Model Implementasi *Mission Assurance* dalam *Business Process Management*

Arwin Datumaya Wahyudi Sumari
Program Studi Asymmetric Warfare
Sekolah Strategi Perang Semesta
Universitas Pertahanan Indonesia
Jakarta, Indonesia
arwin.sumari@yahoo.com, arwin.sumari@idu.ac.id

Firman Munthaha
Program Studi Asymmetric Warfare
Sekolah Strategi Perang Semesta
Universitas Pertahanan Indonesia
Jakarta, Indonesia
firman.munthaha@gmail.com

***Abstrak—Business Process Management* (BPM) menggunakan Teknologi Informasi (TI) sebagai salah satu sarana dalam merealisasikan tujuannya. Aktivitas BPM yang berlangsung dalam *cyberspace* selain memberikan keuntungan yang banyak, juga berdampak pada munculnya kerentanan-kerentanan dan ancaman-ancaman *cyber* dalam keamanan informasi BPM itu sendiri. Prosedur *Mission Assurance* dibutuhkan untuk menjamin keamanan informasi dari ancaman *cyber* yang bersifat dinamis dan terus berkembang. Dalam kajian ini diidentifikasikan peranan *Mission Assurance* dalam memberikan tingkat jaminan yang memadai untuk keberhasilan misi BPM. Identifikasi jaminan dan analisis dilakukan menggunakan *Mission Assurance Category* (MAC) dan *Mission Assurance Analysis Protocol* (MAAP). Hasil kajian menunjukkan *Mission Assurance* dapat memberikan pengukuran untuk menjamin misi dari BPM tercapai. *Mission Assurance* juga dapat mencegah dan mereduksi dampak-dampak dari serangan-serangan *cyber* yang kemungkinan dapat dialami oleh BPM.**

Kata kunci—Ancaman cyber; Business Process Management; Mission Assurance; Mission Assurance Analysis Protocol; Mission Assurance Category

I. PENDAHULUAN

Proses bisnis (*business process*) terus berubah serta berkembang baik teknologi maupun metodologinya. Secara umum terdapat tiga pendekatan dalam perubahan proses bisnis yaitu tradisi manajemen, tradisi manajemen kualitas (*quality management*), dan tradisi TI[4]. Pemanfaatan TI dalam *Business Process Model* (BPM) ditujukan untuk meningkatkan keuntungan dan efektivitas perusahaan. Beberapa kriteria yang menjadi sasaran (*target*) adalah efektivitas dan efisiensi, produktivitas, kinerja, kendali, transparansi, *compliance*, dan standardisasi[3]. Pada pola tradisi TI dalam BPM, *cyberspace* menjadi wilayah (*domain*) beroperasinya aktivitas BPM. Dalam mencapai misinya BPM membutuhkan lingkungan informasi yang handal, tersedia, dan aman untuk membantu menyelesaikannya. Dalam konteks ini keamanan *cyber* (*cyber security*) diperlukan bukan saja untuk mencapai misi namu juga untuk mencegah pihak lain menggangu proses pencapaian misi[7].

Keamaman *cyber* perlu diperhatikan dalam memberikan perlindungan terhadap informasi, pekerjaan, dan program agar tetap berjalan untuk mencapai misi. Misi yang dimaksud dalam kajian ini adalah seperangkat tujuan, yang menjadi sasaran ketika menjalankan suatu proses kerja, sedangkan *assurance* yang dimaksud adalah tingkat keyakinan jaminan keamanan suatu sistem. *Assurance* juga bukan suatu ukuran tentang seberapa aman sistem sebenarnya. Secara umum faktor keamanan memang bukan prioritas utama dalam bisnis yang mengutamakan keuntungan (*profit*), namun manajemen perlu mengerti misi organisasi mereka dan bagaimana sistem informasi mendukungnya.

Integrasi serangkaian proses bisnis sejatinya memiliki jaminan bahwa sistem yang digunakan aman, walaupun secara teknis sangat sulit menjamin bahwa suatu sistem tidak ada kelemahan sedikitpun. Dari penggunaan perangkat lunak (*software*) dan perangkat keras (*hardware*) berikut jaringan Internet atau *intranet*, tidak terdapat jaminan bebas dari celah keamanan atau sistem aman dari serangan *cyber* (*cyber attack*). Oleh karenanya BPM yang memanfaatkan TI secara otomatis akan mendapat resiko ancaman serangan *cyber* dan kerentanan (*vulnerability*) dalam keamanan informasi, sehingga memerlukan suatu mekanisme untuk membantu menangkal (*deterrence*) dan mengamankan sistem informasi BPM. Sarana serangan *cyber* memang melalui *cyberspace*, akan tetapi efek yang dihasilkan secara tidak langsung akan berdampak terhadap aktivitas atau pekerjaan di dunia nyata. Kemudian *cyberspace* sendiri dalam arti yang lebih luas sudah menjadi bagian dari bagian aktivitas hidup di masa kini dan dimana saat ini aktivitas personal dan bisnis sulit lepas dari saluran listrik, telekomunikasi dan internet. Langkah awal pengamanan melalui implementasi *Mission Assurance* ini secara umum diasumsikan dapat memberikan jaminan perlindungan terhadap misi agar sasaran-sasaran misi tetap dapat tercapai.

