dan memutuskan kepada siapa dokumen akan dikirim. Alur kerja berbasis aturan (*rule-based workflow*) memungkinkan administrator untuk membuat aturan yang mendikte aliran dokumen dalam organisasi: misalnya, faktur melewati proses persetujuan dan kemudian diteruskan ke departemen *account-payable*. Aturan yang dinamis memungkinkan dibuatnya cabang pada proses alur kerja. Contoh sederhananya adalah memasukan sejumlah faktur dan jika jumlahnya lebih rendah dari jumlah tertentu yang telah ditetapkan makan faktur tersebut akan mengikuti alur kerja organisasi yang berbeda. Mekanisme alur kerja yang canggih (*advance workflow mechanism*) dapat memanipulasi konten atau sinyal proses eksternal selagi aturan tersebut berjalan. |
| *Collaboration* | *Collaboration* harus melekat dalam *document management system*. Dalam bentuk dasarnya, *colabortive* DMS harus memungkinkan dokumen diambil dan dikerjakan oleh pengguna yang diizinkan (*authorized user*). Akses harus diblokir sementara untuk pengguna lain saat pekerjaan sedang dilakukan pada dokumen. Bentuk lain dari kolaborasi memungkinkan beberapa pengguna untuk melihat dan memodifikasi dokumen pada waktu yang bersamaan pada sesi kolaborasi. Dokumen yang dihasilkan harus dilihat dalam bentuk akhir, dan dalam waktu yang bersamaan juga menyimpan modifikasi yang dilakukan oleh tiap individu dalam sesi kolaborasi. |
| *Versioning* | *Versioning* adalah proses dimana dokumen masuk dan keluar diperiksa dalam *document management system*, yang memungkinkan pengguna untuk menggambil versi sebelumnya dan untuk melanjutkan pekerjaan dari titik acuan yang telah dipilih. *Versioning* sangat berguna bagi dokumen yang terus berubah dari waktu ke waktu dan yang memerlukan pembaharuan, tapi tetap dapat kembali atau mereferensi ke salinan sebelumnya. |
| *Searching* | Mencari dokumen dan berkas menggunakan atribut atau pencarian teks lengkap (*full text search*). Dokumen dapat dicari menggunakan berbagai atribut dan isi dokumen. |
| *Publishing* | *Document publishing* melibatkan prosedur *proofreading, public viewing, authorize, printing* dan *approving*. Penanganan yang tidak semestinya dapat menyebabkan ketidakakuratan dokumen. Dalam industri yang diatur oleh hukum beberapa prosedur harus dibuktikan oleh tanda tangan dan tanggal dimana okumen tersebut ditandatangani. Dokumen yang dipublikasikan harus dalam format yang tidak mudah diubah tanpa pengetahuan atau alat khusus. |

## III. Analisis Dan Evaluasi

### *A. Risk Identification*

Pada proses identifikasi risiko dilakukan pengelompokan risiko berdasarkan sumber daya TI, yang didefinisikan oleh COBIT, yang berhubungan dengan *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL.

Identifikasi yang dilakukan menghasilkan beberapa risiko yang mungkin terjadi pada setiap sumber daya TI yang dimiliki oleh PT. Jabar Telematika (JATEL) antara lain:

1. *Application*
   - *External Attacks*
   - *Malicious Code*
   - *Network Congestion*
   - *System Crash*
2. *Information*
   - *Database Failure*
   - *Data/Document Fraud*
3. *Infrastructure*
   - *Physical Damage*
   - *Hardware Failure*
   - *Power Outages*
   - *Force Majure*

4. *People*
   - *Inappropriate Access*
   - *Abuse of Position of Trus*
   - *Disgruntled Employees*

B. *Risk Assessment*

Pada proses ini dilakukan penilaian terhadap risiko yang terjadi *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL. Penilaian terhadap risiko merupakan gabungan proses yang terdiri dari *risk analysis* (analisis risiko) dan *risk evaluation* (evaluasi risiko).

Penilaian risiko terhadap risiko yang terjadi pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL dilakukan untuk mengevaluasi dan mengestimasi *level of risk* (tingkatan risiko) dari masing-masing risiko yang telah diidentifikasi pada proses identifikasi risiko dan menetapkan *acceptable level of risk* (tingkatan risiko yang dapat diterima) organisasi.

1. *Risk Analysis*

   Analisis risiko dilakukan untuk menentukan seberapa sering risiko pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL dapat terjadi dan seberapa besar dampak yang dihasilkan apabila risiko tersebut terjadi.

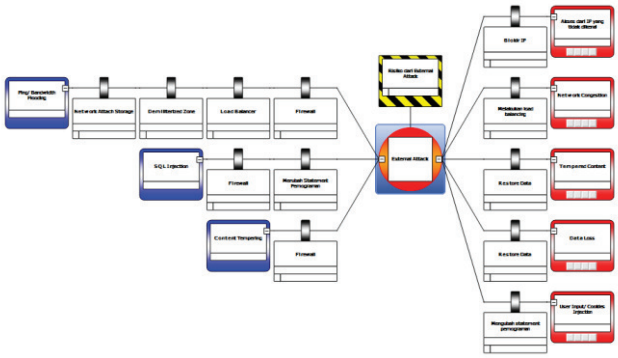
- *Bow-tie Analysis*

  *Bow-tie Analysis* dilakukan agar proses analisis terhadap risiko menghasilkan *recovery* (pemulihan) dan *control* (kontrol).

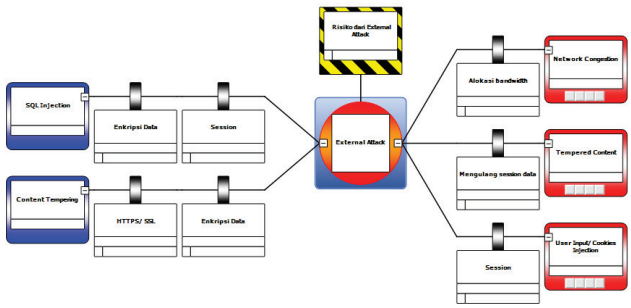
TABEL IV
TABEL *BOW-TIE ANALYSIS* PADA *EXTERNAL ATTACKS*

| Threats | Impact/ Consequences | Recovery | Control |
|---|---|---|---|
| *Ping Flooding* | *Bandwidth Consuming.* Aplikasi tidak dapat diakses. Akses dari IP yang tidak dikenal. *Network Congestion.* | Menghentikan *packet data* dari IP yang tidak dikenal. Memblokir akses dari IP yang tidak dikenal. Melakukan *load balancing.* Mengalokasikan *bandwidth.* | *Firewall. Load Balancer. Network Attach Storage* (NAS). *Demiliterized Zone* (DMZ). *Virtual Private Network* (VPN). |
| *Bandwidth Flooding* | | | |
| *SQL Injection* | Manipulasi Data. Pencurian Data. *User Input Injection. Cookies Injection.* | *Restore Data.* Mengubah *statement* pemograman. *Session.* | *Firewall.* Enkripsi Data. Merubah statement pemograman, *Session.* |
| *Content Tempering* | *Tempered Content.* | *Restore Data.* Mengulang *session data.* | |

Pada Tabel IV diketahui bahwa terdapat empat ancaman yang dapat menyebabkan kemungkinan terjadinya *external attacks* pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL, yaitu *ping flooding, bandwidth flooding, SQL Injection,* dan *Content Tempering*. Pada tabel yang sama dapat juga dilihat *impact/consequences, recovery,* dan *control* untuk *external attacks*.



Gambar 6 Diagram *Bow-tie Analysis* Pada *External Attacks*




Gambar 7 Diagram *Bow-tie Analysis* Usulan Pada *External Attacks*

Gambar 5 dan Gambar 6 merupakan diagram yang dihasilkan dari tabel *bow-tie analysis* pada kelompok risiko *external attacks*.

- Klasifikasi *Impact/Consequences* Pada Kelompok Risiko

  Pada tahap ini dilakukan klasifikasi *impact/ consequences* tiap kelompok risiko pada sumber daya IT yang mendukung penerapan *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL.

TABEL V
KLASIFIKASI *IMPACT/CONSEQUENCES* PADA KELOMPOK RISIKO DI SUMBER DAYA TI *APPLICATION*

| Kelompok Risiko | *Threats* | *Impact/ Consequences* | Klasifikasi |
|---|---|---|---|
| *External Attacks* | *Ping Flooding* | *Bandwidth Consuming* | *Performance* |
| | | Aplikasi tidak dapat diakses | *Availability* |
| | *Bandwidth Flooding* | Akses dari IP yang tidak dikenal | *Security* |
| | | *Network Congestion* | *Performance* |
| | *SQL Injection* | Manipulasi Data | *Security* |
| | | Pencurian Data | *Security* |
| | | *User Input Injection* | *Security* |
| | | *Cookies Injection* | *Security* |
| | *Content Tempering* | *Tempered Content* | *Security* |
| *Malicious Code* | *Trojan Horses* | *Data Loss* | *Availability* |
| | | *Backdoor Access* | *Security* |
| | | *Network Usage* | *Performance* |
| | | Adanya *Backdoor Programing* | *Security* |
| | *Worms* | Replikasi Data | *Security* |
| | | *Network Traffic* | *Performance* |
| | *Viruses* | Replikasi Data | *Security* |
| | | Manipulasi Data | *Security* |
| | | *Infected Areas* | *Security* |
| | *Phising* | Pencurian Data | *Security* |
| *Network Congestion* | *Slow Network Throughtput* | Layanan Terganggu | *Performance* |
| | | Aplikasi tidak bias diakses | *Availability* |
| | | *Bottleneck* | *Performance* |
| *System Crash* | *Application Crashes* | Aplikasi tidak dapat digunakan | *Availability* |
| | | *Data Loss* | *Availability* |
| | *Web Server Crashes* | Aplikasi/ web server tidak dapat diakses | *Availability* |
| | *Operation System Crashes* | *Kernel Panic* | *Availability* |

Pada Tabel V dapat dilihat klasifikasi yang dilakukan pada *impact/consequences* pada kelompok risiko yang terdapat di sumber daya TI *application.*

TABEL VI
KLASIFIKASI *IMPACT/CONSEQUENCES* PADA KELOMPOK RISIKO DI SUMBER DAYA TI *INFORMATION*

| Kelompok Risiko | *Threats* | *Impact/ Consequences* | Klasifikasi |
|---|---|---|---|
| *Database Failure* | *Statement Failure* | *Looping* | *Performance* |
| | | Memory Penuh | *Performance* |
| | | Data tidak tersimpan | *Compliance* |
| | *System Crash* | *Error Connection Database* | *Availability* |
| | | *Application Crashes* | *Availability* |
| | | *Web Server Crashes* | *Availability* |
| | | *Operation System Crashes* | *Availability* |
| | *Human Error* | Kesalahan Statement | *Performance* |
| | | Kesalahan Prosedur yang menyebabkan kerusakan | *Compliance* |
| | *Network Failure* | Data tidak tersimpan karena kerusakan *network interface controller* | *Compliance* |
| | | *Error Connection Database* | *Availability* |
| | *Media Failure* | Data tidak tersimpan karena ekstensi file tidak di *support* | *Compliance* |
| | | *Error Connection Database* | *Availability* |
| | *Disk Failure* | *Bad Hardisk Sector* | *Availability* |
| | *Corrupted File* | *Corrupted Data* | *Availability* |
| *Data/ Document Fraud* | *Content Tempering* | *Tempered Content* | *Availability* |
| | *Content Forging* | *Forged Content* | *Availability* |

Pada Tabel VI dapat dilihat klasifikasi yang dilakukan pada *impact/consequences* pada kelompok risiko yang terdapat di sumber daya TI *information.*

TABEL VII
KLASIFIKASI *IMPACT/CONSEQUENCES* PADA KELOMPOK RISIKO DI SUMBER DAYA TI *INFRASTRUCTURE*

| Kelompok Risiko | *Threats* | *Impact/ Consequences* | Klasifikasi |
|---|---|---|---|
| *Physical Damage* | Pencurian Terhadap *Physical Asset* | Ketidak tersediaan infrastruktur | *Availability* |
| | Kerusakan Terhadap *Physical Asset* | Kerusakan Aset | *Availability* |
| | | *Data Loss* | *Availability* |
| | *Water Damage* | Kerusakan Aset | *Availability* |
| | | *Data Loss* | *Availability* |
| | *Heat* | Hardware tidak aktif | *Availability* |
| | | *Corrupted Data* | *Availability* |

| Kelompok Risiko | *Threats* | *Impact/ Consequences* | Klasifikasi |
|---|---|---|---|
| | | *Data Loss* | *Availability* |
| *Hardware Failure* | *Electrical Dischagrge* | Korsleting | *Availability* |
| | | Kerusakan pada hardware/ modul | *Availability* |
| | | Sengatan Listrik | *Compliance* |
| | *Short Circuit* | Kerusakan pada hardware/ modul | *Availability* |
| | *Power Surges* | *Server Interupts* | *Availability* |
| | | *Hard Bad Sector* | *Availability* |
| | *Overheating* | Hardware tidak aktif | *Availability* |
| | | *Corrupted Data* | *Availability* |
| | | *Data Loss* | *Availability* |
| | *Bad Hardisk Sector* | *Hard Bad Sector* | *Availability* |
| | | *Soft Bad Sector* | *Performance* |
| | | *Corrupted Data* | *Availability* |
| | | *Data Loss* | *Availability* |
| | *Corrupted File* | *Corrupted Data* | *Availability* |
| | | *Data Loss* | *Availability* |
| | *Human Error* | Kerusakan Hardware | *Availability* |
| | | *Data loss* | *Availability* |
| *Power Outage* | *Power Cut/ Power Blackout/ Power Failure* | Ketidak tersediaan Infrastruktur | *Availability* |
| *Force Majure* | Bencana Alam | Kerusakan Infrastruktur | *Availability* |
| | | Kerusakan Hardware | *Availability* |
| | | *Data Loss* | *Availability* |

Pada Tabel VII dapat dilihat klasifikasi yang dilakukan pada *impact/consequences* pada kelompok risiko yang terdapat di sumber daya TI *infrastructure.*

TABEL VIII
KLASIFIKASI *IMPACT/CONSEQUENCES* PADA KELOMPOK RISIKO DI SUMBER DAYA TI *PEOPLE*

| Kelompok Risiko | Threats | Impact/ Consequences | Klasifikasi |
|---|---|---|---|
| *Inappropriate Access* | *Unauthorized Access/ Man in The Middle* | Pencurian Data | *Security* |
| | | Manipulasi Data | *Security* |
| | | Akses yang tidak diinginkan | *Security* |
| *Abuse of Position of Trust* | *Inappropriate Access* | Manipulasi Data | *Security* |
| | | Perubahan Konfigurasi | *Security* |
| | *Content Tempering* | *Tempered Content* | *Security* |
| | *Content Forging* | *Forged Content* | *Security* |
| | Penyebaran Informasi | Tersebarnya informasi rahasia | *Compliance* |
| *Disgruntled Employees* | *Unauthorized Access* | Manipulasi Data | *Security* |
| | | Perubahan Konfigurasi | *Security* |
| | Penyebaran Informasi | Tersebarnya Informasi Rahasia | *Compliance* |
| | Lemahnya Pengetahuan Terhadap Aplikasi | *Output* dari aplikasi tidak optimal | *Performance* |

Pada Tabel VIII dapat dilihat klasifikasi yang dilakukan pada *impact/consequences* pada kelompok risiko yang terdapat di sumber daya TI *people.*

- *Qualitative* dan *Semi-Quantitative Analysis*

*Qualitative* dan *semi-quantitative analysis* dilakukan dengan memberikan nilai pada tiap risiko yang telah teridentifikasi berdasarkan *likelihood* dan *impact*.

Pada Tabel IX dan Tabel X dapat dilihat kriteria penilaian untuk risiko yang telah teridentifikasi dengan menggunakan metode *qualitative* dan *semi-quantitative analysis.*

TABEL IX
NILAI PADA *LIKELIHOOD*

| *Likelihood* | | Frekuensi per Tahun |
|---|---|---|
| *Rating* | Kriteria | |
| 1 | *Rare* | ≤ 5 Kejadian |
| 2 | *Unlikely* | 6 – 10 Kejadian |
| 3 | *Possible* | 11 – 20 Kejadian |
| 4 | *Likely* | 21 – 40 Kejadian |
| 5 | *Almost Certain* | ≥ 41 kejadian |

TABEL X
NILAI PADA *IMPACT*

| *Impact* | | Deskripsi |
|---|---|---|
| *Rating* | Kriteria | |
| 1 | *Insignificant* | Dampak mungkin diabaikan dengan aman. |
| 2 | *Minor* | Dampak kecil dan dapat diatasi dengan prosedur sederhana |
| 3 | *Moderate* | Dampak tergolong besar, namun dapat dikelola dengan menggunakan prosedur tertentu |
| 4 | *Major* | Dampak besar, berpotensi pada *financial cost* dan terhambatnya kinerja organisasi |
| 5 | *Catastrophic* | Dampak ekstrim, berpotensi pada *large financial cost* dan terhentinya kinerja organisasi, serta dampak pada reputasi organisasi |

*e-ISSN: 2443-2229*

Setelah menentukan nilai pada *likelihood* dan *impact* maka penilaian pada masing-masing risiko yang telah didefinisikan pada proses sebelumnya dapat dilakukan. Penilaian risiko berdasarkan nilai *likelihood* dan *impact* secara detail dapat dilihat pada Tabel XI dan Tabel XII.

TABEL XI
IDENTIFIKASI *LIKELIHOOD* DAN *IMPACT*

| No | Identifikasi Risiko | *Likelihood* | *Impact* |
|---|---|---|---|
| 1 | *External Attacks* | *Rare* | *Moderate* |
| 2 | *Malicious Code* | *Rare* | *Minor* |
| 3 | *Physical Damage* | *Rare* | *Moderate* |
| 4 | *Inappropriate Access* | *Rare* | *Major* |
| 5 | *Hardware Failure* | *Rare* | *Minor* |
| 6 | *Power Outages* | *Possible* | *Moderate* |
| 7 | *Database Failure* | *Rare* | *Moderate* |
| 8 | *Force Majure* | *Rare* | *Catastrophic* |
| 9 | *Network Congestion* | *Possible* | *Moderate* |
| 10 | *System Crash* | *Rare* | *Minor* |
| 11 | *Data/Documen Fraud* | *Rare* | *Major* |
| 12 | *Abuse of Position of Trust* | *Rare* | *Major* |
| 13 | *Disgruntled Employees* | *Unlikely* | *Minor* |

TABEL XII
PENILAIAN *LIKELIHOOD* DAN *IMPACT*

| No | Identifikasi Risiko | *Likelihood* | *Impact* |
|---|---|---|---|
| 1 | *External Attacks* | 1 | 3 |
| 2 | *Malicious Code* | 1 | 2 |
| 3 | *Physical Damage* | 1 | 3 |
| 4 | *Inappropriate Access* | 1 | 4 |
| 5 | *Hardware Failure* | 1 | 2 |
| 6 | *Power Outages* | 3 | 3 |
| 7 | *Database Failure* | 1 | 3 |
| 8 | *Force Majure* | 1 | 5 |
| 9 | *Network Congestion* | 3 | 3 |
| 10 | *System Crash* | 1 | 2 |
| 11 | *Data/Documen Fraud* | 1 | 4 |
| 12 | *Abuse of Position of Trust* | 1 | 4 |
| 13 | *Disgruntled Employees* | 1 | 2 |

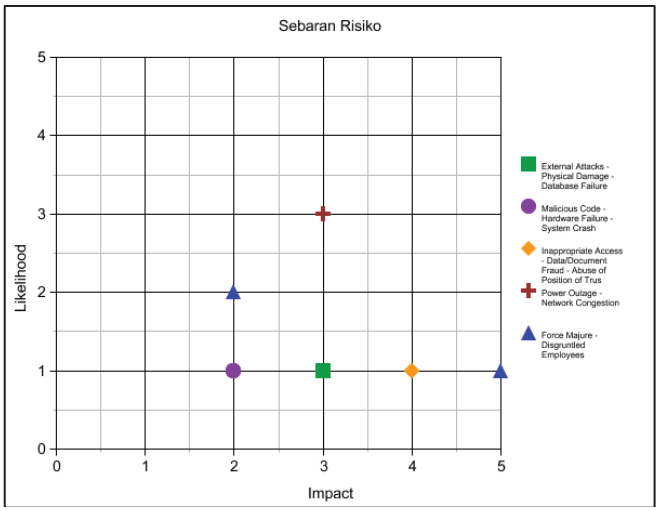
2. *Risk Evaluation*

Pada tahap evaluasi risiko, risiko yang telah teridentifikasi dievaluasi apakah risiko tersebut dapat ditoleransi atau tidak berdasarkan *level of risk* atau tingkatan risiko. Apabila risiko yang telah dinilai masuk kedalam kriteria yang ditetapkan maka risiko tersebut harus mendapatkan *treatment* (perlakuan) sebaliknya apabila risiko tidak termasuk kedalam kriteria yang ditetapkan maka perlakuan terhadap risiko tidak perlu dipertimbangkan lagi.

Evaluasi risiko dilakukan dengan menerapkan proses *mapping* pada grafik (x, y) yang menggambarkan hubungan antara *likelihood* atau frekuensi kejadian dan *impact* atau dampak yang diakibatkan oleh tiap-tiap risiko yang terjadi.

TABEL XIII
MATRIKS EVALUASI RISIKO

| *Likelihood* | | | | | |
|---|---|---|---|---|---|
| 5 | Medium | Medium | High | High | High |
| 4 | Low | Medium | Medium | High | High |
| 3 | Low | Medium | Medium | Medium | High |
| 2 | Low | Low | Medium | Medium | High |
| 1 | Low | Low | Low | Medium | Medium |
| | 1 | 2 | 3 | 4 | 5 |
| | | | *Impact* | | |




Gambar 8 Grafik Sebaran Risiko Berdasarkan *Likelihood* dan *Impact*

Grafik hasil evaluasi tersebut dikategorikan menjadi 3 tingkatan *level of risk* yaitu, *low, medium,* dan *high* berdasarkan matriks evaluasi risiko. Matriks evaluasi risiko dapat dilihat pada Tabel XIII, sedangkan sebaran risiko berdasarkan *likelihood* dan *impact* dapat dilihat pada Gambar 10.

TABEL XIV
MATRIKS EVALUASI RISIKO BERDASARKAN *LIKELIHOOD* DAN *IMPACT*

| *Likelihood* | | | | | |
|---|---|---|---|---|---|
| 5 | | | | | |
| 4 | | | | | |
| 3 | | | R6, R9 | | |
| 2 | | R13 | | | |
| 1 | | R2, R5, R10 | R1, R3, R7 | R4, R11 R12 | R8 |
| | 1 | 2 | 3 | 4 | 5 |
| | | | *Impact* | | |

Keterangan:

| | |
|---|---|
| R: Risiko | R7: *Database Failure* |
| R1: *External Attacks* | R8: *Force Majure* |
| R2: *Malicious Code* | R9: *Network Congestion* |
| R3: *Physical Damage* | R10: *System Crash* |
| R4: *Inappropriate Access* | R11: *Data/Document Fraud* |
| R5: *Hardware Failure* | R12: *Abuse of Position of Trust* |
| R6: *Power Outage* | R13: *Disgruntled Employees* |

Tabel XIV – Matriks Evaluasi Risiko Berdasarkan *Likelihood* dan *Impact* memperlihatkan pengelompokan risiko berdasarkan kategori evaluasi *level of risk* risiko. Secara lebih lengkap evaluasi risiko berdasarkan *level of risk* dapat dilihat pada Tabel XV. Berdasarkan Sebaran Risiko dan *Likelihood-Impact* yang merupakan hasil penggabungan dari *mapping* grafik sebaran risiko dan matriks evaluasi risiko berdasarkan *likelihood* dan *impact.*

TABEL XV
EVALUASI *LEVEL OF RISK* BERDASARKAN SEBARAN RISIKO DAN *LIKELIHOOD-IMPACT*

| No | Identifikasi Risiko | *Likelihood* | *Impact* | *Level of Risk* |
|---|---|---|---|---|
| 1 | *External Attacks* | 1 | 3 | *Low* |
| 2 | *Malicious Code* | 1 | 2 | *Low* |
| 3 | *Physical Damage* | 1 | 3 | *Low* |
| 4 | *Inappropriate Access* | 1 | 4 | *Medium* |
| 5 | *Hardware Failure* | 1 | 2 | *Low* |
| 6 | *Power Outages* | 3 | 3 | *Medium* |
| 7 | *Database Failure* | 1 | 3 | *Low* |
| 8 | *Force Majure* | 1 | 5 | *Medium* |
| 9 | *Network Congestion* | 3 | 3 | *Medium* |
| 10 | *System Crash* | 1 | 2 | *Low* |
| 11 | *Data/Documen Fraud* | 1 | 4 | *Medium* |
| 12 | *Abuse of Position of Trust* | 1 | 4 | *Medium* |
| 13 | *Disgruntled Employees* | 1 | 2 | *Low* |

Dari Tabel X dapat dilihat bahwa dari 13 kelompok risiko yang terjadi di *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di JATEL 6 diantaranya memiliki *level of risk medium* sedangkan sisanya berada pada l*ow level of risk*. Risiko yang termasuk ke dalam *medium level of risk* meliputi *innapropriate access, power outage, force majure, network congestion, data/document fraud,* dan *abuse of position of trust.* Sedangkan risiko yang termasuk ke dalam *low level of risk* adalah *external attacks, malicious code, physical damage, hardware failure, database failure, system crash,* dan *disgruntled employees.*

3. *Risk Treatment*
Pada tahap ini dapat dilihat tindakan yang dilakukan oleh PT. Jabar Telematika (JATEL) dalam mengatasi risiko yang telah teridentifikasi pada aplikasi *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) dan memiliki *medium level of risk*. Pada tahap ini juga ditentukan usulan strategi perlakuan risiko yang tepat dalam mengatasi permasalahan yang sesuai dengan pembahasan ini yaitu dengan *risk prevention* (pencegahan risiko).
Berikut *Organization Risk Treatment* yang dilakukan oleh PT. Jabar Telematika (JATEL):

TABEL XVI
PENANGGULANGAN RISIKO DI JATEL

| ***Organization Risk Treatment*** | | | |
|---|---|---|---|
| **No.** | **Identifikasi Risiko** | ***Threats*** | ***Treatment* di JATEL** |
| 1 | *Inappropriate Access* | *Unauthorized Access* | Dari sisi internal terdapat prosedur *authentication, authorization,* dan *Log System.* Sedangkan dari sisi eksternal terdapat *firewall, NAS,* dan *DMZ.* Juga terdapat *Backup Scheduling.* |
| | | *Man in The Middle* | Dengan memblokir akses dari IP yang tidak diinginkan dan memberikan *password* pada *access point* dan *router.* |
| 2 | *Power Outage* | *Power Cut/ Power Blackout/ Power Failure* | Penggunaan UPS atau *Uninterruptible Power Supply* dan penggunaan *Power Generator.* |
| 3 | *Force Majure* | Bencana Alama | Melakukan aset evakuasi berupa *backup data.* |
| 4 | *Network Congestion* | *Slow Network Througput* | Memindahkan *link* utama ke *link backup.* Mengatasi *bottleneck* dan mengalokasikan *bandwidth.* |
| 5 | *Data/ Document Fraud* | *Content Tempering* | Masih terbatas pada prosedur *authentication* dan *authorization* serta *workflow.* |
| | | *Content Forging* | |
| 6 | *Abuse of Position of Trust* | Penyebaran Informasi Rahasia | Mencoba menghapus informasi yang tersebar sedangkan secara aplikasi terdapat prosedur *authentication, authorization,* dan *log system.* |

Pada Tabel XVI dapat dilihat cara penanggulangan risiko yang terjadi pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) yang dilakukan oleh JATEL. *Treatment* yang dilakukan oleh organisasi dalam memperlakukan risiko masih terbatas pada penanganan yang dilakukan apabila risiko tersebut terjadi dan perlakuan terhadap risiko tersebut hanya mengurangi konsekuensi dari risiko.