Untuk memudahkan pemahaman, makalah akan disampaikan secara mengalir yang diawali dengan latar belakang kajian pada Bagian I. Landasan-landasan teori terkait *Mission Assurance* akan disampaikan dalam Bagian II, dan diikuti oleh Bagian III yang membahas mengenai BPM beserta siklus hidupnya (*life cycle*). Teknik pengaplikasian Mission Assurance pada siklus hidup BPM akan disampaikan pada

Bagian IV beserta penjelasan-penjelasannya. Makalah ini akan ditutup oleh Bagian V dengan beberapa catatan penutup.

II. MISSION ASSURANCE

Mission Assurance adalah membangun tingkat kepercayaan yang memadai untuk keberhasilan misi[2]. *Mission Assurance* berkaitan dengan proses untk memastikan bahwa suatu pekerjaan memilki suatu rencana yang rinci dan terukur. *Mission Assurance* dalam *Cyber Operations*, yakni operasi-operasi dalam *cyberspace* yang diaplikasikan oleh Angkatan Bersenjata Amerika Serikat, menggantikan paradigma lama *Information Assurance*[5]. Tujuan utama dari *Mission Assurance* adalah memberikan spesifikasi yang terukur dari *Mission Essential Functions* (MEF) dan memverifikasi pengimplementasiannya[2]. Tujuan paling penting dari *Mission Assurance* adalah untuk menciptakan keadaan yang mendukung ketahanan kelanjutan proses bisnis penting perusahaan dan melindungi karyawan, aset, layanan, dan fungsi[8]. Dalam pelaksanaannya *Mission Assurance* memilki ruang lingkup yang luas dan hubungan dengan berbagai bidang. Termasuk dalam kajian ini *Mission Assurance* yang awalnya adalah dirancang untuk operasi-operasi militer, dapat dipraktekkan juga untuk aplikasi-aplikasi di bidang non-militer.

Mission Assurance dalam wilayah *cyberspace* memilki empat langkah[5] yaitu, (1) memberikan prioritas bagi MEF atau fungsi-fungsi penting dari misi; (2) pemetaaan aset-aset *cyber* kritis; (3) penilaian kerawanan MEF; (4) mitigasi kerawanan dan resiko. Empat hal inilah yang menjadi landasan teori dalam menyusun *Mission Assurance Category* (MAC). *Mission Assurance* membutuhkan pemetaan MEF terhadap aset-aset yang berada dalam *cyberspace* untuk mengidentifikasi ketergantungan suatu misi dalam *cyberspace* tersebut. Pemetaan ini mengasumsikan bahwa ada musuh atau pihak tertentu yang berusaha untuk mengeksploitasi atau menyerang misi tersebut dengan memanfaatkan media *cyberspace*. Untuk memenuhi kebutuhan kajian ini digunakan protokol analisis untuk *Mission Assurance* yang lebih komperehensif yakni *Mission Assurance Analysis Protocol* (MAAP).

A. Strategi Mission Assurance

Fokus dari strategi ini adalah keseimbangan manajemen resiko operasional dan penyelesaian masalah. Dalam kenyataanya manajemen resiko operasional sering kurang diperhatikan sehingga menyebabkan banyak manajer mendapat resiko berlebih dari yang seharusnya didapat[2]. Di sisi lain ada juga pertimbangan ekonomi untuk mengurangi resiko operasional sedini mungkin. Dalam hal ini tentunya dapat menghemat biaya lebih banyak jika dapat memitigasi resiko selama dalam masa desain dan pengembangan, daripada menunggu hingga operasi berjalan. Terdapat tiga taktik yang digunakan dalam strategi ini, yaitu: (1) mitigasi resiko operasional dalam proses perancangan dan pengembangan; (2) mengelola resiko operasional selama masa operasi secara berkesinambungan; dan (3) menyelesaikan masalah yang terjadi selama operasi.

B. Mission Assurance Category (MAC)

MAC mencerminkan pentingnya informasi yang berkaitan dengan pencapaian tujuan dan sasaran[6]. MAC digunakan utamanya untuk menentukan persyaratan terkait ketersediaan dan integritas. Dalam kajian ini MAC akan digunakan sebagai alat bantu dalam memberikan ukuran dan gambaran karakter kondisi misi bagi BPM. Terdapat tiga kategori MAC yang ditetapkan sebagaimana diperlihatkan dalam Tabel I.

TABEL I. *MISSION ASSURANCE CATEGORIES* (MAC) [6]

	Karakter Kategori	**Toleransi**	**Konsekuensi Gangguan**	**Kebutuhan Sistem**
MAC I	Menangani informasi vital bagi operasional atau efektifitas misi bisnis baik dari segi isi dan ketepatan waktu	Kehilangan integritas atau ketersediaan data tidak dapat diterima	Dapat berimbas menjadi kerugian langsung dan kehilangan efektifitas misi secara berkelanjutan	Tindakan perlindungan baik teknik maupun prosedur yang paling ketat
MAC II	Menangani informasi penting untuk mendukung kelanjutan bisnis..	Kehilangan integritas tidak dapat diterima dan kehilangan ketersediaan data hanya dapat ditoleransi dalam waktu singkat	Terjadi penundaan atau degradasi dalam memberikan komoditas atau layanan dukungan penting yang dapat memberikan dampak serius terhadap efektifitas misi	Perlindungan tambahan untuk memastikan jaminan
MAC III	Menangai informasi yang berkaitan dengan kegiatan operasional bisnis sehari-hari, namun secara material tidak mempengaruhi dukungan dalam jangka pendek	Kehilangan integritas atau ketersediaan data tidak dapat ditoleransi dan dapat diatasi tanpa memberikan dampak signifikan terhadap efektifitas misi	Dapat terjadi penundaan atau degradasi dalam memberikan layanan dukungan atau komoditas	Tindakan perlindungan yang secara umum sebanding dengan praktek komersial

C. Mission Assurance Analysis Protocol (MAAP)

MAAP adalah protokol atau heuristik untuk menentukan tingkat *Mission Assurance* yang berada dalam proses yang kompleks, dan menyediakan pendekatan terstruktur untuk mengnalisis resiko operasional[2]. Dengan menggunakan MAAP, akan dilakukan analisis BPM secara kualitatif berdasarkan tujuh langkah sebagai berikut:

- Menentukan tujuan misi.
- Karakterisasi semua operasi yang dilakukan dalam menyelesaikan misi.
- Menentukan kriteria evaluasi resiko yang berkaitan dengan tujuan misi.
- Idetifikasi mode kegagalan (*failure mode*) yang potensial.
- Melakukan analisis akar masalah untuk setiap mode kegagalan.
- Membangun profil resiko operasional dari misi.
- Memastikan bahwa resiko operasional masih dalam ambang toleransi.

III. KONSEP SIKLUS HIDUP *BUSINESS PROCESS MANAGEMENT*

BPM terus berkembang literaturnya, sehingga secara umum tidak memiliki satu definisi yang sama antar satu literatur dengan lainny. Namun dari sisi dasar-dasar karakternya, BPM adalah pendekatan yang berpusat pada pengelolaan informasi yang berjalan di dalam proses, yang berdasarkan pada prinsip berikut[3]:

- Strategi pengembangan berkelanjutan yang berdasarkan pada pemodelan, otomatisasi, dan pemantauan alur proses bisnis.
- Organisasi proses (*process organization*), menetukan aturan, tanggungjawab, ketrampilan (*skill*) yang diperlukan untuk implementasi, melaksanakan, dan mengendalikan proses.
- Metodologi yang digunakan untuk mempersiapkan langkah-langkah proses yang sesuai dengan strategi perbaikan berkelanjutan (*continuous improvement*) dan siklus organisasi proses (*process organization cycle*).
- Perangkat lunak yang menyediakan sistem informasi dengan lapisan proses bisnis (*business process layer*)**.**

TABEL II. PERKEMBANGAN SIKLUS HIDUP BPM [1]