Setelah melihat cara penanggulangan yang dilakukan oleh JATEL, maka dibuatkan usulan untuk organisasi dalam memperlakukan risiko (*risk treatment*) yang memiliki fungsi untuk mencegah terjadinya risiko dan mengurangi secara substansial kemungkinan terjadinya risiko serta memberikan fungsi kontrol terhadap risiko.

TABEL XVII
USULAN *RISK TREATMENT*

| **Usulan *Organization Risk Treatment*** | | | |
|---|---|---|---|
| **No.** | **Identifikasi Risiko** | ***Threats*** | **Usulan *Risk Treatment*** |
| 1 | *Inappropriate Access* | *Unauthorized Access*<br>*Man in The Middle* | Menerepkan *Safety IT Procedure* seperti; mengakhiri setiap akses, melindungi pc dan *terminals* dengan *password*. Menerapkn *Policy on Use of Network Services* seperti; hanya *user* dan *third parties* yang memeliki *user-id* yang dapat *log-on* kedalam sistem, tidak diizinkan melakukan aktifitas ilegal pada computer dan penggunaan computer harus di monitor oleh organisasi. |
| 2 | *Power Outage* | *Power Cut/ Power Blackout/ Power Failure* | Penggunaan 2 sumber listrik dari gardu yang berbeda untuk keperluan operasional dan infrastruktur jaringan. Serta menerapkan *Data Center Tier.* |
| 3 | *Force Majure* | Bencana Alam | Penerapan *Disaster Recovery System* atau *Disaster Recovery Procedure* juga dengan menerapkan *Data Center Tier*. |
| 4 | *Network Congestion* | *Slow Netrwork Troughput* | Melakukan monitoring *bandwidth*, dengan monitoring *bandwidth* penyempitan akses dapat dicegah dengan mengalokasikan *bandwidth* pada utilitas yang lebih besar. |
| 5 | *Data/Document Fraud* | *Content Tempering*<br>*Content Forging* | Penggunaan HTTP/SLL yang didalamnya terdapat *Secure Socket Layer* (SLL) atau *Transport Layer Security* (TLS). Juga penerapan enkripsi data serta *checksum* untuk mencegah manipulasi konten. |
| 6 | *Abuse of Position of Trust* | Penyebaran informasi rahasia | Adanya prosedur pencegahan seperti; perlindungan dokumen organisasi, pemberian sanksi, dan dengan adanya kontrol dan audit sistem informasi. |

Pada Tabel XVII dapat dilihat usulan strategi perlakuan terhadap risiko (*risk treatment*) untuk organisasi yang memiliki fungsi untuk mencegah terjadinya risiko (*risk prevention*) dan mengurangi secara substansial kemungkinan terjadinya risiko serta memberikan fungsi kontrol terhadap risiko.

## IV. SIMPULAN DAN SARAN

Berdasarkan hasil analisis manajemen risiko teknologi infotmasi (TI) pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di PT. Jabar Telematika (JATEL), terdapat beberapa poin penting yang dapat disimpulkan dari uraian yang telah disampaikan, diantaranya:

1. Proses analisis manajemen risiko teknologi informasi terdiri dari *risk identification, risk assessment,* dan *risk treatment* dapat mengidentifikasi risiko, memberikan penilaian terhadap risiko serta memberikan perlakuan

yang lebih baik terhadap risiko yang mungkin terjadi pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di PT. Jabar Telematika (JATEL).

2. Dari hasil analisis pada aplikasi *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di PT. Jabar Telematika (JATEL) diketahui bahwa terdapat 13 risiko (*external attacks, malicious code, network congestion, system crash, database failure, data/document fraud, physical damage, hardware failure, power outage, force majure, inappropriate access, abuse of position of trust, dan disgruntled employees*) yang teridentifikasi dapat dikelompokan berdasarkan sumber daya TI (*application, information, infrastructure, dan people*) dan dapat diklasifikasikan *impact/consequences*nya berdasarkan *risk classification* (*security, availability, performance dan compliance*). Dari risiko yang telah teridentifikasi, 6 diantaranya pada grafik sebaran risiko dan evaluasi risiko berdasarkan *likelihood* dan *impact* diketahui memiliki tingakatan medium *level of risk.*
3. Penanganan organisasi terhadap risiko yang terjadi pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) secara umum sudah dilakukan dan dapat dikatakan sudah baik hanya saja PT. Jabar Telematika (JATEL) tidak memiliki dokumen *Standard Operational Procedure* atau SOP yang berhubungan dengan manajemen risiko TI di organisasi. Strategi penanganan terhadap risiko yang memiliki fungsi kontrol dan mencegah terjadinya risiko (*risk prevention*) secara substantif dianggap sebagai strategi penanganan risiko yang paling baik. Penerapan *Data Center Tier* dan *Disaster Recovery Procedure* atau DRP juga memegang peranan penting pada implementasi manajemen risiko.

Lalu, berdasarkan hasil analisis manajemen risiko TI yang dilakukan pada aplikasi DMS arsip elektronik di JATEL, terdapat beberapa poin saran yang dapat diuraikan untuk pengembangan analisis manajemen risiko TI dan *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di PT. Jabar Telematika (JATEL), diantaranya:

1. Diharapkan dengan adanya hasil analisis manajemen risiko TI pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di PT. Jabar Telematika (JATEL) dapat dijadikan dokumen inisiasi atau dokumen acuan oleh JATEL dalam mengembangkan *standard operation procedure* (SOP), strategi manajemen risiko, serta *disaster recovery plan* (DRP) sehingga dapat diimplementasikan oleh organisasi.
2. Dengan mengimplementasikan usulan risk treatment dan melanjutkan analisis manajemen risiko hingga tahap *monitoring and review* diharapkan nantinya nilai *lavel of risk* pada tiap-tiap risiko yang terjadi pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) dapat menurun dan organisasi dapat menghasilkan strategi penanganan risiko yang lebih baik.
3. Adanya pengembangan *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di PT. Jabar Telematika (JATEL) sehingga semua komponen *document management system* dapat terpenuhi. Komponen yang dimaksud adalah *capture, validation,* dan *collaboration* yang diharapkan dapat meningkatkan kinerja aplikasi dan *business value* dari JATEL serta mendukung otomatisasi proses bisnis.
4. Penerapan HTTPS/SLL, enkripsi, *session* dan *masking* yang dapat memberikan dukungan terhadap *security* pada *document management system* arsip elektronik ADEL (Aplikasi Dokumen Elektronik) dan NADINE (Naskah Dinas Elektronik) di PT. Jabar Telematika (JATEL)

## DAFTAR PUSTAKA

[1] A. Stevenson, Oxford Dictionary of English, Oxford: Oxford University Press, 2010.
[2] P. Hopkin, Fundamentals of Risk Management: Understanding, Evaluating, and Implementing Effective Risk Management, London: Kogan Page, 2010.
[3] J. J. Hampton, Fundamentals of Enterprise Risk Management: How Top Companies Assess Risk, Manage Exposures, and Seize Opportunities, New York: AMACOM, 2009.
[4] D. Cooper, S. Grey, G. Raymond and P. Walker, Project Risk Management Guidelines: Managing Risk in Large Projects and Complex Procurements, Chichester, West Sussex: John Wiley & Sons Ltd., 2004.
[5] L. J. Susilo and V. R. Kaho, Panduan Manajemen Risiko Berbasis ISO 31000 Industri Non-Perbankan, Jakarta: Penerbit PPM, 2014.
[6] N. R. Council, Improving Risk Communication, Washington DC: National Academy Press, 1989.
[7] Symantec, IT Risk Management Report, Cupertino, CA: Symantec, 2007.
[8] ISACA, COBIT 5 The Risk IT Framework: Principles, Process Details, Management Guidelines, Maturity Models, Rolling Meadows, IL: ISACA, 2009.
[9] ISACA, IT Governance Implementation Guide: Using COBIT and val ITTM, 2nd edition, ISACA, 2007.
[10] JATEL, PT Jabar Telematika: Annual Report 2013, Bandung: PT Jabar Telematika, 2013.
[11] E. E. Pratama and Suhardi, Analisis Nilai & Manajemen Risiko Teknologi Informasi (studi kasus PT. Bank Tabungan Negara), Bandung, 2013.
[12] N. B. Kurniawan, Manajemen Risiko Teknologi Informasi Pada Badan Pusat Statistik, Produk Layanan: Pelayanan Statistik Terpadu, Bandung, 2013.
[13] A. Y. Dewi, Analisis Nilai Teknologi Informasi & Implementasi ISO 31000 Sebagai Manajemen Risiko Teknologi Informasi (Studi Kasus Layanan Pada Direktorat Jendral Pajak Republik Indonesia), Bandung, 2013.

**Nama : Rahmad Kartolo**
**NIM : 182420119**
**Kelas : MTI REGULER B**

“JELASKAN BAGAIMANA KONSEP IT RISK MANAGEMENT PADA ITSM

BERIKAN CONTOH KASUS (JURNAL) “

# Konsep Risiko

Risiko, seperti telah dijelaskan pada bagian sebelumnya, suatu kondisi atau kejadian yang tidak pasti yang bila terjadi dapat memberikan dampak negatif maupun positif. Risiko terjadi secara kumulatif dan dapat mempengaruhi sebuah objektif

Gambar 2 *Concept of Risk* [3]

Berdasarkan Gambar 2 tentang konsep Risiko maka dapat diketahui level of risk (tingkatan risiko). Berdasarkan variabel yang digunakan, probability dan impact, maka level of risk dapat diklasifikasikan sebagai berikut :

**1.Low Probability Low Impact = Low Risk.**

Risiko ini adalah risiko dengan tingkat pengaruh yang paling kecil dibandingkan dengan risiko lainya sehingga, dengan kebijakan tertentu, risiko ini dapat diabaikan.

**2. Low Probability High Impact = Moderate Risk.**

Risiko dengan tingkat pengaruh menengah, meskipun begitu risko ini harus dimonitor dan membutuhkan penanganan yang berkelanjutan tergantung dari dampak yang diberikan.

**3. High Probability Low Impact = Moderate Risk.**

Risiko dengan tingkat pengaruh menengah. Berbeda dengan low probability high impact risiko ini hanya perlu dimonitor.

**4. High Probability High Impact = High Risk.**

Risiko dengan pengaruh yang paling tinggi dibandingkan dengan lainnya. Merupakan risiko berbahaya yang harus diatasi secepatnya.

# Pengertian Manajemen Risiko

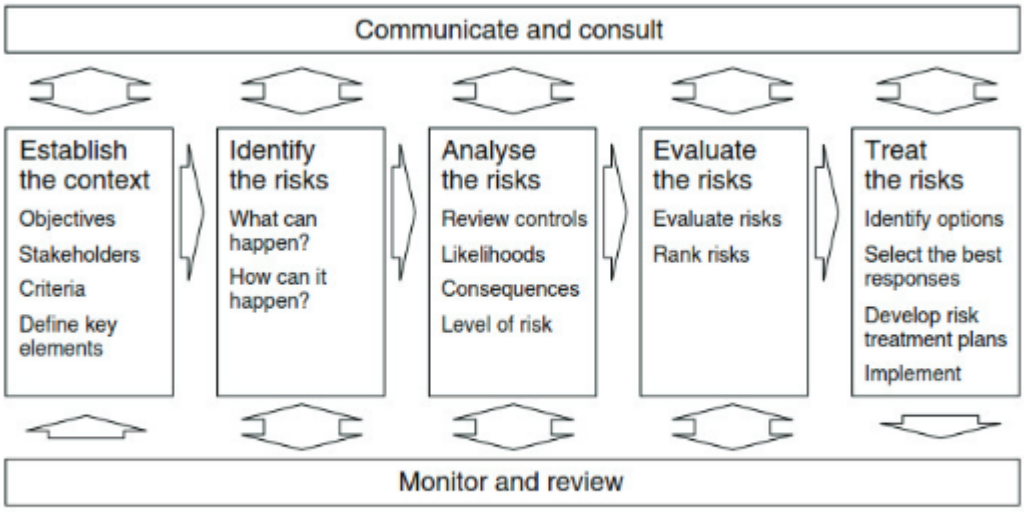
Manajemen risiko mengacu pada budaya, proses dan struktur yang diarahkan pada pengelolaan ketidakpastian .Proses pada manajemen risiko terjadi secara sistematis, terus menerus dan diterapkan dalam segala aspek Dalam konteks organisasi, manajemen risiko diterapkan dalam seluruh bidang yang terdapat dalam organisasi tersebut.

TABEL II
*DEFINITION OF RISK MANAGEMENT* [2]

| Organization | Definition of risk management |
|---|---|
| ISO Guide 73<br>BS 31100 | Coordinated activities to direct and control an organization with regard to risk |
| Institute of Risk Management (IRM) | Process which aims to help organizations understand, evaluate and take action on all their risks with a view to increasing the probability of success and reducing the likelihood of failure |
| HM Treasury | All the processes involved in identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress |
| London School of Economics | Selection of those risks a business should take and those which should be avoided or mitigated, followed by action to avoid or reduce risk |
| Business Continuity Institute | Culture, processes and structures that are put in place to effectively manage potential opportunities and adverse effects |

## Proses Manajemen Risiko

Proses pada manajemen risiko melibatkan pengaplikasian secara sistematis dari pengelolaan kebijakan, proses dan prosedur hingga proses dalam penentuan konteks, mengidentifikasi, menilai, memperlakukan, mengamati, dan mengkomunikasikan risiko




Gambar 3 *Risk Management Process* [4]

Proses dari manajemen risiko berfungsi membantu dalam melakukan pengambilan keputusan yang lebih baik dan meningkatkan efisiensi. Meskipun banyak cara dalam menggambarkan proses manajemen risiko, langkah-langkah dasar yang terdapat dalam proses ini hampir serupa dan biasanya mencakup tiga langkah utama yaitu: risk identification,risk assessment, dan risk treatment

**1.Risk Identification**

Risk identificationbmerupakan proses dalam menentukan apa, bagaimana, dan mengapa suatu kondisi atau kejadian dapat terjadi. Proses identifikasi risiko harus dilakukan secara komprehensif, harus terstruktur berdasarkan faktor-faktor utama agar nantinya risiko dapat dinilai secara sistematis . Risiko dapat diidentifikasi melalui beberapa metodeseperti; checklist, interview atau focused group discussion dan questionnaries. Checklist digunakan untuk menyederhanakan proses identtifikasi risiko. Checklist juga dirancang untuk menghindari atau meminimalkan risiko, seringkali checklist merupakan bagian dari prosedur dokumentasi dan jaminan kualitas organisasi. Questionnaries atau kuesioner merupakan instrumen penelitian yang terdiri dari serangkaian pertanyaan dan petunjuk lainnya dengan tujuan untuk mengumpulkan informasi tertentu dari responden.

**2. Risk Assesment**

Risk assesmentmerupakan keseluruhan proses dari risk analysis dan risk evaluation. Risk analysis adalah proses sistematis dalam menggunakan informasi yang ada untuk menentukan seberapa sering risiko dapat terjadi dan seberapa besar dampak yang dihasilkan bila risiko tersebut terjadi . Proses penilaian risiko pada risk analysis dapat dilakukan dengan metode seperti;

bow-tie analysis, qualitative analysis, dan semi-quantitative analysis. Sedangkan risk evaluation adalah proses dalam membandingkan risiko yang telah diperkirakan dengan kriteria risiko yang telah ditentukan . Evaluasi risiko memperhitungkan apakah risiko dapat ditoleransi atau tidak didasarkan pada level of risk (tingkatan risiko) pada matriks risiko. Bow-tie analysis pada risk analysis merupakan metode analisis yang digunakan untuk menggambarkan kegiatan manajemen risiko agar lebih mudah dimengerti dan diakses.

Gambar 4 *Bow-tie Analysis*

**3. Risk Treatment**

Risk treatment bertujuan untuk menentukan tindakan yang dilakukan dalam mengatasi risiko yang telah teridentifikasi, guna mengurangi pengaruh risiko secara keseluruhan . Risk treatment merubah analisis sebelumnya, risk identification dan risk assessment, menjadi tindakan substantif untuk mengurangi risiko.

Terdapat beberapa risk treatment yang umumnya digunakan, yaitu; risk prevention (pencegahan risiko) dengan tujuan untuk mengurangi secara substansial kemungkinan terjadinya risiko, risk mitigation (mitigasi risiko) dengan tujuan untuk meminimalkan konsekuansi dari risiko, risk sharing (berbagi risiko) dengan tujuan untuk memindahkan risiko tidak hanya ke organisasi lain namun juga ke entitas bisnis ataupin individu, dan risk retention (retensi risiko) atau dikenal juga sebagai penyerapan, toleransi, atau penerimaan risiko.

- **Risk Management Framework**

Secara umum diakui bahwa risk management framework(kerangka kerja manajemen risiko) merupakan dokumenyang menghasilkan informasi pada proses manajemen risiko. Dalam banyak kerangka kerja manajemen risiko, aktivitas manajemen risiko harus dilakukan dalam konteks lingkungan bisnis, organisasi dan risiko yang dihadapi oleh organiasi. Agar konteks dapat dijelaskan dan didefinisikan, kerangka kerja diperlukan dalam mendukung prosesnya [2]. Berikut merupakan risk management framework yang digunakan dalam penelitian:

***1.Symantec: Risk Management Report***

Teknologi Informasi (TI) secara luas dan mendalam telah menjadi saling berhubungan dengan operasi bisnis, risiko TI sendiri pun telah tumbuh menjadi bagian dari keseluruhan komponen operasional

Gambar 5 *IT Risk Classification* [7]

Untuk membantu organisasi dalam memahami dan menganalisa risiko TI dan mengatur strategi mitigasi, maka dibuat framework (kerangka kerja) klasifikasi risiko berdasarkan dampaknya terhadap organisasi. Kerangka kerja tersebut mengklasifikasikan risiko TI sebagai [7]:

- ✓ **Security Risk atau risiko keamanan** – bahwa informasi dapat dirubah, diakses atau digunakan oleh pihak yang tidak bertanggung jawab.
- ✓ **Availability Risk atau risiko ketersediaan** – bahwa informasi atau aplikasi tidak dapat diakses karena system failure (kegagalan sistem) atau bencana alam, termasuk masa pemulihan (recovery).
- ✓ **Performance Risk atau risiko kinerja** – bahwa kinerja yang kurang dari system, aplikasi, personil, atau TI secara keselruhan, dapat mengurangi produktivitas atau nilai bisnis. oCompliance Risk atau risiko pemenuhan – bahwa penanganan atau pengolahan informasi gagal memenuhi peraturan, TI atau persyaratan kebijakan bisnis (business policy requirements).

***2. COBIT 5 for Risk***

COBIT adalah kerangka kerja (framework) yang dibuat oleh ISACA untuk manajemen teknologi informasi (TI)dan tata kelola IT. COBIT adalah toolset yang memungkinkan penggunanya untuk menjembatani kesenjangan antara kebutuhan kontrol, masalah teknisdan risiko bisnis .

Sumber daya TI yang diidentifikasikan dalam COBIT dapat dijelaskan secara singkat sebagai berikut :

- ✓ **Aplikasi (Application**), merupakan suatu sarana atau toolyang digunakan untuk mengolah dan menyimpulkan atau meringkas, baik prosedur manual maupun yang terprogram.

- ✓ **Informasi (Information)**, adalah data-data yang telah diolah untuk kepentingan manajemen dalam membantu mengambil keputusan dalam menjalankan roda bisnisnya. Data-data terdiri obyek-obyek dalam pengertian yang lebih luas (yakni internal dan eksternal), terstruktur dan tidak terstruktur, grafik, suara dan sebagainya.
- ✓ **Infrastruktur (infrastructure),** mencakup hardware, software, sistem operasi, sistem manajemen database, jaringan (networking), multimedia, dan fasilitas-fasilitas lainnya.
- ✓ **Sumber Daya Manusia/SDM (People),** merupakan sumber daya yang paling penting bagi organisasi dalam pengelolaan dan operasionalisasi bisnis organisasi.Kesadaran dan produktivitasnya dibutuhkan untuk merencanakan, mengorganisasikan, melaksanakan, memperoleh, menyampaikan, mendukung, dan memantau layanan TI organisasi.

## Document Management System

Manajemen dokumen, sering disebut sistem manajemen dokumen atau Document Management System (DMS), adalah penggunaan sistem komputer dan perangkat lunak untuk menyimpan, mengelola, dan untuk melacak dokumen elektronik dan gambar elektronik dari informasi berbasis kertas

# PENERAPAN MANAJEMEN RESIKO OPERASIONAL PADA PT. BANK PEMBANGUNAN DAERAH SUMATERA BARAT CABANG PAINAN KABUPATEN PESISIR SELATAN

**Zico Prasetyo, Afriyeni**
Akademi Keuangan dan Perbankan Padang
Afriyeni.yen@gmail.com

***ABSTRACT***

*The research purpose is to understand the effectiveness of operational risk management on PT. Bank Pembangunan Daerah Sumatera Barat Branch Painan in accordance with the regulation of Bank Indonesia No. 11/25/PBI/2009 about the risk management application on the public bank. The research using descriptive qualitative method by present the of risk management application in a company. The data used are primary data that collected from interview method and the secondary data is action plan of PT. Bank Pembangunan Daerah Sumatera Barat Branch Painan. The research result show that the policy and the procedure and the strategy that applied PT. Bank Pembangunan Daerah Sumatera Barat Branch Painan in risk management application is effective according to the minimal standard of Bank Indonesia and adjusted according to the bank scope of business.*

***Keywords** : Risk Management, Operational Risk*

## LATAR BELAKANG

Dalam perbankan, baik bank sentral maupun bank umum semakin menyadari bahwa untuk meminimalkan resiko, maka praktek manajemen resiko *(risk management)* dan tata kelola perusahaan yang baik *(good corporate governance)* harus dilaksanakan.

Dalam rangka menciptakan prakondisi dan infrastruktur pengelolaan resiko maka bank wajib mengambil langkah-langkah persiapan pelaksanaan pengelolaan resikonya. Untuk itu Bank Indonesia menetapkan Peraturan Bank Indonesia Nomor 11/25/PBI/2009 perubahan atas Peraturan Bank Indonesia Nomor 5/8/PBI/2003 tentang Penerapan Manajemen Resiko pada Bank Umum.

Penerapan Manajemen Resiko (*Risk Management*) bertujuan untuk menghindari kerugian yang disebabkan terjadinya suatu resiko atau peristiwa. Fokus dari Manajemen Resiko adalah mengidentifikasi, mengelola dan mengendalikan resiko dengan sebaik-baiknya.Dengan demikian PT. Bank Pembangunan Daerah (BPD) Sumatera Barat Cabang Painan tidak terlepas dari berbagai resiko yang dapat mengakibatkan kegagalan usaha bank.

Pada PT. Bank Pembangunan Daerah (BPD) Sumatera Barat Cabang Painan Penulis menemukan kesalahan pada proses internal, yaitu pada pihak teller yang kurang cekatan dalam melayani nasabah sehingga membutuhkan waktu yang sangat lama yang menyebabkan semakin ramainya nasabah yang antri dan bahkan ada yang sampai berdiri tidak mendapatkan tempat duduk. Tentunya ini sangat mempengaruhi operasional bank walaupun kelihatan sepele tetapi ini juga salah satu faktor kenyamanan nasabah. Nasabah pasti tidak semuanya sabar, tentu ada juga yang tidak. Kekhawatiran penulis hal ini dapat membuat nasabah pindah ke bank pesaing yang pelayanan nya lebih baik.

Pada BPD Sumbar Cabang Painan penulis mendapatkan beberapa data ilmiah di lapangan mengenai permasalahan mengenai pegawai yang mempengaruhi operasional bank bahwa adanya pelatihan karyawan yang tidak terfokus pada bidang kerja yang ditempatinya. Perputaran pegawai yang cukup tinggi juga terjadi sehingga pegawai lama akan dipindahkan dan diganti dengan pegawai baru. Pada beberapa bidang yang harusnya dikerjakan dua orang tetapi dibebankan kepada satu orang sehingga hasil pekerjaan kurang maksimal. Salah satu penyebabnya adalah mutasi pegawai dan belum adanya pengganti.

Permasalahan lain yang penulis ketahui tentang sistem dan teknologi pada BPD Sumbar Cabang Painan adalah masalah jaringan. Kerusakan jaringan terjadi secara mendadak pada waktu tertentu yang mengakibatkan terganggunya pelayanan kepada nasabah.

Dalam kasus yang terjadi Bank BPD Sumbar Cabang Painan tersebut, bahwa terdapat kesalahan manajemen operasional. Berdasarkan data ilmiah diatas, dalam pertimbangan manajemen resiko operasional ini menjadi sangat penting, sehingga nantinya bank dapat meminimalisir resiko dan mendapatkan manfaatnya. Pertimbangannya yaitu manajemen resiko operasional, resiko yang diakibatkan kurangnya informasi dan sistem pengawasan. Dengan demikian kasus yang seperti contoh diatas bisa diminimalisir dengan baik dan tepat.

Berdasarkan uraian latar belakang masalah diatas, maka Penulis mengambil judul "Penerapan Manajemen Resiko Operasional Pada PT. Bank Pembangunan Daerah Sumatera Barat Cabang Painan".

Perumusan Masalah

Adapun rumusan masalah dalam penulisan tugas akhir ini yaitu Bagaimana penerapan Manajemen Resiko operasional pada PT. Bank Pembangunan Daerah Sumatera Barat Cabang Painan?

## TINJAUAN PUSTAKA

### Pengertian Bank

Adapun pengertian bank menurut Undang-Undang RI Nomor 10 Tahun 1998 tentang Perubahan Undang-undang Nomor 7 Tahun 1992 tentang Perbankan adalah "Badan usaha yang menghimpun dana dari masyarakat dalam bentuk simpanan dan menyalurkannya kepada masyarakat dalam bentuk kredit dan/atau bentuk-bentuk lainnya dalam rangka meningkatkan taraf hidup rakyat banyak".

**Pengertian Resiko**

Menurut Peraturan Bank Indonesia No. 11/25/PBI/2009 Pasal 1 Bagian 4 yang berbunyi resiko adalah potensi kerugian akibat terjadinya suatu peristiwa (events) tertentu.

**Jenis Risiko**

Dalam Peraturan Bank Indonesia No. 11/25/PBI/2009 Pasal 4 Ayat (1), yang berbunyi : Resiko sebagaimana dimaksud dalam pasal 2 mencakup :

a. Risiko Kredit
b. Risiko Pasar
c. Risiko Likuiditas
d. Risiko Operasional
e. Risiko Hukum
f. Risiko Reputasi
g. Risiko Stratejik
h. Risiko Kepatuhan

**Manajemen Resiko**

Adapun pengertian Manajemen Resiko dalam Peraturan Bank Indonesia No. 11/25/PBI/2009 Pasal 1 bagian 5 yaitu : "Manajemen resiko adalah serangkaian metedologi dan prosedur yang digunakan untuk mengidentifikasi, mengukur, memantau dan mengendalikan resiko yang timbul dari seluruh kegiatan usaha bank".

**Ruang Lingkup Manajemen Resiko**

Dalam Peraturan Bank Indonesia No. 11/25/PBI/2009 pada pasal 2 Ayat (1) dan (2) yang berbunyi :

Ayat (1) Bank wajib menerapkan Manajemen Resiko secara efektif, baik untuk bank secara individual maupun bank secara konsolidasi dengan perusahaan anak.

Ayat (2) Penerapan Manajemen Resiko sebagaimana dimaksud pada ayat 1 paling kurang mencakup :

1. Pengawasan aktif Dewan Komisaris dan Direksi
2. Kecukupan kebijakan, prosedur, dan penetapan limit manajemen resiko.
3. Kecukupan proses identifikasi, pengukuran, pemantauan, dan pengendalian resiko, serta sistem informasi manajemen resiko dan
4. Sistem pengendalian intern yang menyeluruh

**Pedoman Umum Penerapan Manajemen Resiko**

Sebagai Regulator, Bank Indonesia telah banyak memberikan petunjuk penerapan manajemen resiko dan *good corporate governance* (tata kelola perusahaan yang sehat) bagi perbankan Indonesia. Dalam Lampiran SE No.5/21/DPNP tanggal 29 September 2003 dijelaskan tentang pedoman umum penerapan manajemen resiko oleh bank sebagai berikut :

Pengawasan Aktif Dewan Komisaris dan Direksi

a. Kewenangan dan tanggung jawab pengurus bank. Bank wajib menetapkan wewenang dan tanggung jawab yang jelas pada setiap jenjang jabatan yang terkait dengan penerapan manajemen resiko. Wewenang dan tanggung jawab dewan komisaris dan direksi.

b. Sumber Daya Manusia (SDM) . Bank harus menetapkan kualifikasi SDM yang jelas untuk setiap jenjang jabatan yang terkait dengan penerapan manajemen resiko.

**Organisasi dan Fungsi Manajemen Resiko**

Dalam rangka penerapan manajemen resiko yang efektif, bank harus menyusun struktur organisasi yang susuai dengan tujuan dan kebijakan usaha, ukuran dan kompleksitas serta kemampuan bank.

Dalam kaitan dengan pengembangan struktur organisasi yang ada, bank wajib membentuk Komite Manajemen Resiko (*Risk Management Committe*) dan Satuan Kerja Manajemen Resiko (*Risk Management Unit*).

Kebijakan, Prosedur dan Penetapan Limit Resiko

Kebijakan Manajemen Resiko sekurang-kurangnya meliputi :

Penetapan resiko yang terkait dengan produk dan transaksi perbankan dan Penetapan penggunaan metode pengukuran dan sistem informasi manajemen resiko dalam rangka mengkalkulasi secara tepat eksposur resiko serta aktivitas fungsional bank, dan penetapan pelaporan data dan informasi yang terkait dengan eksposur resiko sebagai input untuk pengambilan keputusan bisnis yang menguntungkan dan tetap memperhatikan prinsip kehati-hatian bank. Penetapan strategi manajemen resiko juga harus mempertimbangkan kondisi keuntungan bank, organisasi bank dan resiko yang timbul sebagai akibat perubahan faktor eksternal dan internal.

Prosedur dan penetapan limit resiko sekurang-kurangnya mencakup Akuntabilitas dan jenjang delegasi wewenang yang jelas, Pelaksanaan kaji ulang terhadap prosedur dan penetapan resiko secara berkala , Dokumentasi dan prosedur penetapan limit yang memadai Penetapan limit resiko wajib mencakup Limit secara keseluruhan, Limit perjenis resiko, Limit peraktivitas fungsional tertentu yang memiliki eksposur resiko.

**Proses Penerapan Manajemen Risiko**

**Identifikasi Risiko**

Tujuan dilakukannya identifikasi risiko adalah untuk mengidentifikasi seluruh jenis risiko yang melekat pada setiap aktivitas fungsional yang berpotensi merugikan bank

**Pengukuran Risiko**

Pendekatan pengukuran risiko digunakan untuk mengukur profil risiko bank. Pendekatan tersebut harus dapat mengukur :

Sensivitas produk/aktivitas terhadapa perubahan faktor-faktor yang mempengaruhinya, baik dalam kondisi normal maupun tidak normal, faktor risiko (*Risk Faktors*) secara individual, eksposur risiko secara keseluruhan (*aggregate*), dengan mempertimbangkan *risk correlation*, seluruh risiko yang melekat pada seluruh transaksi serta produk perbankan dan dapat diintegrasikan dalam sestem informasi manajemen Bank.

**Pemantauan Limit Risiko**

Sebagai bagian dari penerapan pemantauan risiko maka limit risiko sekurang-kurangnya memperhatikan kemampuan modal Bank untuk dapat menyerap eksposur risiko atau kerugian yang timbul, dan tinggi rendahnya eksposur Bank, tersedianya limit secara individual dan keseluruhan/konsolidasi,

mempertimbangkan pengalaman kerugian di masa lalu dan kemampuan sumber daya manusia, memastikan bahwa posisi yang melampaui limit yang telah ditetapkan mendapat perhatian satuan kerja manajemen risiko, komite manajemen risiko dan Direksi.

**Sistem Informasi Manajemen Risiko**

Sebagai bagian dari proses manajemen risiko, Bank harus memiliki sistem informasi manajemen risiko yang dapat memastikan terukurnya eksposur risiko secara akurat, informatif, dan tepat waktu, baik eksposur risiko secara keseluruhan/komposit maupun eksposur per jenis risiko yang melekat pada kegiatan usaha Bank, dipatuhinya penerapan manajemen risiko, tersedianya hasil (realisasi) penerapan manajemen resiko dibandingkan dengan target yang ditetapkan oleh bank sesuai dengan kebijakan dan strategi penerapan manajemen resiko.

Sebagai salah satu output sistem informasi manajemen risiko, laporan eksposur risiko disusun secara berkala oleh Satuan Kerja Manajemen Risiko atau sekelompok petugas yang diberikan wewenang

Pengendalian Risiko

Pelaksanan proses pengendalian risiko harus digunakan Bank untuk mengelola risiko tertentu, terutama yang dapat membahayakan kelangsungan usaha Bank.

Pengendalian risiko dapat dilakukan oleh Bank, antara lain dengan cara *hedging*, dan metode mitigasi risiko lainnya seperti penerbitan garansi, sekuritisasi aset dan *credit derivatives*, serta penambahan modal Bank untuk menyerap potensi kerugian.

**Pengertian Risiko Operasional**

*Basel Capital Accord II* , resiko operasional didefinisikan sebagai : "Resiko kerugian yang terjadi sebagai akibat dari *inadequate* atau *fail internal process, people and systems or external events"*

**Identifikasi Resiko Operasional**

Identifikasi resiko operasional dilakukan dengan tujuan untuk mengidentifikasi seluruh jenis resiko yang berpotensi mempengaruhi kerugian operasional dan karenanya juga mempengaruhi laba rugi perbankan.

Identifikasi resiko operasional yang efektif harus memperhatikan semua faktor, baik internal maupu eksternal.

**Pengukuran Resiko Operasional**

Pengukuran potensi kerugian resiko operasional dapat dilakukan dengan dua metode :

1. Metode standar

a. *Basic Indicator Approach (*BIA)
   Dalam model BIA bank mempergunakan laba kotor rata-rata tiga tahun terakhir sebagai indikator resiko

b. *Standardized Approach* (SA)
   Untuk menghitung potensi kerugian resiko operasional berdasarkan metode SA diperlukan laba kotor dan parameter beta dari masing-masing bisnis bank.

c. *Alternative Standardized Approach (ASA)*

Metode ASA adalah sama dengan metodologi untuk metode SA. Perbedaan nya terletak pada pengukuran untuk resiko operasional untuk *business lines retail banking and commercial banking.*

2. Metode Internal

Dalam metode internal digunakan pendekatan secara *Advanced Measurement Approach (AMA)* yaitu metode yang lebih menekankan pada analisis kerugian operasional. Metode ini memerlukan data base kerugian operasional sekurang-kurangnya dua hingga lima tahun terakhir dan perusahan harus mempunyai teknologi yang tinggi sehingga dengan menggunakan bantuan teknologi tersebut dapat dibuat model menangkap, menyeleksi dan melaporkan informasi operasional.

Pemantauan Resiko Operasional

Bagian Manajemen resiko harus melaksanakan pemantauan resiko operasional secara berkala terhadap seluruh eksposur resiko operasional serta kerugian yang dapat terjadi. Dengan menerapkan sistem pengendalian internal yakni menyediakan laporan berkala mengenai kerugian yang ditimbulkan oleh resiko operasional, manajemen perusahaan akan mendapatkan informasi yang jelas tentang potensi kerugian resiko operasional di masa mendatang

Pengendalian Resiko Operasional

Pengendalian dan mitigasi resiko operasional harus dilaksanakan oleh seluruh unit kerja dan satuan kerja bank , termasuk Bagian Manajemen Resiko dan Direksi Bagian manajemen resiko memiliki sistem teknologi informasi sehingga manajemen dapat melaksanakan pemantauan dan pengendalian resiko operasional. Bagian manajemen resiko juga harus memastikan bahwa bank telah memiliki prosedur dan sistem *back up, contig*ency *plan, and disaster recovery plan* serta sistem keamanan dan *warehouse.*

**Manfaat Manajemen Resiko Operasional (MRO)**

Penerapan terhadap MRO oleh bank memberi manfaat bagi bank (Haris,dkk, 2005 : 27) sebagai berikut :

1. Untuk memastikan bahwa manajemen mengambil langkah yang tepat untuk identifikasi, menilai dan mengelola resiko operasional.
2. Untuk meningkatkan transparansi dan konsistensi atas informasi seluruh organisasi bank dengan menyelaraskan sumber informasi seperti *key risk indicator, risk self assesment, corporate loss database* dan laporan audit
3. Untuk memfasilitasi pendektatan *risk based approach and capital allocation* resiko operasional.
4. Untuk mengurangi kerugian operasional

**Alat Ukur Manajemen Resiko Operasional**

Untuk itu diperlukan alat ukur (Ali, 2006 : 418) untuk mendeteksi penyebab resiko operasional tersebut diantaranya :

1. *Risk & Control Self Assesment*

   Tujuan RSCA adalah untuk meningkatkan pengetahuan dan kesadaran terhadap resiko operasional serta menentukan langkah-langkah untuk memitigasi resiko operasional tersebut, dimana diharapkan dapat menurunkan tingkat kerugian operasional.

2. *Corporate Loss Database*
   Merupakan pusat penyimpanan data kerugian operasional yang dialami bank selama bertahun-tahun yang lalu.
3. *Key Risk Indicator*
   Merupakan suatu kumpulan parameter resiko atas aktivitas operasional yang dilakukan bank

## METODE PENELITIAN

Dalam pengumpulan data dan bahan untuk penelitian ini digunakan metode penelitian sebagai berikut :

Metode Pengumpulan Data

1) Study Lapangan (*Field Research*)
   Peninjauan langsung ke objek yang dipilih untuk meneliti hasil data sekunder. Penelitian langsung ke lapangan ini akan dapat membantu Penulis untuk melengkapi data yang diperlukan. Adapun cara riset lapangan ini adalah dengan mewawancarai langsung pihak-pihak yang berkepentingan dalam hal ini adalah perusahaan dan instansi yang terkait.
2) Study Kepustakaan (*Library Research*)
   Penelitian dilakukan dengan membaca beberapa buku-buku ilmiah dan tulisan-tulisan yang berhubungan dengan pembahasan yang dilakukan.

Metode Analisa Data

Dalam menganalisa data, menggunakan analisa data kualitatif secara deskriptif. Dimana metode kualitatif menggambarkan, memahami dan menjelaskan data yang diteliti selama penelitian berlangsung pada PT. BPD Sumbar Cabang Painan.

## HASIL DAN PEMBAHASAN

Pengawasan Aktif Komisaris dan Direksi

Komisaris dan Direksi PT. BPD Sumbar Cabang Painan telah memahami resiko operasional dan secara aktif mengevaluasi kebijakan dan strategi resiko operasional secara periodik

Kebijakan, Prosedur dan Penetapan Limit

a) BPD Sumbar Cabang Painan memiliki kebijakan pengelolaan resiko operaional yang sesuai dengan misi, strategi bisnis, kecukupan permodalan dan kecukupan sumber daya manusia
b) BPD Sumbar Cabang Painan menetapkan dan menerapkan prosedur untuk menilai resiko operasional
c) Melakukan evaluasi dan pengkinian kebijakan dan prosedur pengelolaan resiko operasional
d) Menetapkan limit (cadangan) resiko operasional dengan mempertimbangkan eksposur resiko dan pengalaman kerugian masa lalu yang diakibatkan oleh resiko operasional.
e) Kebijakan, prosedur dan proses penetapan limit resiko operasional didokumentasikan secara tertulis dan lengkap hingga memudahkan untuk dilakukan jejak audit (*audit trail)*

1) Penyelesaian Transaksi (*Settlement)*

a) BPD Sumbar Cabang Painan melakukan penilaian terhadap tahapan dalam proses penyelesaian transaksi, khususnya mengenai batas akhir perintah pembayaran, batas akhir penerimaan waktu pencatatan pembayaran dana.
b) BPD Sumbar Cabang Painan menyusun suatu prosedur pemantauan penyelesaian transaksi baru atau apabila terdapat transaksi yang belum diselesaikan pembayarannya
c) BPD Sumbar Cabang Painan menyediakan prosedur penyelesaian transaksi yang disebabkan oleh adanya kondisi likuidasi bank yang memburuk
d) BPD Sumbar Cabang Painan melakukan konfirmasi transaksi secara tepat waktu sesuai dengan prosedur yang ditetapkan dan memantau transaksi tersebut secra konsisten

2) Akuntansi

BPD Sumbar Cabang Painan memastikan bahwa penggunaan metode akuntansi adalah sesuai dengan standar akuntansi yang berlaku serta memperhatikan hal-hal sebagai berikut :

a) Melakukan review secara berkala guna memastikan ketetapan metode yang digunakan untuk menilai transaksi
b) Melakukan review secara berkala terhadap kesesuaian metode akuntansi yang digunakan dengan standar akuntansi keuangan yang berlaku
c) Melakukan rekonsiliasi data transaksi secara berkala
d) Mengidentifikasi dan menganalisa setiap ketidakwajaran transaksi yang terjadi
e) Memelihara seluruh dokumen dan arsip yang berkaitan dengan rincian rekening (*accounts), sub-ledgers*, buku besar (*general ledgers),* administrasi klasifikasi aset dan dokumentasi pembentukan provisi, guna memudahkan proses jejak audit

3) Inventarisasi Aset dan Kustodian

a) BPD Sumbar Cabang Painan memelihara data akuntansi dan rincian aset pihak ketiga yang dipeliahara/dititipkan (kustodian)
b) BPD Sumbar Cabang Painan memperoleh informasi yang memadai mengenai keaslian penyimpanan/penitipan aset dalam rangka memastikan bahwa aset yang dititipkan tidak memiliki permasalahan hukum
c) BPD Sumbar Cabang Painan melakukan pengecekan secara berkala antara data aset yang dititipkan dengan perjanjian/kontraknya

4) Profil Nasabah dan Prinsip Mengenal Nasabah (*Know Your Customer/KYC)*

a) BPD Sumbar Cabang Painan menerapkan Prinsip Mengenai Nasabah (KYC) secara konsisten sesuai dengan eksposur resiko operasional.
b) Dalam penerapan KYC tersebut, BPD Sumbar Cabang Painan mewajibkan Customer Service untuk memenuhi seluruh persyaratan dan pedoman tentang Prinsip Mengenal Nasabah (KYC) kepada calon nasabah yang ingin membuka rekening.

5) Profil Karyawan (*Employees' Profiles)*

BPD Sumbar Cabang Painan memiliki dan menerapkan kebijakan tentang tanggung jawab, kewenangan dan akses pegawai/karyawan terhadap sistem informasi tertentu. Kebijakan tersebut didukung oleh prosedur akses terhadap sistem informasi manajemen, sistem informasi akuntansi, sistem pengelolaan resiko, pengamanan di deadling room, dan ruang pemprosesan data.

Proses Identifikasi, Pengukuran, Pemantauan dan sistem Informasi Manajemen Resiko Operasional

1) Identifikasi Resiko Operasional

Dalam proses identifikasi resiko operasional BPD Sumbar Cabang Painan, langkah yang dilakukan :

a) BPD Sumbar Cabang Painan melakukan identifikasi dan analisa terhadap faktor penyebab timbulnya resiko operasional yang melekat pada seluruh aktivitas fungsional, produk, proses dan sistem informasi, baik yang disebabkan oleh faktor intern maupun ekstern yang berdampak negatif terhadap pencapaian sasaran organisasi bank.
b) Hasil identifikasi tersebut selanjutnya digunakan oleh BPD Sumbar Cabang Painan untuk mengembangkan suatu *database* mengenai jenis kerugian (*loss event)* yang ditimbulkan oleh resiko operasional.
c) Metode yang dapat digunakan BPD Sumbar Cabang Painan untuk mengidentifikasi resiko operasional, antara lain :

1. *Self risk assesment* berupa *checklist* untuk mengidentifikasi kekuatan dan kelemahan pada lingkungan operasional Bank,
2. *Risk mapping* berupa pemetaan menurut jenis resiko terhadap aktivitas fungsional, struktur organisasi dan arus proses transaksi.
3. *Key risk indocators* berupa statistik atau matriks yang menyediakan data posisi resiko operasional bank, seperti jumlah pembatalan transaksi, tingkat perputaran pegawai, dan frekuensi kesalahan (*errors)*
4. *Scorecards* yang menyediakan metode untuk mentranslasikan penilaian/kriteria kualitatif menjadi matriks kuantitatif, yang dapat digunakan untuk mengalokasikan kebutuhan modal masing-masing aktivitas fungsional.

2) Pengukuran Resiko Operasional

a) BPD Sumbar Cabang Painan menilai parameter yang mempengaruhi eksposur resiko operasional, antara lain jumlah dan frekuensi :
   1. Kegagalan dan kesalahan sistem;
   2. Sistem administrasi;
   3. Kegagalan hubungan dengan nasabah;
   4. *Accounting error;*
   5. Penundaan dan kesalahan dalam penyelesaian pembayaran;
   6. *Fraud*
   7. Rekayasa akunting
   8. *Strategic failure*

b) Pengumpulan Data Resiko Operasional

1. Sumber utama dalam penerapan manajemen resiko operasional adalah data historis mengenai kerugian bank yang disebabkan resiko operasional yang telah divalidasi dan diverifikasi

2. Data kerugian resiko operasional terdiri dari kejadian (*events)* yang bersifat rutin, berfrekuensi tinggi namun berdampak rendah maupun yang berfrekuensi rendah namun berdampak tinggi terhadap rugi laba bank. Data rendah namun berdampak tinggi.

c) BPD Sumbar Cabang Painan memiliki metodologi pengukuran resiko operasional yang tepat, sumberdaya manusia yang kompeten dan infrastruktur

sistem yang memadai dalam rangka mengidentifikasi dan mengumpulkan data resiko operasional

d) BPD Sumbar Cabang Painan mencatat dan menatausahakan setiap events termasuk jumlah potensi kerugian yang diakibatkan events dimaksud dalam suatu administrasi data.

2) Pemantauan Resiko Operasional

BPD Sumbar Cabang Painan melakukan pemantauan resiko operasional secara berkelanjutan terhadap seluruh eksposur resiko operasional serta kerugian (*loss events)* yang dapat ditimbulkan oleh aktivitas fungsional utama (*major business line),* antara lain dengan cara menerapkan sistem pengendalian intern dan menyediakan laporan berkala mengenai kerugian yang ditimbulkan oleh resiko operasional.

3) Sistem Informasi Manajemen Resiko Operasional

a) BPD Sumbar Cabang Painan memiliki sistem dan teknologi informasi yang memadai.

b) Sistem informasi manajemen menghasilkan laporan yang lengkap dan akurat yang digunakan untuk pemantauan resiko dalam rangka mendeteksi dan mengkoreksi penyimpangan secara tepat waktu dalam rangka proses pengambilan keputusan oleh direksi guna mengurangi potensi terjadinya *loss events*

Pengendalian Resiko Operasional

1) BPD Sumbar Cabang Painan memiliki kebijakan, prosedur dan proses untuk mengendalikan atau memitigasi resiko operasional, sesuai dengan komplesitas operasional bank

2) Dalam penerapan pengendalian resiko operasional, BPD Sumbar Cabang Painan mengembangkan proses untuk memitigasi resiko operasional antara lain pengamanan proses teknologi informasi, asuransi, dan *outsourching* sebagian kegiatan operasional bank.

3) Dalam hal bank mengembangkan pengamanan proses teknologi informasi, BPD Sumbar Cabang Painan memastikan tingkat keamanan dari *electric data processing.*

4) Pengendalian terhadap sistem informasi harus memastikan :

   a) Adanya penilaian berkala terhadap pengamanan sistem informasi, yang disertai dengan tindakan korektif apabila diperlukan.

   b) Tersedianya prosedur *back up* untuk menjamin berjalannya kegiatan operasional bank dan mencegah terjadinya gangguan yang signifikan.

   c) Tersedianya prosedur *back-up* dan rencana darurat (*contigency plan)* yang diuji secara berkala.

   d) Tersedianya penyimpanan informasi dan dokumen yang berkaitan dengan analisa, programming, dan pelaksanaan pemrosesan data.

5) BPD Sumbar Cabang Painan memiliki *support system,* yang sekurang-kurangnya mencakup :

   a) Identifikasi *error* secara dini

   b) Pemrosesan dan penyelesaian seluruh transaksi secara efisien, akurat dan tepat waktu

   c) Kerahasiaan, kebenaran serta keamanan transaksi.

6) BPD Sumbar Cabang Painan melakukan kaji ulang secara berkala terhadap prosedur, dokumentasi, sistem pemrosesan data, *contigency plan*, dan praktek operasional lainnya guna mengurangi kemungkinan terjadinya kesalahan manusia (*human error)* yang menimbulkn resiko operasional.

Contoh Kasus Resiko Operasional

1. Kasus 1

Pada tangggal 07 Januari 2013 nasabah datang ke BPD Sumbar Cabang Painan dengan maksud ingin melakukan penyetoran ke rekening anaknya sebesar Rp. 2.250.000 dengan keadaan kantor yang sedang dipenuhi oleh nasabah lain, nasabah A ikut mengantri. Setelah cukup lama mengantri nasabah A dipanggil oleh *teller*. Kemudian *teller* menanyakan ke nasabah A maksud dan tujuan transaksinya. Setelah memberikan tanda setoran ke *teller*, kemudian *teller* melakukan input data ke komputer sesuai dengan tanda setoran yang diberikan oleh nasabah A setelah menunggu beberapa lama transaksi nasabah A selesai dilakukan. Dengan mengambil bukti setoran yang diberikan oleh *teller* nasabah A kemudian meninggalkan kantor BPD Sumbar Cabang Painan.

Kemudian pada tanggal 08 Januari 2013 nasabah A kembali mendatangi kantor BPD Sumbar Cabang Painan dengan maksud mengkonfirmasikan kepada pihak bank bahwa transaksi penyetoran yang dilakukannya pada tanggal 07 Januari 2013 tidak sampai ke rekening anaknya. Padahal bukti sertoran dan uang telah diserahkan kepada petugas bank yaitu *teller*. Dengan bukti setoran yang ada pada nasabah A, nasabah A kemudian melakukan komplain kepada pihak bank. Dari bukti setoran yang ada pada pihak bank dan nasabah A, pihak bank melakukan pengecekan. Setelah dilakukan pengecekan ternyata terjadi kesalahan antara bukti validasi (Tapak validasi) yang dilakukan oleh teller ternyata berbeda dengan yang dibuat nasabah.