Sumber	Tahun	BPM Life Cycle
Davenport dan Short	1990	Identifikasi proses unutk inovasi Identifikasi perubahan tuas atau pengungkit Membangun visi proses Memahami proses yang sudah berjalan Merancang dan membuat purwarupa (*prototype*) proses yang baru
Van de Aalst et.al.	2003	Perancangan proses Konfigurasi sistem Pelaksanaan proses Diagnosa
Netjes et.al.	2006	Perancangan Konfigurasi Eksekusi Kontrol Diagnosa
Zur Mu¨hlen dan Ho	2006	Analisis organisasi Pemberian spesifikasi dan pemodelan Pemodelan aliran kerja (*workflow*) dan implementasi Eksekusi aliran kerja Pergudangan/pengendalian/penambangan proses (*process mining*) Pemantauan kegiatan bisnis
Hallerbach et.al.	2008	Pemodelan *Instantiation*/seleksi Eksekusi Optimasi
Kannengiesser	2008	Proses perancangan Proses implementasi Proses pemberlakuan (*enactment*) evaluasi proses

Interpretasi fase siklus hidup BPM dalam berbagai literatur terus berkembang dan berbeda-beda sebagaimana ditunjukkan Tabel II. Namun secara menyeluruh, terdapat garis merah berupa enam poin[1] berikut:

- Pembangunan strategi mengenai pengelolaan proses bisnis.
- Definisi dan pemodelan proses yang relevan.
- Implementasi proses dalam organisasi.
- Pelaksanaan proses yang diimplementasikan.
- Pemantauan (*monitoring*) dan pengendalian pelaksanaan proses.
- Optimasi dan perbaikan proses.

Keenam fase dalam siklus hidup BPM di atas akan menjadi bahan analisis yang digunakan sebagai model implementasi *Mission Assurace* dalam BPM.

IV. IMPLEMENTASI *MISSION ASSURANCE* DALAM BPM

Hal pertama yang berhasil ditemukan adalah fase siklus hidup BPM dapat dianalisis dengan protokol MAAP berdasarkan hubungan kriteria yang terkait. Pembagiannya dirumuskan sesuai Tabel III. Kemudian hasilnya ditempatkan ke dalam MAC yang bersesuaian. Dalam analisis ini MAC digunakan untuk memberikan gambaran karakter ketersediaan dan integritas informasi, sedangkan MAAP digunakan sebagai protokol dalam menuntun implementasi *Mission Assurance* sesuai hubunganya dengan fase-fase siklus hidup BPM. Hasil akhirnya adalah setiap fase siklus hidup BPM memiliki karakter dan hasil (*outcome*) tertentu yang dihasilkan dari analisis menggunakan Protokol MAAP berdasarkan skema pada Tabel III.

TABEL III. SKEMA IMPELEMENTASI MISSION ASSURANCE DALAM BPM

Siklus Hidup BPM	Protokol MAAP	MAC
(1) Pembangunan strategi mengenai pengelolaan proses bisnis	(1) Menentukan tujuan misi	MAC I
(2) Definisi dan pemodelan proses yang relevan		
(3) Implementasi proses dalam organisasi	(2) Karakterisasi semua operasi yang dilakukan dalam mengejar misi	
(4) Pelaksanaan proses yang diimplementasikan		
(5) Pemantauan (*monitoring*) dan pengendalian pelaksanaan proses	(3) Definisikan kriteria evaluasi resiko dalam kaitannya dengan tujuan misi	MAC II
	(4) Idetifikasi mode kegagalan yang potensial	
	(5) Lakukan analisis akar masalah untuk setiap mode kegagalan	
(6) Optimasi dan perbaikan proses	(6) Membangun profil resiko operasional dari misi	MAC III
	(7) Memastikan bahwa resiko operasional masih dalam ambang toleransi	

A. Menentukan Tujuan Misi

- Sasaran: Menentukan ruang lingkup dari analisis resiko.
- Deskripsi: Dalam MAAP misi suatu proses kerja digunakan untuk menentukan batas-batas analisis resiko. Semua kegiatan yang dilakukan dalam rangka

menyelesaikan misi dimasukkan dalam analisis. Dengan cara ini identifikasi dan dokumentasi misi memberikan batasan hasil analisis.

- Rasionalisasi: Menentukan tujuan misi penting dilakukan untuk mengetahui ruang lingkup analisis. Selain itu untuk mengatur ruang lingkup analisis, dari misi ditetapkan juga dasar dalam mengukur resiko. Semua potensi kerugian diperiksa selama analisis resiko dalam kaitannya dengan tujuan misi itu sendiri.
- Hasil: Seperangkat dokumentasi tujuan misi yang berisi ruang lingkup analisis resiko.