Dampak dari Kasus 1

Adapun dampak dari kasus 1 yang terjadi diatas adalah :

1) Kesalahan validasi dapat mengurangi kepercayaan nasabah terhadap bank
2) Bagi petugas bank yakni teller kasus tersebut dapat mengurangi kinerja bank dari teller yang melakukan kesalahan karena kurangnya kehati-hatian dari teller
3) Jika kasus tersebut tidak dapat diselesaikan sudah pasti nasabah akan mengalami kerugian financial (sejumlah uang yang disetorkan)
4) Jika nasabah tetap melakukan komplein dan ternyata uang yang disetorkan telah diambil oleh pemilik rekening, dan ternyata tidak dapat dikembalikan, hal ini mendatangkan kerugian bagi teller karena teller harus mengganti uang tersebut karena hal tersebut merupakan tanggung jawab teller.

Penyelesaian dari Kasus 1

Ada beberapa langkah yang dapat dilakukan oleh pihak bank ataupun nasabah untuk menyelesaikan kasus seperti diatas, yakni :

1. Pihak bank yakni BPD Sumbar Cabang Painan segera menghubungi bank yang mewakili nomor rekening yang telah dituju/validasi oleh teller dan membuat surat pernyataan, kemudian mengkonfirmasi bahwa telah terjadi kesalahan validasi. Kemudian bank yang bersangkutan diminta untuk mencari nasabah pemilik rekening tersebut. Bank mengkonfirmasikan nasabah telah terjadi

kesalahan validasi ke rekening bank yang bersangkutan untuk melakukan pengembalian uang ke BPD Sumbar Cabang Painan.

2. Penyelesaian yang kedua adalah penyelesaian yang paling akhir diambil karena langkah ini merupakan langkah yang merugikann teller, yakni teller harus mengganti kerugian yang diderita nasabah A, karena kesalahan datang dari pada teller yang telah salah memasukkan nomor rekening nasabah ke sistem. Langkah ini diambil jika nasabah pemilik rekening setelah dikonfirmasi ternyata tidak bisa dikembalikan dengan alasan telah dipergunakan.

Antisipasi dari Kasus 1

Adapun beberapa tindakan yang dapat dilakukan untuk mengantisipasi dan mengurangi kasus tersebut, yakni :

1. Teller harus mengkonfirmasikan kepada nasabah atas tanda setoran yang telah ditulis sebelumnya
2. Setelah melakukan verifikasi awal dengan melakukan pengecekan dan pencocokan terhadap :
   a. Nomor rekening hasil validasi dengan yang ditulis nasabah
   b. Nama pemilik rekening
   c. Jumlah nominal dan terbilang yang ditulis nasabah
   d. Pemberian tanda tangan yang dibuat oleh nasabah (khusus penarikan tabungan harus cocok dengan yang ada di buku tabungan)
   e. Tanggal transaksi
3. Overbooking

Adalah kegiatan transaksi dari satu rekening ke rekening lainnya tanpa mempengaruhi keadaan kas teller

4. Rekening titipan

Adalah rekening penampung yang harus dimiliki oleh BPD Cabang yang dapat dipergunakan untuk melakukan transaksi antar cabang BPD Sumbar.

2. Kasus 2

Pada tanggal 30 Maret 2016 ketika nasabah BPD Sumbar Cabang Painan sedang ramai untuk menarik uang dan menyetor uang terjadi gangguan sistem yang diakibatkan oleh jaringan yang tidak stabil. Oleh karena itu nasabah semakin ramai, sampai ada nasabah yang berdiri tidak dapat tempat duduk menunggu jaringan pulih kembali. Karena nasabah di akhir bulan memang sangat ramai menarik uang di BPD Sumbar Cabang Painan. Ada yang dari instansi pemerintahan dan pencairan dana tender serta untuk keperluan lain. Dengan adanya gangguan jaringan tersebut maka akan terjadi ganguan pelayanan yakninya keterlambatan nasabah dalam pengambilan uang atau penyetoran uang. Maka dari itu banyak nasabah yang komplen ke pihak bank karena tidak sedikit nasabah memerlukan uang yang akan dicairkan atau disetor perlu cepat.

Dampak dari Kasus 2

Adapun dampak dari kasus 2 diatas adalah:

1. Gangguan jaringan dapat mengurangi kepercayaan nasabah terhadap bank.
2. Jika kasus ini terus terjadi bukan tidak mungkin nasabah akan berpindah ke bank lain yang pelayanan nya lebih baik

Penyelesaian dari Kasus 2

Penyelesaian yang dilakukan oleh BPD Sumbar Cabang Painan yakni pihak bank berusaha menghubungi otoritas yang berwenang dan mengkonfirmasikan bahwa ada gangguan jaringan yang mengakibatkan terganggunya transaksi bank.

BPD Sumbar Cabang Painan memberitahu kepada nasabah bahwa telah terjadi gangguan jaringan dan pihak bank meminta nasabah untuk bersabar sebentar karena akan segera pulih.

## SIMPULAN

Secara keseluruhan penerapan manajemen resiko operasional pada PT. Bank Pembangunan Daerah Sumatera Barat Cabang Painan telah sesuai dengan Peraturan Bank Indonesia No. 11/25/PBI/2009 yang telah dilaksanakan secara efektif. Proses penerapan manajemen resiko operasional pada BPD Sumbar Cabang Painan adalah penerapan yang sesuai dengan konsep-konsep yang ditetapkan oleh Bank Indonesia. PT. BPD Sumbar Cabang Painan secara umum mampu mengendalikan resiko operasional.

. Pada BPD Sumbar Cabang Painan telah menyediakan sumber daya yang berkualitas untuk menyelesaikan tugas pengelolaan secara efektif dengan cara berkala mengirim pegawai untuk mengikuti pelatihan dan ujian sertifikasi manajemen resiko. Dimana pemimpin cabang dan semua pemimpin seksi telah dinyatakan lulus sertifikasi manajemen resiko.

BPD Sumbar Cabang Painan memberikan penilaian kepada karyawannya dengan memasukkan setiap kesalahan dalam kegiatan operasional ke dalam item kesalahan karyawan yang melakukan kesalahan. Dan hal ini akan mengurangi penilaian terhadap karyawan tersebut. Melalui ini secara tidak langsung akan membuat karyawan untuk tidak melakukan kesalahan lagi.

Jadi, dengan demikian BPD Sumbar Cabang Painan sudah menerapkan manajemen resiko sesuai dengan Peraturan Bank Indonesia No. 11/25/PBI/2009. Implementasi manajemen resiko tersebut telah sejalan dengan rekomendasi yang dikeluarkan oleh *Bank International Settlements melalui Basel committe on Banking Supervision* sebagaimana diwajibkan oleh bank indonesia melalui Peraturan Bank Indonesia tentang penerapan manajemen resiko.

## DAFTAR PUSTAKA


Ali, H Masyud. 2006. ***Manajemen Resiko***. Jakarta : PT. Raja Grafindo Persada.

Fahmi, Irham. 2011. ***Manajemen Resiko***. Bandung. Alfabeta CV.

Fernandes, Y. D., & Marlius, D. (2018). Peranan Customer Service Dalam Meningkatkan Pelayanan Kepada Nasabah Pada PT. Bank Pembangunan Daerah Sumatera Barat Cabang Utama Padang. https://doi.org/10.31227/osf.io/wrh3p

Handoko, Sri Redjeki. 1995. ***Teori dan Perilaku Organisasi Perusahaan***. Yogyakarta : BPFE

Haris, Arifin. S. 2005. ***Manajemen Resiko dan Manajemen Resiko Perbankan***. Jakarta : Prima Management Consultan

Herman, Darmawi. 2011. ***Manajemen Perbankan***. Jakarta : Bumi Aksara.

Kasmir. 2014. ***Manajemen Perbankan***. Edisi Revisi, PT. Raja Grafindo Persada

Muslich. 2007. ***Manajemen Resiko Operasional***. Jakarta : Bumi Aksara.

Peraturan Bank Indonesia No. 11/25/PBI/2009 Perubahan atas Peraturan Bank Indonesia No. 5/8/PBI/2003 Tentang Penerapan Manajemen Resiko.

Sinungan, Sondang P. 2001. ***Manajemen Dana Bank***. Jakarta : Bumi Aksara

Susilo, Y. Sri. 2001. ***Bank dan Lembaga Keuangan Lainnya***. Jakarta : PT. Gramedia Pustaka Utama.

Umar. 2001. ***Manajemen Bank***. Jakarta : Pustaka Grafiti.

Undang – undang No. 10 Tahun 1998 Tentang Perubahan Undang – undang No.7 Tahun 1992 Tentang Perbankan.

Wulandari, R., & Susanto, R. (2019). Penerapan Manajemen Risiko Operasional Pada Unit Teller Pada PT. Bank Pembangunan Daerah Sumatera Barat Cabang Lubuk Alung. https://doi.org/10.31219/osf.io/pjgch

Nama : Reynaldi

Nim : 182420111

Matkul : IT Service Management

---

**SOAL**

Jelaskan Bagaimana Konsep IT Risk Management pada ITSM dan erikan contoh kasus (Jurnal)

**JAWAB**

1. Risk Management

   Mengidentifikasi potensi resiko yang disebabkan oleh proses pelayanan IT, merekam resiko-resiko tersebut serta dampaknya dan solusi yang dapat digunakan. Melacak dan menganalisa keretanan Data yang sensitif atau penting. mengklasifikasi file-file berdasarkan dari kesensitifannya, dan memastikan file-file tersebut di sediakan

   dengan perlindungan yang layak

   Contoh kasus:

   "Penerapan Manajemen Resiko Operasional pada PT.Bank pembangunan daerah Sumatera Barat cabang painan Kabupaten Pesisir Selatan"

   Contoh kasus tentang sistem dan teknologi pada BPD Sumbar Cabang Painan adalah masalah jaringan. Kerusakan jaringan terjadi secara mendadak pada waktu tertentu yang mengakibatkan terganggunya pelayanan kepada nasabah. Dalam kasus yang terjadi Bank BPD Sumbar Cabang Painan tersebut, bahwa terdapat kesalahan manajemen operasional. Berdasarkan data ilmiah diatas, dalam pertimbangan manajemen resiko operasional ini menjadi sangat penting, sehingga nantinya bank dapat meminimalisir resiko dan mendapatkan manfaatnya. Pertimbangannya yaitu manajemen resiko operasional, resiko yang diakibatkan kurangnya informasi dan sistem pengawasan

Zico Prasetyo, Afriyeni. 2019. Penerapan Manajemen Resiko Operasional pada PT.Bank pembangunan daerah Sumatera Barat cabang painan Kabupaten Pesisir Selatan, Akademi Keuangan dan Perbankan Padang.

.

# Evaluasi Manajemen Risiko Teknologi Informasi Pada Perusahaan BUMN Menggunakan Standar COBIT 5 (Studi Kasus: PT TASPEN PERSERO)

**Riyan Abdul Aziz[1], Kusrini[2], Sudarmawan[3]**
[1,2,3]Universitas Amikom Yogyakarta
Email :[1]riyan.az@students.amikom.ac.id,
[2]kusrini@amikom.ac.id,[3]sudarmawan@amikom.ac.id

***Abstract***

*PT TASPEN PERSERO has implemented a computerized information technology in achieving its organizational goals. The use of Information Technology in addition to improving the speed and accuracy of information and ICT services within the company, also increases the risk of various types. The high level of dependence on ICT services company to run the main task and functions become important need for information technology risk management to reduce and mitigate the risks that may occur. In order to know whether a company has prevented the occurrence of errors and minimize the risks of information technology it is required a framework evaluation management risk information technology one of which is COBIT 5. The process of evaluating information technology risk management using COBIT 5 is in process domain APO12 (Manage Risk) and process domain EDM03 (Ensure Risk Optimization). From the results of the evaluation of the data obtained through the spread of questionnaires, interviews and observations obtained value capability level domain APO12 and EDM03 are on level 1. The results of this study in the form of questionnaires table of information technology risk evaluation, capability level, and recommendations.*

***Keywords:****COBIT 5, capability level, recommendations*

***Abstraksi***

*PT TASPEN PERSERO telah menerapkan teknologi informasi komputerisasi dalam mencapai tujuan organisasinya. Penggunaan Teknologi Informasi selain meningkatkan kecepatan dan keakuratan informasi serta pelayanan TIK di dalam perusahaan, juga meningkatkan berbagai jenis risiko. Tingginya tingkat ketergantungan perusahaan terhadap layanan layanan TIK untuk menjalankan tugas pokok dan fungsi menjadi hal penting diperlukannya manajemen risiko teknologi informasi untuk mengurangi dan menanggulangi risiko-risiko yang mungkin terjadi. Untuk mengetahui apakah suatu perusahaan tersebut sudah melakukan pencegahan terjadinya kesalahan dan meminimalkan risiko-risiko teknologi informasi maka diperlukan suatu framework evaluasi manajemen risiko teknologi informasi salah satunya adalah COBIT 5. Proses evaluasi manajemen risiko teknologi informasi menggunakan COBIT 5 terdapat pada domain proses APO12 (Manage Risk) dan domain proses EDM03 (Ensure Risk Optimisation). Dari hasil evaluasi terhadap data yang diperoleh melalui penyebaran kuesioner, wawancara dan observasi didapatkan nilai capability level domain APO12 dan*

*EDM03 berada pada level 1. Hasil dari penelitian ini berupa tabel kuesioner evaluasi risiko teknologi informasi, capability level, dan rekomendasi.*

***Kata Kunci:****COBIT 5, capability level, rekomendasi*

## 1. PENDAHULUAN

Saat ini perkembangan teknologi informasi menjadi bagian yang sangat penting hampir di semua kalangan terlebih pada suatu lembaga atau perusahaan. Teknologi informasi dibutuhkan mengingat tingginya kebutuhan dan minat para pengguna akan hal ini. Teknologi informasi yang baik sangat berperan dalam mendukung kegiatan operasional perusahaan dan proses bisnis perusahaan. Elemen dan komponen teknologi informasi di dalam sistem harus saling terintegrasi dan dapat berjalan sesuai dengan tugas dan fungsinya masing-masing sehingga dapat menjalankan aktivitas-aktivitas utama didalamnya demi memenuhi kebutuhan informasi para pengguna atau karyawan.

PT TASPEN merupakan salah satu perusahaan BUMN yang bergerak di bidang pengelolaan dana pensiun dan tabungan hari tua serta perusahaan jasa lainnya. Sebagai salah satu perusahaan besar di Indonesia, PT TASPEN memiliki visi “Menjadi pengelola dana pensiun dan tabungan hari tua (THT) serta jaminan sosial lainnya yang terpercaya” dan misi “Mewujudkan manfaat dan pelayanan yang semakin baik bagi peserta dan stakeholder lainnya secara profesional dan akuntabel, berlandaskan integritas dan etika yang tinggi”. Dibawah tanggung jawab Departemen TI, PT TASPEN menyiapkan anggaran khusus setiap tahunnya dalam jumlah yang tidak kecil untuk pengadaan, pengembangan dan pengelolaan seluruh kegiatan TI, termasuk mengelola risiko TI untuk mencegah dampak risiko yang dapat menimbulkan kerusakan dan kerugian yang mengancam aset TI serta menjaga keamanan informasi.

Meskipun telah dilakukan berbagai kegiatan pengelolaan TI, namun disadari bahwa Departemen TI belum maksimal dalam menjalankan fungsinya karena keterbatasan sumber daya manusia yang sedikit dan belum sepenuhnya siap menghadapi risiko ancaman bencana yang dapat terjadi secara tiba-tiba. Ketidaksiapan tersebut terlihat dari penanganan bencana dan risiko dilakukan secara spontanitas, belum adanya kontrol-kontrol untuk meminimalkan risiko TI seperti halnya kesiapan dalam bentuk perencanaan *Disaster Recovery Planning* (DRP) dan *Business Continuity*

*Plan* (BCP).

Untuk mengukur pencapaian PT TASPEN PERSERO dalam mengelola penerapan manajemen risiko TI dibutuhkan sebuah evaluasi. Evaluasi tersebut terdiri dari beberapa tahapan yang meliputi analisis *capability level*, *gap* dan *risk assessment*. Dari tahapan evaluasi tersebut dihasilkan sebuah rekomendasi dan strategi mitigasi yang dapat dipergunakan PT TASPEN PERSERO dalam melakukan monitoring dan meningkatkan pencapaian kapabilitas manajemen risiko TI serta meminimalisir dampak dan terjadinya risiko.

COBIT 5 merupakan seperangkat pedoman dan hasil dokumentasi versi terbaru yang dihasilkan dan diterbitkan oleh ITGI (*IT Governance Institute*), yang berfungsi untuk membantu auditor, pemangku kepentingan atau pengguna (*user*) dalam menghubungkan antara model kendali bisnis dan model kendali TI. COBIT 5 terbentuk dengan mengintegrasikan beberapa *framework* lain seperti Risk IT *framework*, VAL IT 2.0 dan COBIT 4.1. Selain itu COBIT 5 juga menyesuaikan antara *best practices* yang ada seperti ITIL V3, TOGAF dan standart relevan dari ISO.

Menurut ISACA (2012), COBIT 5 mempunyai dua proses yang membahas mengenai manajemen risiko Teknologi Informasi (TI), yaitu EDM03 dan APO12.

1. EDM03 (*Ensure Risk Optimisation*)

Bertujuan untuk memastikan tingkat risiko dan besarnya toleransi yang dapat diterima perusahaan telah dipahami, diartikulasikan dan dikomunikasikan dengan baik, serta memastikan apakah risiko yang terkait dengan TI telah diidentifikasi dan dikelola dengan baik. Proses EDM03 terdiri dari EDM03.01 (*Evaluate Risk Management*), DM03.02 (*Direct Risk Management*) dan EDM03.03 (*Monitor Risk Management*).

2. APO12 (*Manage Risk*)

Bertujuan untuk mengidentifikasi, menilai dan mengurangi risiko terkait dengan TI agar tidak melebihi batas toleransi yang telah ditentukan organisasi. Dan mengintegrasikan manajemen risiko TI dengan manajemen risiko perusahaan (ERM). Proses ini terdiri dari APO12.01 (*Collect Data*), APO12.02 (*Analyse Risk*), APO12.03 (*Maintain A Risk Profile*), APO12.04 (*Articulate Risk*), APO12.05 (*Define a Risk Management Action Portofolio*) dan APO12.06 (*Respond to Risk*).

Dari hasil studi pustaka yang telah dilakukan, peneliti menggunakan COBIT 5

sebagai kerangka kerja untuk mengevaluasi manajemen resiko teknologi informasi pada PT TASPEN. Dimana fokus pembahasan evaluasi manajemen resiko teknologi informasi menggunakan kerangka kerja COBIT 5 terdapat pada domain proses APO12 (*Manage Risk*) dan EDM03 (*Ensure Risk Optimisation*).

## 2. METODE PENELITIAN

Jenis penelitian ini adalah penelitian studi kasus, dimana peneliti melakukan analisis manajemen resiko teknologi informasi di PT TASPEN. Penelitian ini bersifat penelitian deskriptif yang menggunakan pendekatan kualitatif. Pendekatan kualitatif yaitu penelitian yang menghasilkan data deskriptif berupa kata-kata tertulis atau lisan dari orang-orang dan perilaku yang dapat diamati (Bogdan dan Tylor, 1990). Berikut ini adalah tahapan-tahapan yang dilakukan oleh peneliti dalam melakukan penelitian:

1. Menentukan objek dan subjek penelitian, menentukan kerangka kerja yang tepat serta menggali informasi yang relevan**.**
2. Melakukan pengumpulan data sekunder dan primer, dengan menggunakan metode penyebaran kuesioner, observasi, dan wawancara kepada pihak yang berwenang.
3. Mendeskripsikan kondisi umum organisasi yang meliputi tujuan organisasi, penerapan teknologi informasi dan pihak–pihak yang bertanggung jawab berdasarkan RACI *Chart*.
4. Melakukan analisis penilaian *Capability Level* berdasarkan kerangka kerja COBIT 5 khususnya domain proses EDM03 (*Ensure Risk Optimisation*) dan APO12 (*Manage Risk*).
5. Melakukan *gap analysis*, *risk assessment* dan menentukan langkah mitigasi untuk setiap risiko yang melebihi batas toleransi organisasi.
6. Membuat rekomendasi yang berisi solusi potensial dengan tujuan untuk meningkatkan nilai kapabilitas organisasi.
7. Menyusun kesimpulan yang berisi ringkasan tentang semua langkah yang telah dilalui dalam proses penelitian, guna menjawab rumusan masalah dan tujuan dari penelitian.

## 3. HASIL DAN PEMBAHASAN

### 3.1 Tabel RACI Chart

RACI Chart memiliki fungsi pada tingkat proses tanggung jawab untuk peran pada struktur organisasi suatu perusahaan. RACI Chart mendefinisikan kewenangan seeorang di dalam suatu perusahaan yang berbasis TI.Berikut ini merupakan RACI Chart pada domain APO12 dan EDM03, yang kemudian akan digunakan untuk menentukan responden.

**APO12 RACI Chart**

| Key Management Practice | Board | Chief Executive Officer | Chief Financial Officer | Chief Operating Officer | Business Executives | Business Process Owners | Strategy Executive Committee | Steering (Programmes/Projects) Committee | Project Management Office | Value Management Office | Chief Risk Officer | Chief Information Security Officer | Architecture Board | Enterprise Risk Committee | Head Human Resources | Compliance | Audit | Chief Information Officer | Head Architect | Head Development | Head IT Operations | Head IT Administration | Service Manager | Information Security Manager | Business Continuity Manager | Privacy Officer |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **APO12.01** Collect data. | | I | | | | R | | | R | | R | R | | I | | C | C | A | R | R | R | R | R | R | R | R |
| **APO12.02** Analyse risk. | | I | | | | R | | | C | | R | C | | I | | R | R | A | C | C | C | C | C | C | C | C |
| **APO12.03** Maintain a risk profile. | | I | | | | R | | | C | | A | C | | I | | R | R | R | C | C | C | C | C | C | C | C |
| **APO12.04** Articulate risk. | | I | | | | R | | | C | | R | C | | I | | C | C | A | C | C | C | C | C | C | C | C |
| **APO12.05** Define a risk management action portfolio. | | I | | | | R | | | C | | A | C | | I | | C | C | R | C | C | C | C | C | C | C | C |
| **APO12.06** Respond to risk. | | I | | | | R | | | R | | R | R | | I | | C | C | A | R | R | R | R | R | R | R | R |

Gambar 1. APO12 RACI Chart (COBIT 5: Enabling Process, page 108, ISACA)

**EDM03 RACI Chart**

| Key Governance Practice | Board | Chief Executive Officer | Chief Financial Officer | Chief Operating Officer | Business Executives | Business Process Owners | Strategy Executive Committee | Steering (Programmes/Projects) Committee | Project Management Office | Value Management Office | Chief Risk Officer | Chief Information Security Officer | Architecture Board | Enterprise Risk Committee | Head Human Resources | Compliance | Audit | Chief Information Officer | Head Architect | Head Development | Head IT Operations | Head IT Administration | Service Manager | Information Security Manager | Business Continuity Manager | Privacy Officer |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **EDM03.01** Evaluate risk management. | A | R | C | C | R | C | R | | | I | R | C | | I | C | C | C | R | C | | | | | | | C |
| **EDM03.02** Direct risk management. | A | R | C | C | R | C | R | I | I | I | R | I | I | I | C | C | C | R | C | I | I | I | I | I | I | I |
| **EDM03.03** Monitor risk management. | A | R | C | C | R | C | R | I | I | I | R | R | I | I | C | C | C | R | C | I | I | I | I | I | I | C |

Gambar 2. EDM03 RACI Chart (COBIT 5: Enabling Process, page 39, ISACA)

Pada Tabel 1. RACI chart APO12 dan EDM03, yang didapatkan dari COBIT 5: *Enabling Process*, page 108. 2012 ISACA dapat diketahui *Responsible, Accountable,*

*Consulted* dan *Informed* yang sesuai dan berkompeten sebagai responden dalam proses pengisian kuesioner domain APO12 dan domain EDM03 di PT TASPEN.

Tabel 1. RACI Chart APO12 dan EDM03

| No. | *Management Practice* | RACI Chart | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | APO12 | | | | EDM03 | | | |
| | | R | A | C | I | R | A | C | I |
| 1 | *Chief Excecutive Officer* | | | | 6 | 3 | | | |
| 2 | *Head IT Operations* | 2 | | 4 | | | | | 2 |
| 3 | *Head IT Administration* | 2 | | 4 | | | | | 2 |

Berdasarkan dari Tabel 1., hasil dari penentuan responden menggunakan RACI Chart doman APO12 dan domain EDM03 didapatkan hasil Head IT Operations memiliki nilai *Responsible* dengan jumlah 2 dan nilai *Consulted* dengan jumlah 4. Kemudian *Head IT Administration* memiliki nilai *Responsible* dengan jumlah 2 dan nilai *Consulted* dengan jumlah 4, dan *Chief Excecutive Officer* memiliki nilai *Informed* dengan jumlah 6. Berdasarkan fungsi RACI Chart , Staff IT berperan sebagai *Head IT Operations*, Staff Admin berperan sebagai *Head IT Administration* dan Kepala kantor berperan sebagai *Chief Excecutive Office*. Sehingga dapat disimpulkan bahwa Staff IT, Staff Admin dan Kepala Bagian Teknologi Informatika berkompeten menjadi responden dalam pengisian kuesioner pada domain APO proses APO12 dan domain EDM proses EDM03.

**3.2 Hasil Kuesioner**

Berdasarkan hasil pembuatan RACI *Chart*, dapat diketahui bahwa pihak yang berhak menjadi responden untuk mengisi kuesioner adalah sejumlah tiga orang, antara lain Kepala Bagian TeknologiInformatika, Staf ITdan Staff Admin. Berikut ini adalah hasil rekapitulasi kuesioner domain EDM03 dan APO12:

Tabel 2.RekapitulasiHasilKuesioner Domain EDM03

| **Tujuan** | Memastikan bahwa risiko TI perusahaan tidak melebihi kemampuan dan toleransi perusahaan dalam menerima risiko, serta mengidentifikasi dan mengelola dampak risiko TI terhadap nlai-nilai perusahaan, dan mengurangi terjadinya kegagalan. | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Proses *Ensure Risk Optimisation*** | ***Level* 0** | ***Level* 1** | ***Level* 2** | | ***Level* 3** | | ***Level* 4** | | ***Level* 5** | |
| | | PA 1.1 | PA 2.1 | PA 2.2 | PA 3.1 | PA 3.2 | PA 4.1 | PA 4.2 | PA 5.1 | PA 5.2 |

| | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| ***Rating* berdasarkan presentase** | 100% | 100% | 100 % | 100 % | 50 % | | | | | |
| ***Rating* berdasarkan warna** | | | | | | | | | | |

Tabel 3.RekapitulasiHasilKuesioner Domain APO12

| **Tujuan** | Mengintegrasikan *management* dari risikoTI perusahaan keseluruhan ERM (*Enterprise Risk Management*), dan menyeimbangkan biaya dan keuntungan dari mengelola TI perusahaan. | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| **Proses *Manage Risk*** | ***Level* 0** | ***Level* 1** | ***Level* 2** | | ***Level* 3** | | ***Level* 4** | | ***Level* 5** | |
| | | PA 1.1 | PA 2.1 | PA 2.2 | PA 3.1 | PA 3.2 | PA 4.1 | PA 4.2 | PA 5.1 | PA 5.2 |
| ***Rating* berdasarkan presentase** | 100% | 100% | 100 % | 100 % | | | | | | |
| ***Rating* berdasarkan warna** | | | | | | | | | | |

Hasil dari penilaian ke tiga responden dengan domain EDM03 dan APO12 yang terdapat pada tabel 2. dan tabel 3. didapatkan nilai *capability level* untuk subdomain EDM03 berada pada level 2 (*Managed Process*) dan untuk APO12 berada pada level 2 (*Managed Process*). Pada subdomain EDM03 untuk level 1 sampai dengan 2 sudah mencapai *Fully Achieved*. Karena pada level berikutnya nilai masih berada pada *Largerly Achieved*, maka untuk subdomain ini belum dapat dikatakan berada pada level 3. Sedangkan subdomain APO12 masih berada pada level 2, dikarenakan pada level 3 belum ada yang mencapai level *Largely Achieved*.

### 3.3 Analisis *Capability Level*

Berdasarkan data kuesioner yang telah divalidasi dengan data hasil wawancara dan observasi terhadap bukti pendukung. Dihasilkan nilai *capability level* untuk domain proses EDM03 dan APO12 di PT TASPEN PERSERO berada pada level 1 (*Managed*

*Process*).

Tabel 4. Hasil Analisis *Capability Level*

| Nama Proses | Level Saat Ini | Level Target |
|---|---|---|
| EDM03 (*Risk Optimisation*) | 2 | 3 |
| APO12 (*Managed Process*) | 2 | 3 |

Dan target pencapaian yang ditetapkan perusahaan untuk domain proses EDM03 dan APO12 adalah naik 1 tingkat dari pencapaian saat ini, yaitu berada pada level 3 (*Established Process*). Sehingga dapat disimpulkan dari hasil pencapaian saat ini dan target pencapaian *capability level* yang telah ditentukan, didapatkan jarak atau gap sebesar 1 level/tingkat.

**3.4 Rekomendasi**

Rekomendasi dibuat mengacu kepada hasil anailisis *capability level* guna mengetahui pencapaian menjalankan proses saat ini dan analisis *gap* guna mengetahui target yang ditentukan oleh perusahaan dan nilai kesenjangan yang terjadi. Rekomendasi dibuat dengan tujuan dapat meminimalisir *gap* antara pencapaian saat ini dan target yang telah ditentukan, maupun untuk mencapai target yang telah ditentukan oleh PT TASPEN PERSERO dalam melakukan perbaikan manajemen risiko teknologi informasi. Berikut adalah rekomendasi berdasarkan domain proses EDM03 dan APO12:

1. PT TASPEN PERSERO disarankan untuk membentuk unit atau team khusus yang mempunyai tanggung jawab dalam melakukan pembahasan dan pengelolaan terkait penerapan manajemen risiko Teknologi Informasi didalam perusahaan.
2. Menerbitkan dokumen kontrol berupa *check list* pada saat implementasi penerapan manajemen risiko.
3. Membuat dokumen kontrol performa *staff*, yang terdiri dari hasil kinerja dari penerapan manajemen risiko.
4. Memperkuat kegiatan monitoring penerapan manajemen risiko teknologi informasi untuk bahan evaluasi, agar penerapan manajemen risiko dapat terus diperbaharui dari kekurangan yang belum teridentifikasi.
5. Menerbitkan dokumen tertulis yang berisikan tentang risk assessment yang dikelola

perusahaan sampai dengan langkah mitigasi risiko beserta risk respond terhadap semua risiko TI.

6. Menerbitkan suatu kebijakan dalam melakukan pengukuran terhadap pengelolaan standart proses.
7. Meningkatkan perumusan proses standart yang akan diterapkan, mendefinisikan detail tanggung jawab dan otoritas pelaksanaan aktivitas.
8. Melakukan pengukuran terhadap sejauh mana proses standar dikelola untuk mendukung pengerjaan dari proses yang telah didefinisikan.
9. Melakukan analisis *Cost Benefit* untuk melakukan peramalan frekuensi besarnya kerugian yang harus tanggung maupun keuntungan yang akan diperoleh perusahaan ketika penanganan terhadap setiap skenario risiko teknologi informasi dilakukan.
10. Membuat program-program khusus yang berisi kegiatan pemantauan, review, pengendalian dan pengelolaan terhadap penerapan manajemen risiko teknologi informasi.
11. Mengumpulkan data-data relevan yang dapat dijadikan sumber untuk memastikan kecocokan dan keefektifan proses sebagai bahan evaluasi untuk perbaikan terus-menerus dari proses.
12. PT TASPEN PERSERO harus memastikan kebijakan tentang manjemen risiko yang berkaitan dengan teknologi informasi juga harus terintegrasi atau selaras dengan manajemen risiko secara keseluruhan perusahaan.

## 4. KESIMPULAN

Berdasarkan hasil pembahasan terkait manajemen risiko Teknologi Informasi (TI) yang telah diterapkan oleh PT TASPEN PERSERO, maka dapat diperoleh kesimpulan penelitian sebagai berikut:

1. Proses evaluasi terhadap penerapan manajemen risiko Teknologi Informasi (TI) pada PT TASPEN PERSERO menggunakan kerangka kerja COBIT 5 khususnya domain proses EDM03 *(Ensure Risk Optimation)* dan APO12 *(Manage Risk)* menghasilkan beberapa hal berikut ini:

a. Kemampuan PT TASPEN PERSERO dalam menjalankan proses *Ensure Risk* Optimation (EDM03) dan *Managed Risk* (APO12) sama-sama berada pada level 1 yaitu

*PerformedProcess* yang berarti pada proses *Ensure Risk Optimation* dan *Managed Risk* di PT TASPEN telah diimplementasikan, namun belum digunakan secara optimal dalam mendukung bisnis proses dalam perusahaan.

b. Besarnya *gap* yang terbentuk antara nilai *capability level* yang telah saat ini dengan nilai *capability level* yang ingin dicapai untuk domain proses EDM03 dan APO12 masing-masing adalah sebesar 2.

2. Hasil rekomendasi dan langkah mitigasi yang diberikan untuk bahan pertimbangan rencana perbaikan manajemen risiko Teknologi Informasi (TI) di PT TASPEN PERSERO adalah sebagai berikut:

a. Terdapat 12 rekomendasi yang telah dibuat, supaya dapat meminimalisir kesenjangan (gap) dan nilai capability level pada domain proses EDM03 dan APO12 dapat naik dua tingkat ke level 3.

b. Untuk mengatasi kelemahan dan permasalahan PT TASPEN PERSERO dalam melakukan pengembangan Sistem Telemetri saat ini, untuk menutupi kekurangan dari segi pendidikan yang dimiliki sebagian staff PT TASPEN PERSERO, untuk mengatasi masalah terkait kurangnya staff yang bertugas dalam mengelola teknologi informasi beserta manajemen risiko TI dan permasalahan tentang pembagian tugas yang menumpuk untuk staff TI, serta untuk mengatasi dan mengurangi dampak risiko yang diakibatkan oleh beban penyimpanan yang tinggi.

## 5. SARAN

Berdasarkan hasil analisis manajemen risiko TI yang dilakukan, terdapat beberapa poin saran yang dapat diuraikan untuk pengembangan analisis manajemen risiko TI PT TASPEN dan untuk penelitian selanjutnya.

1. Evaluasi pelaksanaan manajemen risiko teknologi informasi perlu dilakukan secara terus menerus dan terjadwal.
2. Hasil evaluasi dan program perbaikan dapat dijadikan masukan untuk program kerja PT TASPEN PERSERO agar pengelolaan manajemen risiko TI lebih baik.
3. Perlu dilakukan penelitian dengan menggunakan framework manajemen risiko yang lain untuk menjadi pembanding.
4. Program perbaikan perlu dipantau pelaksanaannya agar sesuai dengan harapan yang

diinginkan.

## DAFTAR PUSTAKA

Djojosoedarso, Soeisno, 2003. Prinsip-PrinsipManajemenRisikodanAsuransi, EdisiPertama, SalembaEmpat,Jakarta.

Dyahaloka, Astri., 2016. EvaluasiManajemenResiko E-Procurement Menggunakan COBIT 5 IT Risk (StudiKasus : PT. Pertamina (Persero)). Malang :UniversitasBrawijaya.

Husein, G.M. and Imbar, R.V., 2015. Analisis Manajemen Risiko Teknologi Informasi Penerapan Pada Document Management System di PT. JABAR TELEMATIKA (JATEL). Jurnal Teknik Informatika dan Sistem Informasi

ISACA., 2012. COBIT 5 : A Bussiness Framework for the Governance and Management of Enterprise IT. Rolling Meadows : ISACA.

ISACA., 2012. COBIT 5 : Enabling Process. Rolling Meadows : ISACA.

ISACA., 2012. COBIT 5 : The Risk IT Practitioner Guide. Rolling Meadows : ISACA.

ISACA., 2012. COBIT 5 : For Risk. Rolling Meadows : ISACA.

ISACA., 2012. COBIT 5 : Self-Assessment Guide. Rolling Meadows : ISACA.

ITGI., 2003. Broad Briefing on IT Governance 2nd Edition. Rolling Meadows : IT Governance Institute.

Permenkominfo. 2007. Panduan Umum Tata Kelola Teknologi Informasi Dan Komunikasi Nasional Versi 1. Jakarta : Menteri Komunikasi Dan Informatika.

Pratama, Enda E., and Suhardi., 2013. Analisis Nilai & Manajemen Risiko Teknologi Informasi (Studi Kasus PT. Bank Tabungan Negara. Tbk). Bandung : Institute Teknologi Bandung. Tersedia di : <http://www.academia.edu/> [Diakses 6 Oktober 2016].

Samaptoaji, Sigit, 2014. Evaluasi Pengelolaan Risiko Teknologi Informasi (TI) pada Instansi Pemerintah : Studi Kasus Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementrian Dalam Negeri. Jakarta : Universitas Indonesia.

Setiawan, Alexander, 2009. Evaluasi Penerapan Teknologi Informasi Di Perguruan Tinggi Swasta Yogyakarta Dengan Menggunakan Model Cobit Framework. Seminar Nasional Aplikasi Teknologi Informasi (SNATI). Vol. 1. No. 1. Tersedia di: <http:// www.jurnal.uii.ac.id/index.php> [Diakses 11 November 2016].

Suwarno, Fajrin Rizkia P., 2014. Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Pada Proses Manage Relationship (APO08) (Studi Kasus : PT. OTO Multiartha). Jakarta : Universitas Islam Negeri Syarif Hidayatullah.

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

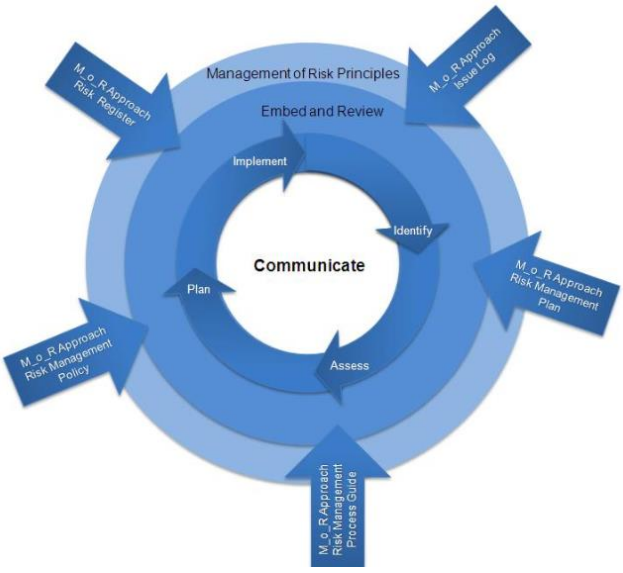
Nama : Rio Permata
NIM : 182420108
Kelas : MTI Reguler B
Mata Kuliah : ITSM

# IT RISK MANAGEMENT PADA ITSM

Manajemen resiko TI merupakan proses identifikasi resiko, penilaian resiko, dan pengambilan langkah-langkah untuk menurunkan resiko sampai level yang dapat diterima. Terdapat tahapan-tahapan penting dalam perencanaan manajemen resiko TI:

1. Identifikasi dan klasifikasi resiko TI
2. Penilaian resiko TI (Business Impact Analysis) dan menentukan prioritas
3. Strategi penanggulangan resiko TI –identifikasi pengendalian TI
4. Implementasi dan dokumentasi dari penanggulangan resiko (pengendalian TI)
5. Pendekatan portofolio resiko TI dan keselarasan dengan strategi bisnis
6. Pengawasan berkala terhadap tingkat resiko TI dan audit.

Management of Risk (M_o_R)merupakan metodologi standar yang dapatdigunakan untukmanajemen resikoTIserta menilai resiko di organisasi(OGC, 2007).Pada gambar 1 merupakankerangka kerja M_o_R.




Gambar 1. Framework Management Risk

Berikut ini merupakan penjelasan dari gambar di atas:

- Prinsip M_o_R : prinsip-prinsip tersebut merupakan esensi dalam pengembangan praktik manajemen resiko yang baik dan diturunkan dari prinsip-prinsip tatakelola perusahaan (corporate governance).
- Pendekatan M_o_R : pendekatan organisasi untuk prinsip-prinsip tersebut dibutuhkan untuk mendefinisikan dan persetujuan dalam dokumen berikut:
    a. Kebijakan manajemen resiko
    b. Panduan proses
    c. Perencanaan
    d. Registrasi resiko
    e. Permasalahan log
- Proses M_o_R –berikut ini menjelaskan empat tahapan aktivitas dalam manajemen resiko:
    a. Identifikasi –ancaman dan peluang dalam aktivitas yang dapat mempengaruhi kemampuan dalam mencapai tujuan
    b. Menilai–pemahaman net effect dari identifikasi ancaman dan peluang aktivitas yang dilakukan.
    c. Merencanakan–mempersiapkan tanggapan manajemen secara spesifik yang dapat mengurangi ancaman dan memaksimalkan peluang.
    d. Implementasi –penerapan rencana manajemen resiko, mengawasi efektivitas dan mengambil langkah yang diperlukan dalam menanggulangi ekspektasi yang tidak sesuai

Referensi : *Irfan Maliki, 2010.Manajemen Resiko Teknologi Informasi I Untuk Keberlangsungan Layanan Publik Menggunakan Framework Information Technology Infrastructure Library (ITIL Versi3)*

**Contoh Kasus :**

Menurut jurnal ***"Evaluasi Manajemen Risiko Teknologi Informasi Pada Perusahaan BUMN Menggunakan Standar COBIT 5 (Studi Kasus: PT TASPEN PERSERO)"*** *Riyan Abdul Aziz, Kusrini, Sudarmawan (2018)* mengungkapkan bahwa :

Untuk mengukur pencapaian PT TASPEN PERSERO dalam mengelola penerapan manajemen risiko TI dibutuhkan sebuah evaluasi. Evaluasi tersebut terdiri dari beberapa tahapan yang meliputi analisis capability level, gap dan risk assessment. Dari tahapan evaluasi tersebut dihasilkan sebuah rekomendasi dan strategi mitigasi yang dapat dipergunakan PT

TASPEN PERSERO dalam melakukan monitoring dan meningkatkan pencapaian kapabilitas manajemen risiko TI serta meminimalisir dampak dan terjadinya risiko.

COBIT 5 merupakan seperangkat pedoman dan hasil dokumentasi versi terbaru yang dihasilkan dan diterbitkan oleh ITGI (IT Governance Institute), yang berfungsi untuk membantu auditor, pemangku kepentingan atau pengguna (user) dalam menghubungkan antara model kendali bisnis dan model kendali TI. COBIT 5 terbentuk dengan mengintegrasikan beberapa framework lain seperti Risk IT framework, VAL IT 2.0 dan COBIT 4.1.

Selain itu COBIT 5 juga menyesuaikan antara best practices yang ada seperti ITIL V3, TOGAF dan standart relevan dari ISO. Menurut ISACA (2012), COBIT 5 mempunyai dua proses yang membahas mengenai manajemen risiko Teknologi Informasi (TI), yaitu EDM03 dan APO12.

1. EDM03 (Ensure Risk Optimisation)

   Bertujuan untuk memastikan tingkat risiko dan besarnya toleransi yang dapat diterima perusahaan telah dipahami, diartikulasikan dan dikomunikasikan dengan baik, serta memastikan apakah risiko yang terkait dengan TI telah diidentifikasi dan dikelola dengan baik. Proses EDM03 terdiri dari EDM03.01 (Evaluate Risk Management), DM03.02 (Direct Risk Management) dan EDM03.03 (Monitor Risk Management).

2. APO12 (Manage Risk)

   Bertujuan untuk mengidentifikasi, menilai dan mengurangi risiko terkait dengan TI agar tidak melebihi batas toleransi yang telah ditentukan organisasi. Dan mengintegrasikan manajemen risiko TI dengan manajemen risiko perusahaan (ERM). Proses ini terdiri dari APO12.01 (Collect Data), APO12.02 (Analyse Risk), APO12.03 (Maintain A Risk Profile), APO12.04 (Articulate Risk), APO12.05 (Define a Risk Management Action Portofolio) dan APO12.06 (Respond to Risk).

Dari hasil studi pustaka yang telah dilakukan, digunakan COBIT 5 sebagai kerangka kerja untuk mengevaluasi manajemen resiko teknologi informasi pada PT TASPEN. Dimana fokus pembahasan evaluasi manajemen resiko teknologi informasi menggunakan kerangka kerja COBIT 5 terdapat pada domain proses APO12 (Manage Risk) dan EDM03 (Ensure Risk Optimisation).

**Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer** e-ISSN: 2548-964X
Vol. 2, No. 1, Januari 2018, hlm. 101-110 http://j-ptiik.ub.ac.id

# Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Kerangka Kerja COBIT 5 (Studi Kasus Pada Perum Jasa Tirta I Malang)

**M. Habibullah Arief[1], Suprapto[2]**

Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]m.habibullaharief@gmail.com, [2]spttif@ub.ac.id

**Abstrak**

Besarnya kontribusi sistem telemetri guna menunjang tugas utama Perum Jasa Tirta I Malang dalam melakukan penanggulangan banjir menjadikannya sebagai sistem vital yang harus terhindar dari risiko yang dapat menghambat dan mempengaruhi hasil monitoring banjir, yang berpotensi menimbulkan kerugian bagi masyarakat sekitar sungai. Untuk meminimalisir dampak risiko tersebut, Perum Jasa Tirta I Malang telah membuat kebijakan mengenai manajemen risiko diantaranya mengelola profil risiko. Untuk mengetahui pencapaian penerapan manajemen risiko teknologi informasi Perum Jasa Tirta I Malang penulis melakukan evaluasi menggunakan kerangka kerja COBIT 5 pada domain proses EDM03 (*Ensure Risk Optimisation*) dan APO12 (*Manage Risk*). Dari hasil evaluasi terhadap data yang diperoleh melalui penyebaran kuesioner, wawancara dan observasi didapatkan nilai *capability level* domain EDM03 dan APO12 sama-sama berada pada level 2. Untuk target *capability level* yang ingin dicapai Perum Jasa Tirta I Malang terhadap kedua domain proses tersebut berada pada level 3, dengan demikian menghasilkan *gap* sebesar 1 level. Selanjutnya juga diperlukan identifikasi risiko untuk mengetahui apakah kontrol saat ini telah sesuai serta mampu menurunkan *impact* dan *probability* suatu risiko dengan melakukan penilaian risiko (*Risk Assessment*). Berdasarkan hasil evaluasi tersebut disusunlah rekomendasi dan strategi mitigasi yang dapat dipergunakan Perum Jasa Tirta I Malang dalam melakukan perbaikan penerapan manajemen risiko teknologi informasi.

**Kata Kunci**: *COBIT 5, capability level, gap, risk assessment, rekomendasi, strategi mitigasi*

**Abstract**

*The amount of contribution from telemetry system to support the main job of Perum Jasa Tirta I Malang on handling the flood prevention, making telemetry system as a vital system that must be spared from the risks. That risk might obstruct and effect the result of flood monitoring which potencially harmfull to society. Perum Jasa Tirta I Malang was established a policies about risk management, include managing the risk profile. An evaluation on the implementation of information technology risk management in Perum Jasa Tirta I Malang was done to measure the capability level accomplishment. Cobit 5 framework, especially in process domain EDM03 (Ensure Risk Optimisation) and APO12 (Manage Risk), was used as the basis of the evaluations, it turned out that capability level for both of process domain EDM03 and APO12 were on level 2. Target of capability level that want to be achieved by Perum Jasa Tirta I Malang for both of process domain EDM03 and APO12 are on level 3. In other words, the interval of deviation (gap) from the two domain process was 1. And then, risk identification was needed to figure out wether the current control was appropriated. Besides that, risk assessment was also needed to reduce impact and probability of the the risks. From the evaluation result, recomendation and mitigation strategy ware made to support the improvement for the implementation of risk management information and technology at Perum Jasa Tirta I Malang.*

**Keywords**: *COBIT 5, capability level, gap, risk assessment, recommendations, mitigation strategies*

## 1. PENDAHULUAN

Jasa Tirta I Malang merupakan Badan Usaha Milik Negara (BUMN) yang berbentuk Perum, yang mempunyai tugas mengelola SDA (Sumber Daya Air). Dalam mengelola bidang Sumber Daya Air, Perum Jasa Tirta I Malang juga berkewajiban untuk melindungi masyarakat dari daya rusak air dengan melakukan kegiatan penanggulangan banjir. Dalam menjalankan kewajiban tersebut Perum Jasa Tirta I Malang didukung oleh sebuah teknologi yang berfungsi untuk melakukan monitoring curah hujan dan

tinggi muka air, teknologi tersebut bernama Sistem Telemetri. Dengan adanya sistem tersebut dampak dari terjadinya banjir dapat diminimalisir.

Besarnya kontribusi sistem telemetri guna menunjang tugas utama Perum Jasa Tirta I Malang dalam melakukan penanggulangan banjir menjadikannya sebagai sistem vital yang harus terhindar dari risiko-risiko yang dapat menghambat/mempengaruhi hasil monitoring banjir, yang berpotensi menimbulkan kerugian bagi masyarakat sekitar sungai. Untuk meminimalisir dampak risiko tersebut, Perum Jasa Tirta I Malang telah membuat kebijakan mengenai penerapan manajemen risiko TI diantaranya adalah mengelola profil risiko. Dalam penerapannya, sistem telemetri tidak sepenuhnya terhindar dari berbagai risiko. Risiko tersebut meliputi peralatan telemetri menghasilkan data yang tidak akurat/presisi, data *corrupt*, sistem telemetri masih dalam tahap pengembangan, kurangnya *staff* TI, belum adanya unit khusus yang menangani manajemen risiko TI pada Perum Jasa Tirta I Malang.

Untuk mengukur pencapaian Perum Jasa Tirta I Malang dalam mengelola penerapan manajemen risiko TI dibutuhkan sebuah evaluasi. Evaluasi tersebut terdiri dari beberapa tahapan yang meliputi analisis *capability level*, *gap* dan *risk assessment*. Dari tahapan evaluasi tersebut dihasilkan sebuah rekomendasi dan strategi mitigasi yang dapat dipergunakan Perum Jasa Tirta I Malang dalam melakukan monitoring dan meningkatkan pencapaian kapabilitas manajemen risiko TI serta meminimalisir dampak dan terjadinya risiko.

COBIT 5 merupakan salah satu kerangka kerja yang dapat dipergunakan oleh peneliti dalam melakukan evaluasi manajemen risiko TI pada Perum Jasa Tirta I Malang. Didalam COBIT 5 hanya terdapat 2 domain proses yang menangani manajemen risiko Teknologi Informasi, yaitu domain proses EDM03 (*Ensure Risk Optimisatin*) dan APO12 (*Manage Risk*).

## 2. LANDASAN KEPUSTAKAAN

### 2.1 Kajian Pustaka

Penulis melakukan kajian pustaka terhadap penelitian dari Astri Dyahaloka dengan judul Evaluasi Manajemen Risikio *E-Procurement* Menggunakan COBIT 5 IT *Risk* (Studi Kasus: PT. Pertamina (Persero)) karena memiliki topik dan kerangka kerja yang sama. Yang kedua adalah penelitian dari Sigit Samaptoaji dengan judul "Evaluasi Pengelolaan Risiko Teknologi Informasi (TI) Pada Instansi Pemerintah: Studi Kasus Direktorat Jenderal Kependudukan Dan Pencatatan Sipil Kementerian Dalam Negeri" yang dipergunakan sebagai acuan dan pedoman dalam melakukan *Risk Assessment* dan mitigasi.

### 2.2 Manajemen Risiko TI

Risiko TI merupakan risiko yang diakibatkan dari penggunaan teknologi informasi, yang berpotensi menimbulkan dampak. Upaya dalam mengelola risiko tersebut dapat disebut dengan manajemen risiko TI.