Impelementasi BPM:

- Salah satu sasaran utama BPM adalah identifikasi aktivitas dan hubungan diantara aktivitasnya serta kemudian merepresentasikannya dalam model bisnis. Dalam fase Pembangunan strategi yang merupakan awal dari siklus hidup BPM, MAAP memiliki sasaran adanya dokumentasi tujuan (*goal*) dan ruang lingkup analisis resiko untuk aktivitas beserta hubungan antar aktivitasnya. Aktivitas disini dapat berupa bisnis proses.
- Dalam fase pemodelan proses, proses bisnis diidentifikasi, *review*, dan direpresentasikan dalam model bisnis. Oleh karenanya dalam tahap ini analisia resiko dilakukan terhadap model bisnis yang menjadi representasi proses bisnis. Teknik pemodelan proses bisnis seperti validasi, simulasi, dan verifikasi juga dapat menjadi alat bantu dalam ruang lingkup analisis resiko.

B. Karakterisasi Semua Operasi yang Dilakukan dalam Menyelesaikan Misi

- Sasaran: Memberikan ciri-ciri karakteristik kinerja operasional dari proses.
- Deskripsi: Setelah tujuan misi diidentifikasi, semua operasi yang dilakukan dalam mengejar tujuan tersebut harus ditandai untuk memberikan tolok ukur kinerja operasional. Minimal, harus menentukan parameter kinerja berikut untuk proses yang dianalisis.
- Rasionalisasi: Sebuah model yang akurat dari karakteristik kinerja operasional sangat diperlukan dalam menggambarkan resiko operasional. Hal ini digunakan untuk menggambarkan mana kinerja aktual yang menyimpang atau tidak, sehingga memberikan dasar untuk identifikasi resiko.
- Hasil: Model operasional dari proses kerja yang dianalisis

Impelementasi BPM: Setelah model proses bisnis dibentuk dan diverifikasi, langkah berikutnya adalah implementasi.

- Fase implementasi proses dalam organisasi. Dalam fase ini sistem perlu dikonfigurasi menyesuaikan dengan lingkungan organisasi. Perangkat lunak yang sudah digunkan perlu diintegrasikan juga dengan *Business Process Model Software* (BPMS), begitu juga terkait interaksi antara karyawan dengan BPMS. Kemudian dalam bagian organnisasi proses perlu diberikan spesifikasi karakter seperti apa organisasi proses yang dapat menjamin dan mendukung keberhasilan misi.
- Fase pelaksanaan proses dibutuhkan untuk menjamin bahwa kegiatan proses yang dilakukan sesuai dengan tahapan pelaksanaan yang ditentukan dalam pemodelan proses. Implementasi proses bisnis berisi informasi tentang pelaksanaan proses dan lingkungan teknis serta organisasi di mana mereka akan dieksekusi.

C. Menentukan Kriteria Evaluasi Resiko yang Berkaitan dengan Tujuan Misi

- Sasaran: Menentukan satu standar eksplisit terhadap resiko operasional yang dapat diukur secara seragam.
- Deskripsi: Semua potensi kerugian dalam analisis resiko diukur dalam kaitannya dengan mencapai tujuan misi. Evaluasi kriteria resiko ditentukan parameter untuk memperkirakan nilai dampak dan probabilitas.
- Rasionalisasi: Evaluasi kriteria resiko penting karena memberikan pedoman umum terhadap resiko operasional yang diukur. Memiliki pedoman kriteria tunggal untuk semua operasi merupakan bagian penting dari membangun toleransi resiko operasional yang seragam dalam proses terdistribusi (*distributed process*).
- Hasil: dokumentasi satu pedoman kriteria yang digunakan untuk mengukur dampak, probabilitas, dan eksposur resiko (*risk exposure*)[1].

Impelementasi BPM: Dalam implementasinya di BPM, pemetaan manajemen resiko BPM yang komprehensif dapat menjadi alternatif untuk menjadi pedoman dalam mengukur dampak, probabilitas, dan eksposur resiko. Senada dengan enam hal dalam siklus hidup BPM yang digunakan dalam kajian ini, Muehlen dan Ting-Yi Ho[10] melakukan pemetaan manajemen resiko BPM terhadap taksonomi resiko berdasarkan enam hal dalam siklus hidup yakni:

1. Analisis organisasi.
2. Perancangan.
3. Implementasi.
4. Eksekusi.
5. Pemantauan.
6. Pengendalian.

Pemetaan tersebut diperlihatkan pada Tabel IV, yakni menghubungkan antara faktor resiko dengan resiko yang berkaitan dalam siklus hidup berdasarkan nomor urut.

TABEL IV. PEMETAAN RESIKO BPM TERHADAP TAKSONOMI RESIKO

Faktor Resiko	Resiko Terkait Siklus Hidup
Metode	• Proses analisis atau metode desain tidak valid [1,2] • Metode pemetaan tidak valid (masalah untuk solusi, solusi untuk implementasi) [1,2][2,3] • Metode pemodelan tidak valid [2, 3] • Metode pelaksanaan tidak valid [3] • Metode evaluasi tidak valid [5] • Inkonsistensi evaluasi /pengukuran metode [5], [6] • Mekanisme umpan balik (*feedback*) tidak valid [2,5]
Komunikasi	• Miskomunikasi tujuan [1,2] • Kurangnya komunikasi antara para pemangku kepentingan [semua]

[1] *Risk exposure is the quantified potential for loss that might occur as a result of some activity.*Eksposur resiko adalah kemungkinan kehilangan terkuantisasi yang dapat terjadi sebagai hasil dari suatu aktivitas. Dikutip dari http://www.businessdictionary.com/definition/risk-exposure.html.

Faktor Resiko	Resiko Terkait Siklus Hidup
Metode	• Proses analisis atau metode desain tidak valid [1,2] • Metode pemetaan tidak valid (masalah untuk solusi, solusi untuk implementasi) [1,2][2,3] • Metode pemodelan tidak valid [2, 3] • Metode pelaksanaan tidak valid [3] • Metode evaluasi tidak valid [5] • Inkonsistensi evaluasi /pengukuran metode [5], [6] • Mekanisme umpan balik (*feedback*) tidak valid [2,5]
	• Adanya asumsi tersembunyi dalam proses perancangan dan implementasi [1,2,3]
Informasi	• Informasi yang tidak memadai [Semua] • Informasi tidak valid [1, 2], [2, 3], [5, 2] • Konversi informasi tidak valid [6, 5] • Penyalahgunaan informasi [1,2], [4,6], [5]
Perubahan Manajemen	• Kegagalan untuk mendesain ulang pekerjaan / fungsi [1, 2] • Kegagalan untuk melakukan perubahan yang diperlukan [2] • Ketidakmampuan untuk mengenali masalah [5, 2] • Ketidakmampuan untuk bereaksi terhadap perubahan yang ditunjuk [Semua]
Sistem/ Teknologi	• Kurangnya penerimaan terhadap teknologi [semua] • Penyalahgunaan teknologi [Semua] • Kurangnya fleksibilitas teknologi [Semua] • Kurangnya kompatibilitas teknologi [Semua] • Kurangnya skalabilitas teknologi [Semua]
Kepemimpinan /Manajemen	• Kurangnya kepemimpinan /manajemen [Semua] • Inkonsistensi kepemimpinan/manajemen [Semua] • Tidak adanya kepemimpinan manajemen [Semua]
Sumber daya/ ketrampilan (*skill*)	• Tidak adanya sumber daya/ ketrampilan (*skill*) [Semua] • Penyalahgunaan sumber daya /ketrampilan [Semua] • Ketidakmampuan untuk menggunakan sumber daya/ketrampilan [Semua]
Strategi	• Definisi strategis akurat [Semua] • Definisi strategi tidak jelas [Semua] • Tidak adanya definisi strategis [Semua]

D. Identifikasi Mode Kegagalan yang Potensial

- Sasaran: Teridentifikasinya cara-cara dimana proses dapat menjadi gagal dalam memenuhi kinerja dengan karakteristik tertentu.
- Deskripsi: Semua mode kegagalan yang relevan untuk proses diidentifikasi dengan menganalisis kinerjanya seperti yang didefinisikan dalam model operasional. Sebagaimana digunakan dalam konteks ini, mode kegagalan adalah situasi dimana proses tidak memenuhi parameter tertentu dari kinerjanya. Ini biasanya terjadi ketika kinerja aktual menyimpang dari kinerja yang diinginkan atau diharapkan, yang pada gilirannya, dapat mempengaruhi kemampuan untuk mencapai baik tujuan lokal atau salah satu tujuan misi. Selama proses analisis, mode kegagalan diidentifikasi untuk

  1) Kondisi operasional yang normal atau sudah diperkirakan.

  2) Keadaan yang tidak tersuga atau dipicu oleh peristiwa tertentu.

- Rasionalisasi: Identifikasi mode kegagalan yang potensial, melahirkan tipe dampak yang dapat diharapkan selama operasi dan memberikan informasi penting yang diperlukan ketika mengidentifikasi resiko operasional.
- Hasil: Dokumentasi daftar semua mode kegagalan untuk proses kerja.