Menurut Westerman (2007) manajemen risiko TI (Teknologi Informasi) merupakan gabungan beberapa proses yang terdiri dari identifikasi, pengkajian, pengembangan stategi mitigasi dan komunikasi risiko TI yang berpotensi menimbulkan dampak negatif dan dapat merugikan organisasi.

### 2.3 COBIT 5

COBIT 5 merupakan seperangkat pedoman dan hasil dokumentasi versi terbaru yang dihasilkan dan diterbitkan oleh ITGI (*IT Governance Institute*), yang berfungsi untuk membantu auditor, pemangku kepentngan atau pengguna (*user*) dalam menghubungkan antara model kendali bisnis dan model kendali TI.

COBIT 5 terbentuk dengan mengintegrasikan beberapa *framework* lain seperti Risk IT *framework*, VAL IT 2.0 dan COBIT 4.1. Selain itu COBIT 5 juga menyesuaikan antara *best practices* yang ada seperti ITIL V3, TOGAF dan standart relevan dari ISO.

Menurut ISACA (2012) terdapat tujuh tahapan dalam siklus implementasi COBIT 5, yaitu:

1. *Initiate Programme*, merupakan tahap untuk mengidentifikasi penggerak perusahaan.
2. *Define Problems and Opportunities*, merupakan tahap untuk melakukan penilaian *capability level* untuk mengetahui kondisi organisasi saat ini dan menemukan kekurangan yang dimiliki.
3. *Define Road Map*, merupakan tahap untuk melakukan penetapan target dan analisis *gap* untuk meningkatkan upaya perbaikan dan mengidentifikasi adanya solusi potensial.
4. *Plan Programme*, merupakan tahap untuk

merencanakan solusi yang dianggap tepat untuk diterapkan.

5. *Execute Plan*, merupakan tahap untuk mengimplementasikan solusi yang telah direncanakan serta melakukan pemantauan terhadap keselarasan bisnis.
6. *Realise Benefits*, merupakan tahap transisi secara berkelanjutan dengan menerapkan praktik tata kelola atau manajemen yang telah ditingkatkan kedalam proses bisnis dan memantau perkembangannya dengan memetakannya pada matriks berdasarkan kinerja dan manfaat yang ingin diperoleh.
7. *Review Effectiveness*, merupakan tahap untuk melakukan evaluasi keberhasilan yang telah dicapai, kemudian melakukan identifikasi seluruh kebutuhan perbaikan secara berkala.

Menurut ISACA (2012), COBIT 5 mempunyai dua proses yang membahas mengenai manajemen risiko Teknologi Informasi (TI), yaitu EDM03 dan APO12.

1. EDM03 (*Ensure Risk Optimisation*)
   Bertujuan untuk memastikan tingkat risiko dan besarnya toleransi yang dapat diterima perusahaan telah dipahami, diartikulasikan dan dikomunikasikan dengan baik, serta memastikan apakah risiko yang terkait dengan TI telah diidentifikasi dan dikelola dengan baik. Proses EDM03 terdiri dari EDM03.01 (*Evaluate Risk Management*), DM03.02 (*Direct Risk Management*) dan EDM03.03 (*Monitor Risk Management*)
2. APO12 (*Manage Risk*)
   Bertujuan untuk mengidentifikasi, menilai dan mengurangi risiko terkait dengan TI agar tidak melebihi batas toleransi yang telah ditentukan organisasi. Dan mengintegrasikan manajamen risiko TI dengan manajemen risiko perusahaan (ERM). Proses ini terdiri dari APO12.01 (*Collect Data*), APO12.02 (*Analyse Risk*), APO12.03 (*Maintain A Risk Profile*), APO12.04 (*Articulate Risk*), APO12.05 (*Define a Risk Management Action Portofolio*) dan APO12.06 (*Respond to Risk*).

### 2.4 *Risk Assessment*

ISACA (2012) menjelaskan bahwa secara umum *risk assessment* berfungsi untuk mengidentifikasi risiko potensial baik yang berasal dari internal maupun eksternal organisasi, dan menilai sejauh mana dampak yang ditimbulkan oleh risiko tersebut dapat mengganggu jalannya proses bisnis dan tujuan organisasi. Penilaian tersebut menghasilkan nilai *inherent risk* dan *residual risk*, yang dianalisis menggunakan perspektif *probability* dan *impact*.

Langkah perusahaan dalam merespon risiko dengan cara mengurangi besarnya *probability* (peluang) dan *impact* (dampak) yang ditimbulkan dari risiko disebut dengan *risk mitigation*.

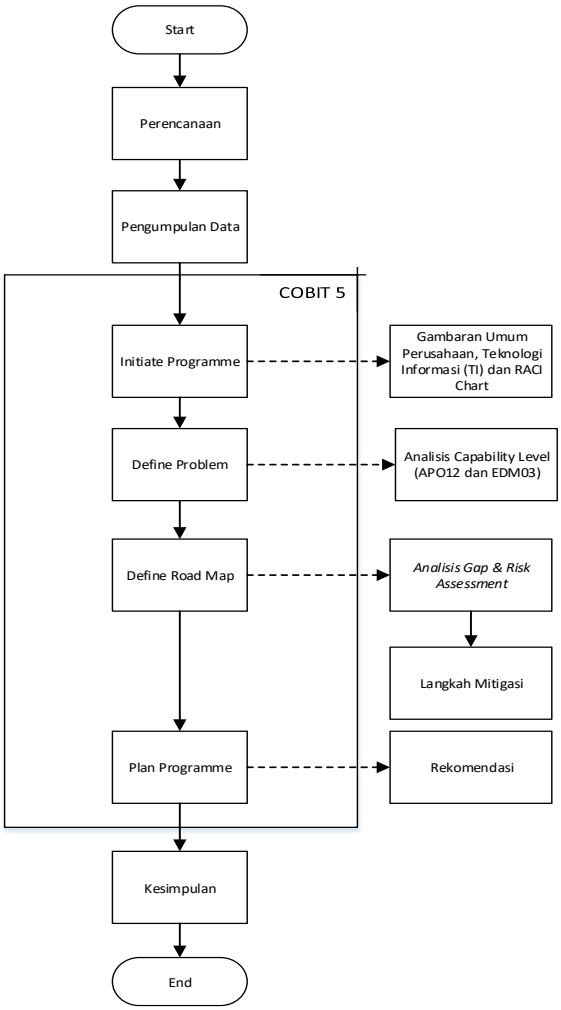
### 2.5 Sistem Telemetri

Sistem Telemetri merupakan sistem yang digunakan untuk memonitoring potensi banjir di Wilayah Sungai (WS). Sistem tersebut terdiri dari *software* yang dipergunakan di *master station* dan *hardware* yang terdiri dari sensor curah hujan dan tinggi muka air yang terdapat di stasiun pemantau. Data dari sensor akan dikirimkan ke *master station* untuk dikelola, yang nantinya dihasilkan status sungai. Agar ketika terdapat potensi banjir Perum Jasa Tirta I Malang akan segera mengetahuinya, dan dapat dengan cepat melakukan tindakan selanjutnya. Sehingga masyarakat di sekitar Wilayah Sungai (WS) dapat terhindar dari daya rusak air.

## 3. METODOLOGI

1. Menentukan objek dan subjek penelitian, menentukan kerangka kerja yang tepat serta menggali informasi yang relevan**.**
2. Melakukan pengumpulan data sekunder dan primer, dengan menggunakan metode penyebaran kuesioner, observasi, dan wawancara kepada pihak yang berwenang.
3. Mendeskripsikan kondisi umum organisasi yang meliputi tujuan organisasi, penerapan teknologi informasi dan pihak–pihak yang bertanggung jawab berdasarkan RACI *Chart*.
4. Melakukan analisis penilaian *Capability Level* berdasarkan kerangka kerja COBIT 5 khususnya domain proses EDM03 (*Ensure Risk Optimisation*) dan APO12 (*Manage Risk*).
5. Melakukan *gap analysis*, *risk assessment* dan menentukan langkah mitigasi untuk setiap risiko yang melebihi batas toleransi organisasi.
6. Membuat rekomendasi yang berisi solusi potensial dengan tujuan untuk meningkatkan nilai kapabilitas organisasi.
7. Menyusun kesimpulan yang berisi ringkasan tentang semua langkah yang telah

dilalui dalam proses penelitian, guna menjawab rumusan masalah dan tujuan dari penelitian.




**Gambar 1.** Diagram Alur Penelitian

## 4. HASIL

### 4.1 Hasil Kuesioner

Berdasarkan hasil pembuatan RACI *Chart*, dapat diketahui bahwa pihak yang berhak menjadi responden untuk mengisi kuesioner adalah sejumlah tiga orang, antara lain Kepala Bagian Hidro Informatika, Tenaga Ahli IT *Software* & *Database* dan bagian *Hardware*.

**Tabel 1.** Rekapitulasi Hasil Kuesioner

| ***Prosess Assesment Results*** | | | | | | | |
|---|---|---|---|---|---|---|---|
| Nama Proses | *Proces Capability Level* | | | | | | Total Responden |
| | 0 | 1 | 2 | 3 | 4 | 5 | |
| ***Evaluate, Direct, and Monitoring*** | | | | | | | |
| EDM03 (*Risk Optimisation*) | 0 | 0 | 3 | 0 | 0 | 0 | 3 |
| ***Align, Plan, and Organise (APO)*** | | | | | | | |
| APO12 (*Manage Risk*) | 0 | 0 | 3 | 0 | 0 | 0 | 3 |

Dari hasil pengisian kuesioner oleh ketiga responden tersebut, yang selanjutnya juga telah dilakukan proses validasi diperoleh nilai *capiability level* untuk domain proses EDM03 (*Risk Optimisation*) dan APO12 (*Manage Risk*) Perum Jasa Tirta I Malang berada pada level 2 (*Managed Process*).

### 4.2 Hasil Wawancara dan Observasi

Wawancara dilakukan dua kali, yang pertama bertujuan untuk mengetahui gambaran umum tentang perusahaan. Dan wawancara yang kedua berfungi sebagai sarana untuk melakukan validasi terhadap hasil kuesioner, yang nantinya juga didukung oleh kegiatan observasi terhadap dokumen-dokumen pendukung yang relevan.

Dari hasil wawancara dapat diketahui bahwa Perum Jasa Tirta I Malang sudah menerapkan manajemen risiko TI yang terbukti dengan adanya pengelolaan terhadap risiko yang tertuang kedalam profil risiko, belum adanya unit/bagian khusus yang bertugas mengelola risiko TI, kurangnya staff yang bertugas dalam mengelola teknologi informasi, staff IT mempunyai kewajiban banyak yang dibuktikan dengan mempelajari struktur organisasi beserta tugas yang diberikan, seluruh risiko TI khususnya sistem telemetri sudah diidentifikasi dan dikelola dengan baik kedalam bentuk profil risiko, setiap pelaksanaan proses atau kegiatan mempunyai standar aturan dan pedoman yang tertuang dalam Instruksi Kerja (IK) dengan NO. DOK QI/BIL/01 mengenai pedoman keamanan informasi dan NO. DOK QI/BIL/02 membahas tentang pengelolaan sistem telemetri termasuk prosedur kalibrasi. Setiap kegiatan implementasi, pemeliharaan, perbaikan, kontrol, dan lainnya, semua akan didokumentasikan kedalam bentuk laporan yang akan dilaporkan setiap triwulan (3 bulan) kepada pimpinan, dimana pedoman dalam pembuatan laporan tersebut juga tercantum didalam Instruksi Kerja. Perum Jasa Tirta I Malang mempunyai perencanaan dalam pengelolaan teknologi informasu yang tertuang kedalam *Masterplan* perusahaan. Dari hasil wawancara, Perum jasa Tirta I Malang menyatakan bahwa manajemen risiko TI merupakan bagian penting yang harus diterapkan dan dikembangkan terus menerus.

Semua pertanyaan yang diajukan pada saat wawancara merupakan kebutuhan mendapatkan informasi yang relevan dengan penelitian. Begitu juga dengan dokumen pendukung yang dipelajari pada saat observasi.

## 5. PEMBAHASAN

### *5.1* Analisis *Capability Level* dan *Gap*

Berdasarkan data kuesioner yang telah divalidasi dengan data hasil wawancara dan observasi terhadap bukti pendukung. Dihasilkan nilai *capability level* untuk domain proses EDM03 dan APO12 di Perum Jasa Tirta I Malang berada pada level 2 (*Managed Process*).

**Tabel 2.** Hasil Analisis *Capability Level* dan *Gap*

| Nama Proses | Level Saat Ini | Level Target | *Gap* |
|---|---|---|---|
| EDM03 (*Risk Optimisation*) | 2 | 3 | 1 |
| APO12 (*Managed Process*) | 2 | 3 | 1 |

Dan target pencapaian yang ditetapkan perusahaan untuk domain proses EDM03 dan APO12 adalah naik 1 tingkat dari pencapaian saat ini, yaitu berada pada level 3 (*Established Process*). Sehingga dapat disimpulkan dari hasil pencapaian saat ini dan target pencapaian *capability level* yang telah ditentukan, didapatkan jarak atau gap sebesar 1 level/tingkat.

### 5.2 *Risk Assessment*

Pada tahapan *Risk Assessment* ini terdapat proses yang harus dijalani, yang meliputi:

1. Analisis Risiko (*Risk Analysis*)

*Risk Analysis* bertujuan untuk menentukan seberapa sering (*probability*) suatu risiko dapat terjadi dan seberapa besar dampak (*impact*) yang dihasilkan oleh risiko tersebut yang harus ditanggung oleh perusahaan. *Risk Analysis* diawali dengan melakukan identifikasi risiko, menentukan parameter *probability* dan *impact*, menentukan parameter *rating* risiko, dan yang terakhir adalah melakukan penilaian risiko terhadap *inherent risk* dan *residual risk*.

Adapun pengelompokan risiko berdasarkan aset dapat dilihat dalam tabel 3 berikut ini.

**Tabel 3.** Rekapitulasi Berdasarkan Aset

| No | Kategori Aset | Jumlah *Risk Issue* | Persentase |
|---|---|---|---|
| 1 | Aplikasi | 1 | 3.85 % |
| 2 | Fasilitas | 1 | 3.85 % |
| 3 | Infrastruktur TI | 4 | 15.38 % |
| 4 | Informasi / Data | 7 | 26.92 % |
| 5 | Proses | 10 | 38.46 % |
| 6 | SDM | 3 | 11.54 % |
| | Total | 23 | 100 % |

Dari tebel tersebut diketahui bahwa kategori aset dengan *risk issue* terbanyak adalah kategori proses yang mempunyai persentase sebesar 38.46% dengan jumlah 10 *risk issue*.

Sedangkan untuk pengelompokan risiko berdasarkan skenario risiko dapat dilihat pada tabel 4 berikut ini.

**Tabel 4.** Rekapitulasi Berdasarkan Skenario Risiko

| No | Skenario Risiko | Jumlah *Risk Issue* |
|---|---|---|
| 1 | *Logical Trespassing* | 1 |
| 2 | *Data(base) Integrity* | 2 |
| 3 | *Utilities Performance* | 1 |
| 4 | *Logical Attacks* | 1 |
| 5 | *Malware* | 1 |
| 6 | *System Capacity* | 1 |
| 7 | *Infrastructure (Hardware)* | 3 |
| 8 | *IT Expertise and Skills* | 1 |
| 9 | *New Technology* | 1 |
| 10 | *IT Staff* | 2 |
| 11 | *State of Infrastructure Technology* | 1 |
| 12 | *Project Delivery* | 8 |
| 13 | *Regulatory Compliance* | 2 |
| 14 | *Acts of Nature* | 1 |
| | **Total** | 26 |

Dari tebel tersebut diketahui bahwa skenario risiko dengan *risk issue* terbanyak adalah *project delivery* dengan jumlah 8.

Dari hasil rekapitulasi risiko berdasarkan aset dan skenario risiko serta mempertimbangkan parameter *probability* dan *impact* yang telah dibuat, maka dapat diketahui kategori risiko dasar (*Inherent Risk*). *Inherent Risk* merupakan risiko yang dinilai tanpa memasukkan unsur pengendalian yang telah diterapkan. Adapun rekapitulasi hasil penilaian risiko terhadap *Inherent Risk* yang disusun berdasarkan aset dapat dilihat pada tabel 5 berikut ini.

**Tabel 5.** Penilaian *Inherent Risk* Berdasarkan Aset

| No | Kategori Aset | Nilai Risiko Dasar | | | | |
|---|---|---|---|---|---|---|
| | | Rendah | Rendah Menengah | Menengah | Menengah Tinggi | Tinggi |
| 1 | Aplikasi | 0 | 0 | 0 | 1 | 0 |
| 2 | Fasilitas | 0 | 0 | 1 | 0 | 0 |
| 3 | Infrastruktur TI | 0 | 0 | 4 | 0 | 0 |
| 4 | Informasi / Data | 0 | 0 | 6 | 1 | 0 |
| 5 | Proses | 0 | 0 | 9 | 0 | 1 |
| 6 | SDM | 0 | 0 | 0 | 0 | 3 |
| | Total | 0 | 1 | 20 | 2 | 4 |

Sedangkan untuk penilaian residual merupakan risiko yang dinilai dengan memasukkan unsur pengendalian yang telah diterapkan oleh Perum Jasa Tirta I Malang. Adapun rekapitulasi hasil penilaian risiko terhadap *Inherent Risk* yang disusun berdasarkan aset dapat dilihat pada Tabel 5 berikut ini. Adapun rekapitulasi hasil penilaian risiko terhadap *Residual Risk* yang disusun berdasarkan aset di Perum Jasa Tirta I Malang dapat dilihat pada tabel 6 berikut ini.

**Tabel 6.** Penilaian *Residual Risk* Berdasarkan Aset

| No | Kategori Aset | Nilai Risiko Akhir | | | | |
|---|---|---|---|---|---|---|
| | | Rendah | Rendah Menengah | Menengah | Menengah Tinggi | Tinggi |
| 1 | Aplikasi | 0 | 1 | 0 | 0 | 0 |
| 2 | Fasilitas | 1 | 0 | 0 | 0 | 0 |
| 3 | Infrastruktur TI | 4 | 0 | 0 | 0 | 0 |
| 4 | Informasi / Data | 7 | 0 | 0 | 0 | 0 |
| 5 | Proses | 9 | 0 | 0 | 1 | 0 |
| 6 | SDM | 0 | 0 | 1 | 0 | 2 |
| | Total | 21 | 1 | 1 | 1 | 2 |

2. Evaluasi Risiko (*Risk Evaluation*)

*Risk evaluation* bertujuan untuk mengevaluasi apakah risiko – risiko tersebut dapat ditoleransi atau tidak oleh perusahaan. *Risk evaluation* dilakukan dengan menggambarkan hubungan antara *probability* (kecenderungan) dan *impact* (dampak) kedalam sebuah matriks yang disebut *Risk Map*. Dari *Risk Map* tersebut dapat diketahui risiko mana saja yang membutuhkan tindakan dan penanganan untuk menanggulanginya.

**Tabel 7.** *Risk Map*

| Impact | | | | | | | |
|---|---|---|---|---|---|---|---|
| Sangat Besar (5) | 0 | 0 | 0 | 0 | 0 | 0 | |
| Besar (4) | 2 | 0 | 0 | 0 | 1 | 1 | |
| Sedang (3) | 0 | 0 | 0 | 0 | 0 | 0 | |
| Kecil (2) | 23 | 21 | 1 | 0 | 0 | 1 | |
| Sangat Kecil (1) | 1 | 0 | 0 | 1 | 0 | 0 | |
| Total | 26 | 21 | 1 | 1 | 1 | 2 | |
| | Total | Sangat Jarang (1) | Jarang (2) | Kadang-kadang (3) | Sering (4) | Sangat Sering (5) | |
| | | Probability | | | | | |

## 5.3 Strategi dan Langkah Mitigasi

Langkah mitigasi dapat dirancang dengan melakukan pemetaan skenario risiko IT ke dalam kerangka kerja COBIT untuk mendapatkan risiko – risiko yang relevan. Skenario risiko TI yang dipetakan terdiri dari 1 *Risk Issue* yang termasuk dalam *New Technology*, 2 *Risk Issue* yang termasuk dalam *IT Staff*, 1 *Risk Issue* yang termasuk dalam *System Capacity* dan 1 *Risk Issue* yang termasuk dalam *IT Expertise and Skills.* Adapun langkah strategi mitigasi yang disarankan kepada Perum Jasa Tirta I Malang dalam menyikapi beberapa *Risk Issue* dapat dilihat pada tabel langkah mitigasi berikut ini.

**Tabel 8.** Langkah Mitigasi *New Technology*

| Skenario Risiko | Langkah Mitigasi |
|---|---|
| 1. *New Technology*<br><br>Deskripsi Risiko:<br>- Pengembangan Sistem Telemetri | - Membentuk *team* IT yang secara khusus bertanggung jawab dalam mengambangkan Sistem Telemetri.<br>- Menyediakan *staff* yang cukup pada Team IT.<br>- Terdapat pembagian tugas dan target spesifik dalam pengembangan Sistem Telemetri yang tertuang dalam *Masterplan* perusahaan.<br>- Melakukan analisis *effectiveness-cost* dan *cost-benefit analysis*, dengan melakukan identifikasi investasi jangka panjang, menghitung nilai prioritas setiap investasi dan menentukan rangking prioritas investasi pengembangan sistem. Apakah |

| | |
|---|---|
| | dikembangkan sendiri atau bekerja sama dengan pihak ketiga, dengan mempertimbangkan aspek jumlah staff yang dimiliki oleh Perum Jasa Tirta I Malang. Yang disertai kebijakan atau aturan baku yang jelas mengenai keputusan yang telah diambil. |

**Tabel 9.** Langkah Mitigasi IT *Expertise and Skills*

| Skenario Risiko | Langkah Mitigasi |
|---|---|
| 2. *IT Expertise and Skills*<br><br>Deskripsi Risiko:<br>- Pendidikan Staff | - Memberikan training dan pelatihan kepada seluruh *staff* IT mengenai teknologi informasi yang digunakan.<br>- Menyempurnakan pola rekruitmen dan pelatihan SDM.<br>- Memeriksa latar belakang calon staff TI, termasuk batas minimal pendidikan dan keterampilan.<br>- Memberikan penugasan terhadap *staff* berdasarkan beban kerja dan kompetensi, agar *staff* dapat bekerja dengan disiplin dan penuh dengan tanggung jawab.<br>- Melakukan monitoring dan evaluasi kerja terhadap seluruh *staff*. Agar tingkat kemampuan staff dapat terpantau dengan baik sesuai dengan kebutuhan perusahaan. |

**Tabel 10.** Langkah Mitigasi IT *Staff*

| Skenario Risiko | Langkah Mitigasi |
|---|---|
| 3. *IT staff*<br><br>Deskripsi Risiko:<br>- Kurangnya *staff* yang bertugas dalam mengelola IT beserta manajemen risiko<br>- Pembagian tugas yang menumpuk | - Membentuk *team* IT yang secara khusus bertanggung jawab dalam mengelola IT perusahaan. Termasuk dalam mengelola manajemen risiko.<br>- Menambah jumlah *staff* pada bagian pengelolaan IT. Agar tidak terjadi penumpukan tugas dan tugas selesai sesuai target.<br>- Melakukan monitoring dan evaluasi kerja terhadap seluruh *staff*<br>- *Staff* diberi tugas sesuai dengan beban kerja dan kompetensi, agar *staff* dapat bekerja dengan disiplin dan penuh dengan tanggung jawab.<br>- Melakukan analisis *effectiveness-cost* dan *cost-benefit analysis*, dengan melakukan identifikasi investasi jangka panjang tentang rekrutmen staff (mandiri atau kerjasama), menghitung nilai prioritas setiap investasi dan menentukan rangking prioritas investasi. |

**Tabel 11.** Langkah Mitigasi *System Capacity*

| Skenario Risiko | Langkah Mitigasi |
|---|---|
| 4. *System Capacity*<br><br>Deskripsi Risiko:<br>- Beban penyimpanan server tinggi | - Membentuk *team* IT yang secara khusus bertanggung jawab dalam mengelola server perusahaan.<br>- Membuat aturan atau kebijakan tentang *capacity planning*, monitoring dan evaluasi untuk seluruh sistem informasi yang akan diimplementasikan.<br>- Membuat pemisahan server setiap sistem yang digunakan, agar ketika *load* data berjalan dengan cepat.<br>- Mengembangkan Sistem Telemetri, agar seluruh data yang terekam oleh IPCamera tidak langsung disimpan. Melaikan hanya pada kondisi tertentu saja, agar mengurangi beban kerja server.<br>- Meningkatkan jumlah server. |

## 5.4 Rekomendasi

Rekomendasi dibuat mengacu kepada hasil anailisis *capability level* guna mengetahui pencapaian menjalankan proses saat ini dan analisis *gap* guna mengetahui target yang ditentukan oleh perusahaan dan nilai kesenjangan yang terjadi. Rekomendasi dibuat dengan tujuan dapat meminimalisir *gap* antara pencapaian saat ini dan target yang telah ditentukan, maupun untuk mencapai target yang telah ditentukan oleh Perum Jasa Tirta I Malang dalam melakukan perbaikan manajemen risiko teknologi informasi. Berikut adalah rekomendasi berdasarkan domain proses EDM03 dan APO12:

1. Perum Jasa Tirta I Malang disarankan untuk membentuk unit atau team khusus yang

mempunyai tanggung jawab dalam melakukan pembahasan dan pengelolaan terkait penerapan manajemen risiko Teknologi Informasi didalam perusahaan.
2. Menerbitkan dokumen kontrol berupa *check list* pada saat implementasi penerapan manajemen risiko.
3. Membuat dokumen kontrol performa *staff*, yang terdiri dari hasil kinerja dari penerapan manajemen risiko.
4. Memperkuat kegiatan monitoring penerapan manajemen risiko teknologi informasi untuk bahan evaluasi, agar penerapan manajemen risiko dapat terus diperbaharui dari kekurangan yang belum teridentifikasi.
5. Menerbitkan dokumen tertulis yang berisikan tentang risk assessment yang dikelola perusahaan sampai dengan langkah mitigasi risiko beserta risk respond terhadap semua risiko TI.
6. Menerbitkan suatu kebijakan dalam melakukan pengukuran terhadap pengelolaan standart proses.
7. Meningkatkan perumusan proses standart yang akan diterapkan, mendefinisikan detail tanggung jawab dan otoritas pelaksanaan aktivitas.
8. Melakukan pengukuran terhadap sejauh mana proses standar dikelola untuk mendukung pengerjaan dari proses yang telah didefinisikan.
9. Melakukan analisis *Cost Benefit* untuk melakukan peramalan frekuensi besarnya kerugian yang harus tanggung maupun keuntungan yang akan diperoleh perusahaan ketika penanganan terhadap setiap skenario risiko teknologi informasi dilakukan.
10. Membuat program-program khusus yang berisi kegiatan pemantauan, review, pengendalian dan pengelolaan terhadap penerapan manajemen risiko teknologi informasi.
11. Mengumpulkan data-data relevan yang dapat dijadikan sumber untuk memastikan kecocokan dan keefektifan proses sebagai bahan evaluasi untuk perbaikan terus-menerus dari proses.
12. Perum Jasa Tirta I Malang harus memastikan kebijakan tentang manjemen risiko yang berkaitan dengan teknologi informasi juga harus terintegrasi atau selaras dengan manajemen risiko secara keseluruhan perusahaan.