Implementasi BPM: Salah satu kunci operasional BPM adalah keluwesan (*flexibility*) atau kemampuan untuk berubah. Dengan adanya identifikasi mode kegagalan yang potensial, manajemen dapat membuat perubahan strategi atau gerakan untuk menghindari daftar mode kegagalan yang potensial. Daftar mode kegagalan yang potensial ini digunakan dalam fase pemantauan dan pengendalian pelaksanaan proses.

E. Melakukan Analisis Akar Masalah untuk Setiap Mode Kegagalan

- Sasaran: Teridentifikasinya resiko tertentu yang dapat mengakibatkan kegagalan proses.
- Deskripsi: Analisis akar masalah dari masing-masing mode kegagalan perlu dilakukan untuk mengetahui keadaan tertentu yang memicunya.
- Rasionalisasi: Analisis akar masalah penting dilakukan untuk mangetahui kombinasi kerentanan-kerentanan (*combination of vulnerabilities*), ancaman-ancaman, and kendali-kendali yang dapat menghasilkan mode kegagalan tertentu. Analisis ini sangat penting untuk menangkap hubungan timbal balik yang kompleks dan ketergantungan antar kondisi yang menyebabkan setiap kejadian yang spesifik dari resiko operasional.
- Hasil: Seperangkat resiko operasional.

Implementasi BPM: Penilaian kerentanan diperlukan untuk mengetahui celah keamanan. Hasil identifikasi ini nantinya dapat digunakan untuk meminimalkan kerugian jika ada yang berusaha memanfaatkan kerentanan tersebut. Hasil dari identifikasi kerentanan ini adalah seperangkat daftar kerentanan dan kelemahan yang terdapat dalam sistem, baik teknis seperti perangkat lunak, perangkat keras, jaringan, dan juga sisi non-teknis seperti organisasi dan manajemen.

F. Membangun Profil Resiko Operasional dari Misi

- Sasaran: Terbangunnya sebuah pandangan komprehensif yang secara akurat mencerminkan bagaimana resiko operasional dapat mempengaruhi misi.
- Deskripsi: Mengembangkan profil resiko operasional untuk misi memerlukan tiga kegiatan analisis tambahan. Pertama, resiko terkait dengan cara yang ditentukan, menghasilkan pandangan agregasi resiko operasional untuk misi. Pada dasarnya, sebuah faktor resiko tunggal rantai sebab-akibat (*causal chain*) yang mempengaruhi misi dikembangkan. Kedua, nilai eksposur resiko operasional untuk misi ditentukan dengan menggunakan kriteria evaluasi resiko yang didefinisikan dan semua data yang relevan dikumpulkan melalui analisis. Akhirnya, analisis terhadap lajur kritis (*critical path*) dari resiko rantai sebab-akibat dilakukan untuk

mengidentifikasi faktor-faktor yang mendorong eksposur resiko operasional dengan misi.

- Rasionalisasi: Sebelum kegiatan mitigasi substansial diinisiasi untuk meningkatkan proses *Mission Assurace*, penting juga untuk mengembangkan profil resiko operasional dari misi.
- Hasil: Profil resiko operasional dari misi.

Implementasi BPM: Analisis resiko operasional dapat diletakkan dalam dua kriteria kondisi operasional yaitu:

- Normal atau kondisi yang diharapkan (intrinsik).
- Keadaan yang tidak terduga atau kejadian dipicu peristiwa (ekstrinsik).

Profil resiko operasional harus menggambarkan efek resiko baik intrinsik maupun ekstrinsik agar dapat memberikan karakter sejauh mana resiko terhadap misi. Profil resiko operasional yang lengkap mengandung tiga komponen yaitu, (1) resiko rantai sebab-akibat (*risk causal chain*); (2) ukuran eksposur resiko operasional misi; dan (3) kunci resiko utama.

G. Memastikan bahwa Resiko Operasional Masih dalam Ambang Toleransi

- Sasaran: Dapat dikembangkannya rencana mitigasi untuk memastikan bahwa resiko operasional sesuai dengan batasan toleransi.
- Deskripsi: Nilai eksposur resiko operasional untuk misi telah ditetapkan. Manajemen harus memutuskan apakah nilai yang dapat diterima. Sebuah analisis *trade-off* dilakukan untuk mempertimbangkan biaya relatif yang terkait dengan pilihan mitigasi terhadap berbagai potensi untuk mengurangi resiko operasional agregasi. Profil resiko operasional menyediakan dasar untuk analisis *trade-off*, dimana resiko yang tersisa (*residual*) yang diperiksa di bawah skenario mitigasi.
- Rasionalisasi: Kendala Organisasi selalu membatasi jumlah sumber daya mitigasi yang dapat diterapkan dalam situasi tertentu. Beratnya biaya berbanding relatif dan manfaat yang terkait dengan pilihan mitigasi sangat penting untuk memastikan resiko yang dibawa dalam batas yang dapat diterima dan dipertahankan pada tingkat dari waktu ke waktu, serta memberikan manajemen keyakinan yang wajar dalam keberhasilan misi.
- Hasil: Dokumentasi rencana mitigasi