## 6. KESIMPULAN

Berdasarkan hasil pembahasan terkait manajemen risiko Teknologi Informasi (TI) yang telah diterapkan oleh Perum Jasa Tirta I Malang, maka dapat diperoleh kesimpulan penelitian sebagai berikut:

1. Proses evaluasi terhadap penerapan manajemen risiko Teknologi Informasi (TI) pada Perum Jasa Tirta I Malang menggunakan kerangka kerja COBIT 5 khususnya domain proses EDM03 *(Ensure Risk Optimation)* dan APO12 *(Manage Risk)* menghasilkan beberapa hal berikut ini:
   a. Kemampuan Perum Jasa Tirta I Malang dalam menjalankan proses *Ensure Risk* Optimation (EDM03) dan *Managed Risk* (APO12) sama-sama berada pada level 2 yaitu *Managed Process* yang berarti aktivitas yang berkaitan dengan perencanaan, pemantauan (monitoring) dan penyesuaian pada proses *Ensure Risk Optimation* dan *Managed Risk* telah dikelola dengan baik oleh Perum Jasa Tirta I Malang serta hasil kerjanya telah ditetapkan, dipantau dan dikelola dengan tepat.
   b. Besarnya *gap* yang terbentuk antara nilai *capability level* yang telah saat ini dengan nilai *capability level* yang ingin dicapai untuk domain proses EDM03 dan APO12 masing-masing adalah sebesar 1.
   c. Ditemukannya 26 *risk issue* yang terbagi dalam 6 kategori aset dan 14 skenario risiko. Dan juga ditemukan bahwa terdapat 4 skenario risiko yang tidak sesuai dengan *risk appetite* perusahaan.
2. Hasil rekomendasi dan langkah mitigasi yang diberikan untuk bahan pertimbangan rencana perbaikan manajemen risiko Teknologi Informasi (TI) di Perum Jasa Tirta I Malang adalah sebagai berikut:
   a. Terdapat 12 rekomendasi yang telah dibuat, supaya dapat meminimalisir kesenjangan (*gap*) dan nilai *capability level* pada domain proses EDM03 dan APO12 dapat naik satu tingkat ke level 3.
   b. Dari 4 skenario risiko yang terdiri dari 5 *risk issue* yang tidak sesuai dengan *risk appetite* perusahaan, maka

dibuatlah langkah mitigasi terhadap skenario risiko *New Technology*, IT *Expertise and Skills*, IT *Staff*, dan *System Capacity*. Langkah mitigasi dirancang untuk mengatasi kelemahan dan permasalahan Perum Jasa Tirta I Malang dalam melakukan pengembangan Sistem Telemetri saat ini, untuk menutupi kekurangan dari segi pendidikan yang dimiliki sebagian *staff* Perum Jasa Tirta I Malang, untuk mengatasi masalah terkait kurangnya *staff* yang bertugas dalam mengelolaa teknologi informasi beserta manajemen risiko TI dan permasalahan tentang pembagian tugas yang menumpuk untuk staff TI, serta untuk mengatasi dan mengurangi dampak risiko yang diakibatkan oleh beban penyimpanan yang tinggi.

## DAFTAR PUSTAKA


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

Dyahaloka, Astri., 2016. *Evaluasi Manajemen Resiko E-Procurement Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Pertamina (Persero))*. Malang : Universitas Brawijaya.

Hayaty, M., Rosidi, A., and Arief, M.R., 2013. *Risk Assessment Dan Business Impact Analysis Sebagai Dasar Penyusunan Disaster Recovery Plan (Studi Kasus Di Stmik Amikom Yogyakarta)*. *SEMNASTEKNOMEDIA ONLINE*, 1(1), pp.23-1.

Husein, G.M. and Imbar, R.V., 2015. *Analisis Manajemen Risiko Teknologi Informasi Penerapan Pada Document Management System di PT. JABAR TELEMATIKA (JATEL)*. *Jurnal Teknik Informatika dan Sistem Informasi*, *1*(2). Tersedia di: <http:// http://jutisi.maranatha.edu/index.php/jutisi> [Diakses 6 Oktober 2016].

ISACA., 2012. *COBIT 5 : A Bussiness Framework for the Governance and Management of Enterprise IT*. Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : Enabling Process.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : The Risk IT Practitioner Guide.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : For Risk.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : Self-Assessment Guide.* Rolling Meadows : ISACA.

Islamiah, Mega Putri., 2014. *Tata Kelola Teknologi Informasi (IT Governance) Menggunakan Framework Cobit 5: Studi Kasus Dewan Kehormatan Penyelenggara Pemilu* (*DKPP*). Jakarta : Universitas Islam Negeri Syarif Hidayatullah. Tersedia di : <http://repository.uinjkt.ac.id> [Diakses 11 November 2016].

ITGI., 2003. *Broad Briefing on IT Governance 2nd Edition*. Rolling Meadows : IT Governance Institute.

JASA TIRTA I, 2014. *Pedoman Tata kelola Perusahaan (Code Of Corporate Governance) Perum Jasa Tirta I Malang*. Malang : Perum Jasa Tirta I Malang.

Keputusan Presiden Republik Indonesia Nomor 2 Tahun 2014 Tentang Penambahan Wilayah Kerja Perusahaan Umum (PERUM) Jasa Tirta I Di Wilayah Sungai Toba Asahan, Wilayah Sungai Serayu, Bogowonto, Dan Wilayah Sungai Jratunseluna. Jakarta : Presiden Republik Indonesia.

Kusumaningrum, Vika P., 2016. *Evaluasi Teknologi Informasi Menggunakan Framework COBIT 5 Pada Domain DSS (Delivery Service and Support) (Studi Kasus : PT. PLN (Persero) Rayon Ngawi).* Malang : Universitas Brawijaya.

Masyhuri, Imam., and Febriliyan, Samopa., 2013. *Pengembangan Manajemen Risiko Teknologi Informasi Pada Sistem Penerimaan Peserta Didik Baru (PPDB Online) KEMENDIKBUD Menggunakan Framework NIST SP800-30. Prosiding Seminar Nasional Manajemen Teknologi XVIII MMT-ITS.*

Perarturan Pemerintah Republik Indonesia Nomor 46 Tahun 2010 Tentang Perusahaan Umum (PERUM) Jasa Tirta I. Jakarta : Presiden Republik Indonesia.

Permenkominfo. 2007. *Panduan Umum Tata Kelola Teknologi Informasi Dan Komunikasi Nasional Versi 1*. Jakarta : Menteri Komunikasi Dan Informatika.

Perum Jasa Tirta I., 2017. *Profil Perum Jasa Tirta I.* [online] Tersedia di : <http://jasatirta1.co.id/id_ID/profil/> [Diakses 11 November 2016].

Pratama, Enda E., and Suhardi., 2013. *Analisis Nilai & Manajemen Risiko Teknologi Informasi (Studi Kasus PT. Bank Tabungan Negara. Tbk).* Bandung : Institute Teknologi Bandung. Tersedia di : <http://www.academia.edu/> [Diakses 6 Oktober 2016].

Samaptoaji, Sigit, 2014. *Evaluasi Pengelolaan Risiko Teknologi Informasi (TI) pada Instansi Pemerintah : Studi Kasus Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementrian Dalam Negeri*. Jakarta : Universitas Indonesia.

Setiawan, Alexander, 2009. *Evaluasi Penerapan Teknologi Informasi Di Perguruan Tinggi Swasta Yogyakarta Dengan Menggunakan Model Cobit Framework. Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*. Vol. 1. No. 1. Tersedia di: <http:// www.jurnal.uii.ac.id/index.php> [Diakses 11 November 2016].

Suwarno, Fajrin Rizkia P., 2014. *Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Pada Proses Manage Relationship (APO08) (Studi Kasus : PT. OTO Multiartha).* Jakarta : Universitas Islam Negeri Syarif Hidayatullah.

Symantec., 2007. *IT Risk Management Report*. Vol. 1

Teruri, Shabrina., 2016. *Evaluasi Manajemen Resiko Migrasi Sistem MES Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Krakatau Steel (Persero)Tbk).* Malang : Universitas Brawijaya.

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

**Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer** e-ISSN: 2548-964X
Vol. 2, No. 1, Januari 2018, hlm. 91-100 http://j-ptiik.ub.ac.id

# Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Petrokimia Gresik)

**Nurfitri Zukhrufatul Firdaus[1], Suprapto[2]**

Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Brawijaya
Email: [1]fitri.firdaus0@gmail.com, [2]spttif@ub.ac.id

**Abstrak**

SAP (*System Application and Product in Data Processing*) merupakan jenis software ERP yang digunakan oleh PT. Petrokimia Gresik untuk menunjang otomatisasi proses bisnis perusahaan dan mendukung proses pengambilan keputusan agar lebih efektif dan efisien. Untuk mengantisipasi timbulnya risiko yang dapat mengganggu jalannya proses bisnis perusahaan, PT. Petrokimia Gresik menerapkan manajemen risiko berdasarkan standart ISO 31000:2009. Dalam hal ini perlu dilakukan evaluasi untuk mnegetahui pencapaian penerapan manajemen risiko teknologi informasi pada PT. Petrokimia Gresik dengan menggunakan kerangka kerja COBIT 5 khususnya pada domain proses APO12 (Risk Management) dan EDM03 (Ensure Risk Optimation). Untuk memperoleh data yang akurat, maka teknik pengumpulan data yang digunakan adalah dengan melakukan pengisian lembar kerja evaluasi, obeservasi langsung dan wawancara dengan pihak yang berwenang. Proses evaluasi tersebut terdiri dari beberapa tahapan, antara lain melakukan analisis *capability level*, analisis *gap* dan analisis *risk assessment* untuk mengidentifikasi risiko – risiko potensial serta menilai sejauh mana dampak yang dapat ditimbulkan. Berdasarkan hasil analisis tersebut, maka didapatkan nilai *capability level* untuk domain proses EDM03 berada pada level 2 dan domain proses APO12 berada pada level 3 serta menghasilkan 16 buah strategi mitigasi dan 9 buah rekomendasi yang dapat digunakan untuk membantu perbaikan penerapan manajemen risiko teknologi informasi di PT. Petrokimia Gresik.

**Kata kunci**: *COBIT 5, capability level, manajemen risiko, analisis gap, risk assessment, mitigasi risiko*

**Abstract**

*SAP (System Application and Product in Data Processing) is a type of ERP Software that used by PT. Petrokimia Gresik to support business process automation and support decision-making process to be more effective and efficient. To anticipate the potential problems that might obstruct business processes at the company, so PT. Petrokimia Gresik managed to use risk management based on the standards of ISO 31000:2009. An evaluation on the implementation of IT risk management was done to measure its capability level accomplishment. COBIT 5 Framework, especially in process domain APO12 (Risk Management) dan EDM03 (Ensure Risk Optimation), was used as the basis of the evaluation. To collect accurate data, the data were obtained by filling evaluation worksheet, conducting a direct observation and an interview to the people in charge. The process of evaluating the implementation of IT risk management consists of several stages, including capability level analysis, gap analysis and risk assessment analysis to identify potential risks and assess the extent of the impacts of each risk. From the evaluation result, it turned out that capability level for process domain EDM03 was on level 2 and on level 3 for process domain APO12 and 16 mitigation strategy and 9 recommendation were made to support the improvement for the implementation of risk management information and technology at PT. Petrokimia Gresik.*

**Keywords**: *COBIT 5, capability level, risk management, gap analysis, risk assessment, risk mitigation*

## 1. PENDAHULUAN

Salah satu perusahaan yang telah memanfaatkan teknologi informasi dan menerapkan manajemen risiko teknologi informasi sebagai sarana pendukung untuk mencapai tujuan perusahaan adalah PT. Petrokimia Gresik. Untuk meningkatkan kualitas perusahaan dibidang teknologi informasi, PT. Petrokimia Gresik menerapkan sistem ERP – SAP yang terdiri dari sepuluh

modul. Disamping itu PT. Petrokimia Gresik juga menerapkan beberapa aplikasi Non ERP untuk menunjang jalannya Sistem ERP-SAP. Dengan diterapkannya Sistem tersebut diharapkan mampu menunjang otomatisasi proses bisnis perusahaan dan mendukung proses pengambilan keputusan secara efektif dan efisien. Namun pada kenyatannya, penerapan Teknologi Informasi (TI) pada perusahaan tidak selalu berjalan sesuai dengan yang diharapkan, sehingga menimbulkan risiko – risiko yang dapat merugikan perusahaan. Oleh karena itu untuk mengelola segala macam risiko yang dapat mengganggu jalannya proses bisnis dan menimbulkan kerugian, maka PT. Petrokimia Gresik telah menerapkan manajemen risiko berdasarkan pada Standart ISO 31000 : 2009 sejak tahun 2003.

Padatnya proses bisnis yang berjalan di PT. Petrokimia Gresik, mengakibatkan aktivitas pengelolaan risiko menjadi kurang optimal, sehingga masih ditemukan risiko yang dapat menghambat jalannya proses bisnis perusahaan. Risiko – risiko tersebut diantaranya berupa gangguan jaringan internet, gangguan arus listrik, kurang optimalnya dukungan teknis operasional ERP, gangguan komunikasi data antara user dengan server ERP dan lain sebagainya. Oleh karena itu perlu adanya evaluasi manajemen risiko Teknologi Informasi (TI) untuk mengetahui tingkat kapabilitas pengelolaan risiko yang telah dicapai, sehingga dapat meningkatkan kemampuan perusahaan dalam mengelola setiap risiko terkait penerapan sistem ERP-SAP pada PT. Petrokimia Gresik. Dari evaluasi tersebut menghasilkan rekomendasi berupa saran maupun usulan yang dapat digunakan oleh perusahaan untuk meminimalisir terjadinya risiko – risiko yang tidak diinginkan. Salah satu *framework* yang dapat digunakan untuk mengevaluasi manajemen risiko Teknologi Informasi (TI) pada PT. Petrokimia Gresik adalah COBIT 5 khususnya pada domain proses APO12 (*Manage Risk*) dan EDM03 (*Ensure Risk Optimisatin*). Digunakannya domain tersebut karena dalam COBIT 5, hanya ada dua domain yang membahas secara terperinci mengenai manajemen risiko Teknologi Informasi (TI).

## 2. LANDASAN KEPUSTAKAAN

### 2.1. Kajian Pustaka

Adapun penelitian – penelitian terdahulu yang relevan dengan penelitian ini adalah sebagai berikut:

1. Penelitian yang dilakukan oleh Astri Dyahaloka yang berjudul "Evaluasi Manajemen Risikio *E-Procurement* Menggunakan COBIT 5 *IT Risk* (Studi Kasus : PT. Pertamina (Persero))". Penelitian tersebut menggunakan kerangka kerja COBIT 5 dengan domain EDM03 dan APO12. Dalam melakukan evaluasi, penelitian tersebut menggunakan analisis *capability level*, analisis *gap* dan analisis SWOT, sehingga menghasilkan nilai *capability level* yang telah dicapai dan rekomendasi untuk perbaikan penerapan manajemen risiko.
2. Penelitian yang dilakukan oleh Sigit Samaptoaji yang berjudul "Evaluasi Pengelolaan Risiko Teknologi Informasi (TI) pada Instansi Pemerintah : Studi Kasus Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementerian Dalam Negeri". Dalam melakukan evaluasi, penelitian tersebut menggunakan analisis *risk assessment* dan penentuan strategi atau langkah mitigasi, sehingga menghasilkan dokumen profil risiko teknologi informasi yang dapat dijadikan sebagai masukan atau pertimbangan dalam proses pengambilan keputusan.

### 2.2 Manajemen Risiko

Djojosoedarso (2003) menjelaskan bahwa manajemen risiko merupakan proses menjalankan aktivitas manajemen untuk menanggulangi munculnya risiko, baik yang dihadapi perusahaan maupun yang dihadapi oleh masyarakat. Sehingga dapat disimpulkan bahwa fungsi – fungsi manajemen yang dijalankan untuk menanggulangi risiko mencakup proses pengelolaan, pengukuran dan penilaian risiko. Dalam hal ini manajemen risiko dimaksudkan untuk mengurangi dampak negatif dari suatu risiko, menghindari terjadinya risiko, menampung sebagian atau keseluruhan dari konsekuensi risiko atau mengalihkan risiko kepada pihak lain.

### 2.3. COBIT 5

*Control Objective for Information and Related Technology* (COBIT) merupakan seperangkat pedoman dan hasil dokumentasi yang berfungsi untuk membantu auditor, pemangku kepentingan atau pengguna (*user*) dalam menghubungkan antara model kendali bisnis dan model kendali TI. COBIT

dikembangkan untuk menerapkan *Governance of Enterprise IT*. Versi terbaru yang dikeluarkan oleh *IT Governance Institute* dikenal sebagai COBIT 5. COBIT 5 terbentuk dengan mengintegrasikan Risk IT *framework*, VAL IT 2.0 dan COBIT 4.1. Selain itu COBIT 5 juga menyesuaikan antara *best practices* yang ada seperti ITIL V3, TOGAF dan standart relevan dari ISO.

Dalam melakukan evaluasi, ISACA (2012) menjelaskan bahwa terdapat tujuh buah tahapan yang harus diterapkan menurut siklus implementasi COBIT 5, antara lain:

1. *Initiate Programme*, yaitu proses identifikasi pemicu perubahan seperti kondisi trend, kinerja, implementasi perangkat lunak, isu penting dan tujuan organisasi yang mampu memberikan dorongan untuk berubah.
2. *Define Problems and Opportunities*, yaitu proses penyelarasan antara tujuan penerapan TI dengan risiko maupun strategi organisasi, serta mengutamakan tujuan penerapan TI, tujuan organisasi dan proses penerapan TI yang paling utama.
3. *Define Road Map*, yaitu proses penetapan target untuk meningkatkan upaya perbaikan dan diikuti dengan analisis *gap* untuk menentukan beberapa solusi potensial.
4. *Plan Programme*, yaitu proses perencanaan solusi yang dianggap layak untuk dijalankan.
5. *Execute Plan*, yaitu proses penerapan solusi yang telah disarankan ke dalam aktivitas keseharian serta melakukan pemantauan untuk memastikan bahwa keselarasan bisnis dapat dicapai dan kinerja dapat diukur.
6. *Realise Benefits*, yaitu proses transisi secara berkelanjutan dengan menerapkan praktik tata kelola atau manajemen yang telah ditingkatkan ke dalam proses bisnis dan memantau perkembangannya dengan memetakannya pada matriks berdasarkan kinerja dan manfaat yang ingin diperoleh.
7. *Review Effectiveness*, yaitu proses evaluasi keberhasilan yang telah dicapai secara umum, kemudian melakukan identifikasi segala kebutuhan perbaikan secara berkala untuk lebih meningkatkan praktik tata kelola atau manajemen.

Menurut ISACA (2012), COBIT 5 telah menyediakan dua proses yang berkaitan dengan penerapan manajemen risiko, antara lain:

1. EDM03 : *Ensure Risk Optimisation*
   Proses EDM03 bertujuan untuk memastikan apakah tingkat risiko dan besarnya toleransi yang dapat diterima oleh perusahaan telah dimengerti, diartikulasikan dan dikomunikasikan dengan baik, serta memastikan apakah risiko – risiko yang terkait dengan Teknologi Informasi (TI) telah diidentifikasi dan dikelola dengan baik. Proses EDM03 terbagi menjadi 3 atribut, yaitu *Evaluate Risk Management*, *Direct Risk Management* dan *Monitor Risk Management.*
2. APO12 : *Manage Risk*
   Proses APO12 bertujuan untuk mengidentifikasi, menilai dan mengurangi risiko terkait dengan teknologi Informasi (TI) agar tidak melebihi batas toleransi yang telah ditentukan oleh manajemen eksekutif organisasi. Selain itu proses APO12 juga bertujuan untuk mengintegrasikan manajamen risiko Teknologi Informasi (TI) dengan manajemen risiko perusahaan (ERM). Proses APO12 terbagi menjadi enam subdomain, yaitu *Collect Data*, *Analyse Risk*, *Maintain A Risk Profile*, *Articulate Risk*, *Define a Risk Management Action Portofolio* dan *Respond to Risk*

Penilaian *Capability Level* untuk setiap proses tersebut digolongkan menjadi enam tingkatan, yaitu Level 0 (*Incomplete Process*), Level 1 (*Performed Process*), Level 2 (*Managed process*), Level 3 (*Established Process*), Level 4 (*Predictable process*) dan Level 5 (*Optimized process*).

### 2.4. *Risk Assessment*

ISACA (2012) menjelaskan bahwa Secara umum *Risk Assessment* berfungsi untuk mengidentifikasi risiko potensial baik yang berasal dari *internal* maupun *eksternal* organisasi, selain itu juga menilai sejauh mana dampak yang ditimbulkan oleh risiko tersebut dapat mengganggu jalannya proses bisnis dan tujuan organisasi. Besarnya dampak dapat diukur melalui penilaian *Inherent Risk* dan *Residual Risk*, serta dianalisis melalui dua perspektif antara lain *Probability/Likelihood* dan *Impact/Consequence*.

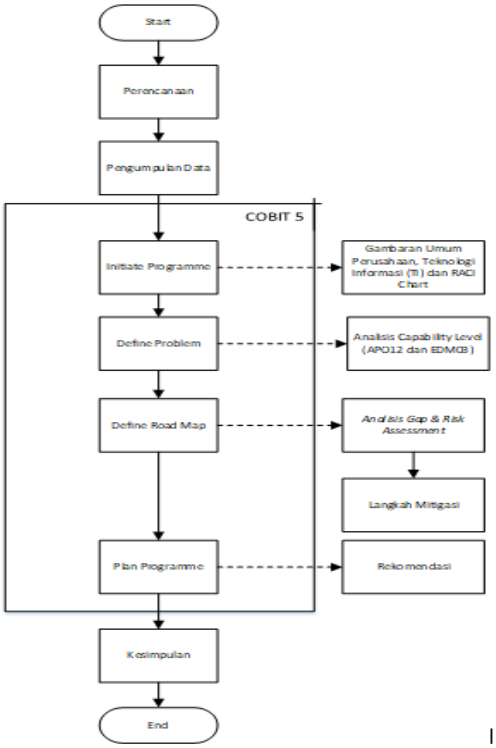
Untuk menyelaraskan antara risiko - risiko yang ditemukan dengan batas toleransi risiko yang telah ditentukan oleh organisasi, maka diperlukan adanya *Risk Response* atau Respon Risiko. Dalam penelitian ini, langkah yang diambil untuk merespon risiko adalah dengan melakukan *Risk Reduction* atau *Mitigation*, yaitu salah satu metode yang dilakukan dengan cara mengurangi besarnya *Probability* atau

*Likelihood* (Peluang atau kecenderungan) dan *Impact* atau *Consequence* (Dampak) yang ditimbulkan dari risiko tersebut.

### 2.5. Sistem ERP – SAP

*System Application and Product in Data Processing* (SAP) merupakan *software* jenis *Enterprise Resources Planning* (ERP) yang dikembangkan untuk menunjang jalannya kegiatan operasional suatu organisasi agar lebih efektif dan efisien. Adapun modul – modul SAP yang diimplementasikan di PT. Petrokimia Gresik antara lain *Material Management, Production Planning, Plant Maintenance, Sales Distribution, Financial Accounting Controlling, Human Capital Management, Quality Management, Fund Management, Business Planning and Consolidation* dan *Dashboard*.

## 3. METODOLOGI




Gambar 1. Diagram Alur Penelitian

1. Menentukan objek penelitian dan kerangka kerja yang tepat serta menggali informasi yang terkait**.**
2. Melakukan pengumpulan data, baik data primer maupun data sekunder dengan cara melakukan pengisian lembar kerja evaluasi, melakukan observasi langsung, melakukan wawancara dengan pihak – pihak yang berwenang dan studi kepustakaan.
3. Mendeskripsikan gambaran umum mengenai kondisi umum organisasi, visi dan misi sebagai tujuan organisasi, gambaran umum sistem informasi atau teknologi informasi yang diterapkan dan pihak – pihak yang bertanggung jawab dalam penerapan manajemen risiko berdasarkan RACI *Chart*.
4. Melakukan analisis penilaian *Capability Level* berdasarkan kerangka kerja COBIT 5 khususnya domain proses EDM03 (*Ensure Risk Optimisation*) dan APO12 (*Manage Risk*).
5. Melakukan *Gap Analysis*, *Risk Assessment* dan menentukan langkah mitigasi untuk setiap risiko yang melebihi batas toleransi perusahaan berdasarkan data yang diperoleh dari hasil lembar kerja evaluasi, observasi dan wawancara.
6. Membuat rekomendasi untuk menentukan solusi potensial berdasarkan hasil analisis *Capability Level*, *Gap Analysis* dan *Risk Assessment*.
7. Menyusun kesimpulan yang berisi ringkasan tentang semua langkah - langkah yang telah dilalui dalam melakukan penelitian.

## 4. HASIL

### 4.1. Hasil Lembar Kerja Evaluasi

Berdasarkan hasil pembuatan RACI *Chart*, dapat diketahui bahwa pihak yang berhak menjadi responden untuk mengisi lembar kerja evaluasi adalah sejumlah tiga orang, antara lain Manager Dept. TEKINFO, Kabag. Infrastruktur TEKINFO dan Manager Dept. TKP & MR.

Tabel 1. Rekapitulasi Hasil Lembar Kerja Evaluasi

| *Prosess Assesment Results* | | | | | | | |
|---|---|---|---|---|---|---|---|
| **Nama Proses** | ***Proces Capability Level*** | | | | | | **Total Responden** |
| | **0** | **1** | **2** | **3** | **4** | **5** | |
| *Evaluate, Direct, and Monitoring* | | | | | | | |
| EDM03 | 0 | 0 | 3 | 0 | 0 | 0 | 3 |
| *Align, Plan, and Organise (APO)* | | | | | | | |
| APO12 | 0 | 0 | 0 | 3 | 0 | 0 | 3 |

Dari Tabel 1 diatas, dapat diketahui bahwa hasil pengisian lembar kerja evaluasi yang dilakukan oleh tiga orang responden menunjukkan nilai *Capability Level* terkait proses EDM03 berada pada Level 2 dan nilai *Capability Level* terkait proses APO12 berada pada Level 3.

### 4.2. Hasil Observasi dan Wawancara

Dalam mengelola proses bisnis perusahaan, PT. Petrokimia Gresik telah mendukung penerapan sistem yang bernama ERP-SAP. Sistem tersebut diharapkan mampu

mengintegrasikan seluruh proses bisnis yang ada pada perusahaan dan mensinergiskan proses bisnis dari masing – masing anggota Pupuk Indonesia *Holding Company* (PIHC). Dalam hal ini, pihak yang bertanggung jawab mendukung jalannya Sistem ERP-SAP, mengintegrasikan sistem atau aplikasi yang dibuat sendiri dengan Sistem ERP-SAP, serta meningkatkan kualitas SDM untuk mendukung penerapan Sistem ERP-SAP adalah Departemen TEKINFO.

Dalam penerapan Sistem ERP – SAP tersebut, tidak pernah lepas dari suatu risiko. Oleh karena itu untuk mengelola segala bentuk risiko perusahaan, Departemen TKP & MR telah menerapkan manajemen risiko berdasarkan standart dan kebijakan yang ditetapkan yaitu ISO 31000 : 2009. Standart dan kebijakan tersebut tertuang dalam dokumen Kebijakan Manajemen Risiko, Pedoman Penerapan Manajemen Risiko, Prosedeur Penerapan Manajeen Risiko, Panduan Penilaian Penerapan Manajemen Risiko dan Pedoman Manajemen Risiko PT. Pupuk Indonesia (Persero). Selama ini penerapan manajemen risiko pada PT. Petrokimia Gresik dimulai dengan melakukan identifikasi terhadap semua risiko yang muncul, menganalisis setiap risiko yang telah diidentifikasi, mengevaluasi setiap risiko, melakukan pengendalian dan penanganan risiko serta melakukan monitoring dan review terhadap pengendalian dan penanganan. Selanjutnya hasil dari aktivitas pengelolaan risiko tersebut disusun dalam sebuah dokumen yang bernama Profil Risiko PT. Petrokimia Gresik.

Dalam mengelola setiap risiko perusahaan, Departemen TKP & MR memiliki aplikasi yang bernama SIMAR (Sistem Informasi Manajemen Risiko) dan program kerja yang bernama Klinik Risiko. Dengan adanya aplikasi SIMAR dan program Klinik Risiko tersebut, dapat memudahkan Departemen TKP & MR dalam memantau penerapan manajemen risiko pada setiap unit kerja.

### 4.3. Hasil Temuan

Berdasarkan hasil lembar kerja evaluasi, observasi dan proses wawancara dengan pihak Departemen TKP & MR dan Departemen TEKINFO PT. Petrokimia Gresik, didapatkan beberapa temuan berikut:

1. Adanya layanan Tata Kelola Perusahaan dan Manajemen Risiko pada PT. Petrokimia Gresik, namun belum adanya manajemen atau team yang dibentuk secara khusus untuk mengelola segala macam risiko terkait dengan teknologi informasi.
2. Pengelolaan risiko yang dilakukan oleh Departemen TKP & MR pada PT. Petrokimia Gresik masih secara umum yaitu dilakukan pada seluruh unit kerja perusahaan dan belum berfokus secara spesifik pada penerapan teknologi informasi.
3. Tidak semua risiko teknologi informasi telah didokumentasikan dan dikelola dengan baik.
4. Belum secara penuh memantau kesesuaian seluruh risiko yang dikelola dengan risk appetite.
5. Dalam melakukan analisis risiko tersebut, belum disertai dengan analisis *cost benefit* yaitu perkiraan frekuensi besarnya keuntungan dan kerugian yang berhubungan dengan penanganan setiap skenario risiko.

## 5. PEMBAHASAN

### 5.1. Analisis *Capability Level*

Berdasarkan hasil pengisian lembar kerja evaluasi yang dilakukan oleh 3 responden dari Departemen TKP & MR dan Departemen TEKINFO PT. Petrokimia Gresik dapat diketahui bahwa nilai *capability level* yang telah dicapai subdomain EDM03 berada pada Level 2 dan nilai *capability level* yang telah dicapai subdomain APO12 berada pada Level 3. Hal tersebut dapat dilihat pada Tabel 2 di bawah ini.

Tabel 2. Rekapitulasi Hasil Gap Analysis

| Nama Proses | Level Saat Ini | Level Target | *Gap* |
|---|---|---|---|
| EDM03 | 2 | 3 | 1 |
| APO12 | 3 | 4 | 1 |

### 5.2. Analisis *Gap*

Berdasarkan hasil wawancara, diperoleh informasi bahwa level target yang ingin dicapai oleh Departemen TKP & MR dan Departemen TEKINFO PT. Petrokimia Gresik adalah naik satu level untuk setiap domain prosesnya, yaitu domain proses EDM03 berada pada Level 3 dan domain proses APO12 berada pada Level 4. Sehingga besarnya *gap* yang terbentuk antara level yang terjadi saat ini dan level target yang ingin dicapai pada domain proses EDM03 dan APO12 adalah sebesar 1.

### 5.3. *Risk Assessment*

Proses *Risk Assessment* dilakukan berdasarkan dua tahapan, antara lain:

1. *Risk Analysis*

*Risk Analysis* bertujuan untuk menentukan seberapa sering risiko tersebut dapat terjadi dan seberapa besar dampak yang dihasilkan oleh risiko tersebut. *Risk Analysis* diawali dengan melakukan identifikasi risiko, menentukan parameter *probability*, menentukan parameter *impact*, menentukan parameter *rating* risiko, melakukan penilaian risiko terhadap *inherent risk* dan *residual risk*.

Adapun pengelompokan risiko berdasarkan skenario risiko dapat dilihat dalam Tabel 3 berikut ini.

Tabel 3. Rekapitulasi Berdasarkan Skenario Risiko

| No | Skenario Risiko | Jumlah *Risk Issue* |
|---|---|---|
| 1 | *New Technology* | 1 |
| 2 | *Software Implementation* | 2 |
| 3 | *Destruction of Infrastructure* | 1 |
| 4 | *IT Staff* | 1 |
| 5 | *IT Expertise and Skills* | 2 |
| 6 | *Software Integrity* | 2 |
| 7 | *Infrastructure (Hardware)* | 3 |
| 8 | *System Capacity* | 2 |
| 9 | *Malware* | 1 |
| 10 | *Logical Attacks* | 1 |
| 11 | *Utilities Performance* | 1 |
| 12 | *Data(base) Integrity* | 2 |
| 13 | *Logical Trespassing* | 1 |
| 14 | *Operational IT Errors* | 2 |
| 15 | *Acts of Nature* | 1 |
| | Total | 23 |

Sedangkan untuk pengelompokan risiko berdasarkan aset dapat dilihat dalam Tabel 4 berikut ini.

Tabel 4. Rekapitulasi Berdasarkan Aset

| No | Kategori Aset | Jumlah *Risk Issue* | Persentase |
|---|---|---|---|
| 1 | Aplikasi | 5 | 21,74 % |
| 2 | Fasilitas | 1 | 4,35 % |
| 3 | Infrastruktur TI | 3 | 13,04 % |
| 4 | Informasi / Data | 7 | 30,43 % |
| 5 | Proses | 4 | 17,39 % |
| 6 | SDM | 3 | 13,04 % |
| | Total | 23 | 100 % |

Sebelum melakukan penilaian risiko terhadap *Inherent Risk* dan *Residual Risk*, terlebih dahulu menentukan standart penilaian berupa parameter *probability* (kecenderungan), parameter *impact* (dampak) dan parameter *Rating* Risiko. Dari hasil rekapitulasi risiko berdasarkan aset dan skenario risiko serta mempertimbangkan parameter *probability* dan *impact* yang telah dibuat, maka dapat diketahui kategori risiko dasar (*Inherent Risk*). *Inherent Risk* merupakan risiko yang dinilai tanpa memasukkan unsur pengendalian yang telah diterapkan. Adapun rekapitulasi hasil penilaian risiko terhadap *Inherent Risk* yang disusun berdasarkan aset dapat dilihat pada Tabel 5 berikut ini.

Tabel 5. Penilaian *Inherent Risk* Berdasarkan Aset

| No | Kategori Aset | Nilai Risiko Dasar | | | | |
|---|---|---|---|---|---|---|
| | | Rendah | Rendah Menengah | Menengah | Menengah Tinggi | Tinggi |
| 1 | Aplikasi | 0 | 0 | 4 | 0 | 1 |
| 2 | Fasilitas | 0 | 0 | 1 | 0 | 0 |
| 3 | Infrastruktur TI | 0 | 1 | 2 | 0 | 0 |
| 4 | Informasi / Data | 0 | 0 | 5 | 2 | 0 |
| 5 | Proses | 0 | 0 | 4 | 0 | 0 |
| 6 | SDM | 0 | 0 | 2 | 1 | 0 |
| | Total | 0 | 1 | 18 | 3 | 1 |

Berdasarkan hasil wawancara dengan beberapa perwakilan dari Dept. TEKINFO dan Dept. TKP & MR, dapat diketahui bahwa setiap risiko – risiko yang teridentifikasi telah memiliki pengendalian tersendiri. Pengendalian tersebut digunakan sebagai dasar untuk melakukan penilaian Residual Risk. Adapun rekapitulasi hasil penilaian risiko terhadap *Residual Risk* yang disusun berdasarkan aset dapat dilihat pada Tabel 6 berikut ini.

Tabel 6. Penilaian *Residual Risk* Berdasarkan Aset

| No | Kategori Aset | Nilai Risiko Dasar | | | | |
|---|---|---|---|---|---|---|
| | | Rendah | Rendah Menengah | Menengah | Menengah Tinggi | Tinggi |
| 1 | Aplikasi | 4 | 0 | 1 | 0 | 0 |
| 2 | Fasilitas | 1 | 0 | 0 | 0 | 0 |
| 3 | Infrastruktur TI | 3 | 0 | 0 | 0 | 0 |
| 4 | Informasi / Data | 5 | 0 | 2 | 0 | 0 |
| 5 | Proses | 3 | 1 | 0 | 0 | 0 |
| 6 | SDM | 1 | 0 | 2 | 0 | 0 |
| | Total | 17 | 1 | 5 | 0 | 0 |

2. *Risk Evaluation*

*Risk Evaluation* bertujuan untuk mengevaluasi apakah risiko – risiko tersebut dapat ditoleransi atau tidak oleh perusahaan. *Risk Evaluation* dilakukan dengan menggambarkan hubungan antara *probability* (kecenderungan) dan *impact* (dampak) ke dalam sebuah matriks yang disebut *Risk Map*. Dari *Risk Map* tersebut dapat diketahui risiko mana saja yang membutuhkan tindakan untuk

mengatasinya. Adapun hasil pemetaan *Risk Map* dapat dilihat pada Tabel 7 berikut ini.

Tabel 7. *Risk Map*

| *Impact* | | | | | | | |
|---|---|---|---|---|---|---|---|
| | **Sangat Besar (5)** | 0 | 0 | 0 | 0 | 0 | 0 |
| | **Besar (4)** | 0 | 0 | 0 | 0 | 0 | 0 |
| | **Sedang (3)** | 1 | 0 | 0 | 0 | 0 | 1 |
| | **Kecil (2)** | 11 | 5 | 0 | 0 | 0 | 16 |
| | **Sangat Kecil (1)** | 3 | 3 | 0 | 0 | 0 | 6 |
| | **Total** | 15 | 8 | 0 | 0 | 0 | 23 |
| | | **Sangat Jarang (1)** | **Jarang (2)** | **Kadang-kadang (3)** | **Sering (4)** | **Sangat Sering (5)** | **Total** |
| | | ***Probability*** | | | | | |

Berdasarkan Tabel 7 di atas, dapat diketahui bahwa terdapat 5 buah risiko yang termasuk dalam kategori Menengah (M) dan 1 buah risiko yang termasuk dalam kategori Menengah Rendah (LM). Kedua kategori tersebut termasuk dalam jenis risiko yang tidak dapat diterima oleh perusahaan, sehingga untuk mengurangi dampak terjadinya risiko perlu dilakukan tindakan mitigasi.

## 5.4. Strategi dan Langkah Mitigasi

Langkah mitigasi dapat dirancang dengan melakukan pemetaan skenario risiko IT ke dalam kerangka kerja COBIT untuk mendapatkan risiko – risiko yang relevan. Skenario risiko TI yang dipetakan terdiri dari 1 *Risk Issue* yang termasuk dalam *New Technology*, 1 *Risk Issue* yang termasuk dalam *System Capacity*, 2 *Risk Issue* yang termasuk dalam *Data(base) Integrity* dan 2 *Risk Issue* yang termasuk dalam *IT Expertise and Skills.* Adapun langkah strategi mitigasi yang disarankan untuk PT. Petrokimia Gresik dalam menyikapi beberapa *Risk Issue* dapat dilihat pada Tabel 8 sampai Tabel 11 berikut ini.

Tabel 8. Langkah Mitigasi *New Technology*

| Risiko | Langkah Mitigasi |
|---|---|
| 1. Permintaan aplikasi diluar modul SAP tidak terpenuhi. | - Menyediakan Staff IT yang secara khusus bertanggung jawab dalam proses perancangan dan pembuatan aplikasi.<br>- Memberikan *training* dan pelatihan kepada seluruh Staff IT mengenai perkembangan teknologi informasi terkini.<br>- Melakukan *Outsourcing* untuk memenuhi banyaknya permintaan aplikasi.<br>- Melakukan analisis *cost-benefit* untuk menentukan investasi jangka panjang dan menentukan prioritas aplikasi yang harus dipenuhi terlebih dahulu. |

Tabel 9. Langkah Mitigasi *System Capacity*

| Risiko | Langkah Mitigasi |
|---|---|
| 1. Operasional SAP lambat dan kurang optimal | - Menyediakan Staff IT yang secara khusus bertanggung jawab dalam proses monitoring dan evaluasi terhadap operasional SAP.<br>- Mengadakan *User Licence* pada setiap unit kerja. |

Tabel 10. Langkah Mitigasi *Data(base) Integrity*

| Risiko | Langkah Mitigasi |
|---|---|
| 1. Gangguan komunikasi data antara PG dengan PIHC.<br>2. Gangguan transmisi data antar departemen. | - Menyediakan Staff IT yang secara khusus bertanggung jawab dalam menjaga integritas dan keamanan data.<br>- Menjalin kerja sama dengan Team IT dari PIHC.<br>- Menyediakan *helpdesk* untuk menampung segala keluhan terkait dengan integritas data, sehingga dapat ditindak lanjuti dengan segera.<br>- Menggunakan teknik *outomatic switch* jika terjadi *failure.* |

Tabel 11. Langkah Mitigasi *IT Expertise and Skills*

| Risiko | Langkah Mitigasi |
|---|---|
| 1. Dukungan teknis dari Team IT kurang optimal.<br>2. Adanya *gap* terkait kemampuan yang dimiliki Staff IT | - Meningkatkan kompetensi setiap Staff IT dengan menambah intensitas dalam mengadakan pelatihan atau training terkait dengan Sistem ERP - SAP.<br>- Memperbaiki pola rekruitmen dan pelatihan SDM.<br>- Mengasah kemampuan setiap Staff IT dengan memberikan penugasan atau pekerjaan yang berbeda – beda, agar Staff IT mampu menguasai segala bidang kompetensi yang berhubungan dengan IT.<br>- Mengadakan monitoring dan evaluasi terhadap kinerja seluruh Staff IT.<br>- Bekerja sama dengan Team IT dari PIHC untuk meningkatkan dukungan teknis operasional ERP – SAP.<br>- Menyediakan *helpdesk* tersendiri untuk memudahkan Staff IT dalam menangani setiap keluhan. |

### 5.5.Rekomendasi

Berdasarkan hasil evaluasi manajemen risiko teknologi informasi PT. Petrokimia Gresik dengan menggunakan analisis *capability level* dan *risk assessment* (Penilaian Risiko), disusunlah beberapa rekomendasi yang dapat digunakan untuk mengembangkan dan memperbaiki penerapan manajemen risiko teknologi informasi serta mengurangi terjadinya risiko teknologi informasi di PT. Petrokimia Gresik. Berikut ini adalah hasil rekomendasi yang telah dibuat berdasarkan domain proses EDM03 dan APO12. Berikut ini merupakan hasil rekomendasi yang diberikan kepada PT. Petrokimia Gresik:

1. Membentuk *team* atau manajemen khusus di bawah naungan Departemen TKP & MR yang bertugas untuk mengelola dan mengkoordinasikan penerapan manajemen risiko teknologi informasi, khususnya sistem ERP-SAP di PT. Petrokimia Gresik.
2. Melakukan evaluasi terhadap kinerja staff serta memberikan pelatihan terkait penerapan manajemen risiko teknologi informasi untuk meningkatkan kompetensi SDM.
3. Membuat dokumen tertulis yang fokus membahas mengenai pedoman dan prosedur penerapan manajemen risiko teknologi informasi, khususnya sistem ERP-SAP di PT. Petrokimia Gresik.
4. Menetapkan metode yang tepat untuk memonitoring penerapan manajemen risiko teknologi informasi di PT. Petrokimia Gresik sehingga dapat memantau kesesuaian antara risiko yang ditemukan dengan *Risk Appetite.*
5. Membuat dokumen tertulis yang membahas mengenai mitigasi risiko, *Business continuity Plan*, *Disaster Recovery Plan*, dan *risk respond* dari seluruh risiko terkait dengan penerapan teknologi informasi.
6. Membuat dokumen tertulis yang membahas mengenai *Cost Benefit Analysis* untuk memperkirakan frekuensi besarnya kerugian dan keuntungan yang harus ditanggung ketika melakukan penanganan pada setiap skenario risiko teknologi informasi.
7. Meningkatkan intensitas kegiatan pemantauan, review, pengendalian dan pengelolaan terhadap penerapan manajemen risiko teknologi informasi melalui program Klinik Risiko dan Kajian Ulang Manajemen Risiko.
8. Membuat dokumen tertulis yang berbentuk seperti Profil Risiko namun secara khusus menampung hasil identifikasi risiko, analisis risiko (baik berupa analisis sumber, penyebab dan akibat dari risiko), evaluasi penilaian risiko dan pengendalian atau penanganan risiko terkait dengan risiko teknologi informasi.
9. Mengoptimalkan penggunaan Sistem Informasi Manajemen Risiko (SIMAR) dalam melakukan pengelolaan risiko teknologi informasi

## 6. KESIMPULAN

Berdasarkan hasil pembahasan terkait penerapan manajemen risiko teknologi informasi pada PT. Petrokimia Gresik, maka dapat diperoleh kesimpulan sebagai berikut:

1. Proses evaluasi penerapan manajemen risiko teknologi informasi pada PT. Petrokimia Gresik menggunakan kerangka kerja COBIT 5 khususnya subdomain EDM03 *(Ensure Risk Optimation)* dan APO12 *(Manage Risk)* menghasilkan beberapa hal berikut ini:
   a. Nilai *Capability Level* untuk subdomain EDM03 berada pada Level 2 yaitu *Managed Process*. Sedangkan Nilai *Capability Level* untuk subdomain APO12 berada pada Level 3 yaitu *Established Process.*
   b. Besarnya *gap* yang terbentuk antara nilai *capability level* yang telah diperoleh dengan nilai *capability level* yang ingin dicapai untuk subdomain EDM03 dan APO12 masing – masing adalah sebesar 1.
   c. Ditemukannya 23 *risk issue* yang terbagi dalam 15 skenario risiko. Dan dari kelima belas skenario risiko tersebut, terdapat 4 skenario risiko yang membutuhkan strategi dan langkah mitigasi.
2. Hasil rekomendasi dan langkah mitigasi yang diberikan untuk perbaikan manajemen risiko teknologi informasi di PT. Petrokimia Gresik adalah sebagai berikut:
   a. Dibuatnya 9 buah rekomendasi agar nilai *Capability Level* pada subdomain EDM03 dapat mencapai Level 3 dan pada subdomain APO12 dapat mencapai Level 4.
   b. Dibuatnya 16 langkah mitigasi berdasarkan 6 buah *risk issue* yang termasuk dalam 4 buah skenario risiko,

diantaranya *new technology, database integrity, system capacity* dan *IT expertise skills.* Langkah mitigasi tersebut dirancang untuk memenuhi permintaan aplikasi diluar modul SAP; untuk mengatasi gangguan transmisi data antara departemen dan departemen serta antara PG dengan pihak PIHC; untuk mengoptimalkan operasional SAP; untuk mengoptimalkan dukungan teknis dari team IT dan untuk mengurangi *gap* yang timbul akibat tidak meratanya kemampuan atau *skill* yang dimiliki oleh setiap staff IT.

## 7. DAFTAR PUSTAKA


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

Dyahaloka, Astri, 2016. *Evaluasi Manajemen Risiko E-Procurement Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Pertamina (Persero)).* Malang : Universitas Brawijaya.

Febriyanti, Aulia., and Bekti C.H, S.Si., M.Kom., 2012. *Manajemen Risiko pada Pengelolaan Data di Bagian Pengolahan Data PT. Petrokimia Gresik. Jurnal Teknik POMITS,* 1(1), pp 1-6. Tersedia di: <http://digilib.its.ac.id> [Diakses 26 Januari 2017]

*Menggunakan Framework Cobit 5: Studi Kasus Dewan Kehormatan Penyelenggara Pemilu* (DKPP). Jakarta : Universitas Islam Negeri Syarif Hidayatullah. Tersedia di : <http://repository.uinjkt.ac.id> [Diakses 24 September 2016]

ITGI., 2003. *Broad Briefing on IT Governance 2nd Edition*. [e-book]. Rolling Meadows : IT Governance Institute.

Petrokimia Gresik, 2012. *Profil.* [Online] Tersedia di : <http://www.petrokimia-gresik.com/> [Diakses 11 Juli 2016].

Pratama, Enda E., and Suhardi., 2013. *Analisis Nilai & Manajemen Risiko Teknologi Informasi (Studi Kasus PT. Bank Tabungan Negara. Tbk).* Bandung : Institute Teknologi Bandung. Tersedia di : <http://www.academia.edu/> [Diakses 6 Oktober 2016].

Pressman, Roger S., 2005. *Software*

Hayaty, M., Rosidi, A., and Arief, M.R., 2013. *Risk Assessment Dan Business Impact Analysis Sebagai Dasar Penyusunan Disaster Recovery Plan (Studi Kasus Di Stmik Amikom Yogyakarta). SEMNASTEKNOMEDIA ONLINE*, 1(1), pp.23-1.

Husein, G.M. and Imbar, R.V., 2015. *Analisis Manajemen Risiko Teknologi Informasi Penerapan Pada Document Management System di PT. JABAR TELEMATIKA (JATEL). Jurnal Teknik Informatika dan Sistem Informasi*, *1*(2). Tersedia di: <http:// http://jutisi.maranatha.edu/index.php/jutisi> [Diakses 6 Oktober 2016]

ISACA., 2012. *COBIT 5 : A Bussiness Framework for the Governance and Management of Enterprise IT.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : Enabling Process.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : The Risk IT Practitioner Guide.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : For Risk.* Rolling Meadows : ISACA.

ISACA., 2012. *COBIT 5 : Self-Assessment Guide.* Rolling Meadows : ISACA.

Islamiah, Mega Putri., 2014. *Tata Kelola Teknologi Informasi (IT Governance) engineering: a practitioner's approach*. United Kingdom : Palgrave Macmillan.

Samaptoaji, Sigit, 2014. *Evaluasi Pengelolaan Risiko Teknologi Informasi (TI) pada Instansi Pemerintah : Studi Kasus Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementrian Dalam Negeri.* Jakarta : Universitas Indonesia. Tersedia di: <http://lib.ui.ac.id> [Diakses 29 Maret 2017]

Setiawan, Alexander, 2009. *Evaluasi Penerapan Teknologi Informasi Di Perguruan Tinggi Swasta Yogyakarta Dengan Menggunakan Model Cobit Framework. Seminar Nasional Aplikasi Teknologi Informasi (SNATI)*. Vol. 1. No. 1. Tersedia di: <http:// http://www.jurnal.uii.ac.id/index.php> [Diakses 24 September 2016]

Suwarno, Fajrin Rizkia P., 2014. *Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Pada Proses Manage Relationship (APO08) (Studi Kasus : PT. OTO Multiartha).* Jakarta : Universitas Islam Negeri Syarif Hidayatullah. Tersedia di : <http://repository.uinjkt.ac.id> [Diakses 24 September 2016]

Teruri, Shabrina., 2016. *Evaluasi Manajemen Resiko Migrasi Sistem MES Menggunakan COBIT 5 IT Risk (Studi Kasus : PT. Krakatau Steel (Persero)Tbk).* Malang : Universitas Brawijaya.

Wibisono, Diaz Mahardika, 2015. *Pengukuran Tingkat Kapabilitas Proses Pengelolaan Risiko Teknologi Informasi Pada Direktorat Sistem Informasi Universitas Airlangga Berdasarkan COBIT 5 Proses APO12 Manage Risk.* Surabaya : Universitas Airlangga.