Implementasi BPM: Dalam fase optimasi dan perbaikan proses ini, informasi yang tersedia digunakan untuk evaluasi dan meningkatkan model proses bisnis beserta implementasinya. Rencana mitigasi diperlukan untuk memberikan patokan ambang batas tercapainya misi. Oleh karenanya evaluasi dan perbaikannya (*improvement*) menjadi fokus dalam implementasi BPM.

V. CATATAN-CATATAN PENUTUP

Berdasarkan kajian yang telah diuraikan dalam makalah ini, disampaikan catatan-catatan bahwa pemanfaatan TI dalam BPM perlu diperhatikan juga sisi keamananya. Fokus tetap bisnis adalah untuk memperoleh keuntungan (*profitable*) dan kekompetitivan (*competitiveness*), namun kewaspadaan terhadap keamanan informasi yang penting dan kritis tetap perlu diprioritaskan. Terdapat dua aspek yang secara bersama memberikan pengaruh terhadap keamanan informasi dari penggunaan TI dalam BPM, yaitu aspek teknis dan aspek manajemen beserta Sumber Daya Manusia (SDM). Dari sisi teknis baik perangkat lunak, perangkat keras, jaringan yang merupakan bagian dari sistem perlu diberi tingkat jaminan atau keyakinan keamanannya. Kemudian dari sisi manajemen beserta SDM, analisis resiko operasional dapat memberikan ukuran seberapa tinggi ancaman terhadap misi, dikaitkan besarnya ketergantungan manajemen dan SDM terhadap *cyberspace*. Dari hasil analisis dapat dilihat juga bahwa dengan diterapkannya *Mission Assurance*, dapat memperkecil bukan hanya untuk ancaman *cyber* namun juga dapat mereduksi dampak yang akan didapat jika terjadi serangan *cyber*.

DAFTAR PUSTAKA

[1] C. Houy, P. Fettke, and P. Loos, "Empirical Research in Business Process Management – Analysis of an Emerging field of Research", *Business Process Management Journal*, Vol. 16 No. 4, 2010, pp. 619-661.

[2] C.J. Alberts and A.J. Dorofee, "Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments", *Networked System Survivability Program*, Technical Note CMU/SEI-2005-TN-032, Carnegie Mellon University, 2005.

[3] F. Rivard, G.A. Harb, and P. Meret, "The Transverse Information System: New Solution for IS and Business Performance", ISTE and John Wiley & Sons, 2009.

[4] J.V. Brocke dan M. Rosemann, "Handbook on Business Process Management 1", *International Handbooks on Information Systems*, German, Springer-Verlag Berlin Heidelberg, 2010.

[5] M.D. Pritchett, "Cyber Mission Assurance: A Guide to Reducing the Uncertainties of Operating In a Contested Cyber Environment", *Graduate Research Project*, U.S. Air Force Institute of Technology, June 2012.

[6] "US Department of Defense Instruction Number 8500.2 Information Assurance (IA) Implementation", ASD (C3I), Ed., U.S. DoD, 2003.

[7] K. Rhodes. (2010, January 15). "Cybersecurity must Start with Mission Assurance". Available: http://washingtontechnology.com/Articles/2010/01/13/Predict-globally-protect-locally.aspx?s=wtdaily_190110&Page=1.

[8] R. K. Abercrombie, F.T. Sheldon, and M.R. Grimaila, "A Systematic Comprehensive Computational Model for Stake Estimation in Mission Assurance, Applying Cyber Security Econometrics System (CSES) to Mission Assurance Analysis Protocol (MAAP)", *IEEE International Conference on Social Computing/IEEE International Conference on Privacy, Security, Risk, and Trust*, 2010.

[9] K. Jabbour and S. Muccio, "The Science of Mission Assurance," *Journal of Strategic Security*, Vol. 4, No.2, Summer 2011, pp. 61-74.

[10] M.Z. Muehlen and D.T.Y. Ho, "Risk Management in the BPM Lifecycle", *BPM 2005 Workshops*, LNCS 3812, pp. 454-466, German, Springer-Verlag, Berlin Heidelberg, 2006.