ANALISIS RISIKO DAN TINGKAT *MATURITY* DARI ASET INFORMASI KRITIKAL (Studi Kasus di Direktorat Aerostructure PT. X)

Tri Joko Setiarso

Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI
Jl. Ir. H. Juanda 96 Bandung 40132

e-mail: jokotriva@gmail.com

ABSTRAK

Manajemen risiko sangat diperlukan untuk mengurangi risiko kehilangan dan melindungi aset informasi yang kritikal dan melindungi dari pihak-pihak yang tidak berkepentingan.

Ketergantungan PT. X pada teknologi informasi, dan belum diterapkannya *assessment* dan analisis risiko menyebabkan lemahnya keamanan aset informasi yang berakibat pada berkurangnya pendapatan dan kemampuan menangkap peluang bisnis.

Analisis risiko dan tingkat *maturity* dari aset informasi kritikal bertujuan mencari kesalahan kinerja layanan sistem informasi termasuk kesalahan klasifikasi, kesalahan analisis ancaman dan kerentanan, serta kesalahan implementasi pengamanan aset informasi.

Penelitian aset informasi harus mempertimbangkan fungsi bisnis, karena kualitas layanan dari fungsi bisnis terkait akan mempengaruhi kualitas aset informasi. Analisis risiko aset informasi kritikal dapat diperluas ke bidang pendidikan, karena memiliki kesamaan karakter aset informasi kritikal.

Kata-kata kunci: manajemen risiko, aset informasi kritikal, *assessment* risiko, analisis risiko, *maturity*, informasi kritikal

1. PENDAHULUAN

Manajemen risiko dapat mengurangi risiko kehilangan dan melindungi perusahaan dari penyalahgunaan oleh pihak-pihak yang tidak bertanggung jawab. Manajemen risiko memerlukan *assessment* risiko yang tepat, agar dapat membuat ukuran pencegahan atau pengendaliannya. Penelitian analisis risiko yang pernah

dilakukan dirasakan belum mampu mengakomodasi kebutuhan pengamanan aset dengan tepat.

PT. X adalah industri strategis yang harus dapat memenuhi kebutuhan pemerintah dan menguntungkan dari segi bisnis. Ketergantungannya pada teknologi informasi dan belum diterapkannya *assessment* dan analisis risiko telah melemahkan kontrol keamanan aset informasi dan sumber daya manusia yang berakibat pada berkurangnya pendapatan dan kemampuan menangkap peluang bisnis.

Penelitian teknik analisis risiko dan tingkat *maturity* dari aset informasi kritikal bertujuan untuk meneliti kinerja layanan sistem informasi. Sumber-sumber kesalahan kinerja layanan sistem informasi antara lain adalah: kesalahan klasifikasi aset informasi, kesalahan analisis ancaman dan kerentanan, kesalahan implementasi pengendalian keamanan aset informasi kritikal. Temuan dalam kajian diharapkan dapat memberikan masukan dalam pengamanan aset informasi saat menyimpan, memproses, dan menyebarkan informasi organisasi, serta memberikan informasi yang benar pada manajemen agar mudah memutuskan anggaran teknologi informasi, dan masukan pada saat restrukturisasi atau reposisi sumber daya manusia.

Penelitian ini dilakukan di Direktorat Aerostructure (Dit.AE) yang memiliki *core competency* di bidang manufaktur komponen pesawat dan memiliki prospek yang baik sejalan dengan perkembangan lingkungan industri penerbangan.

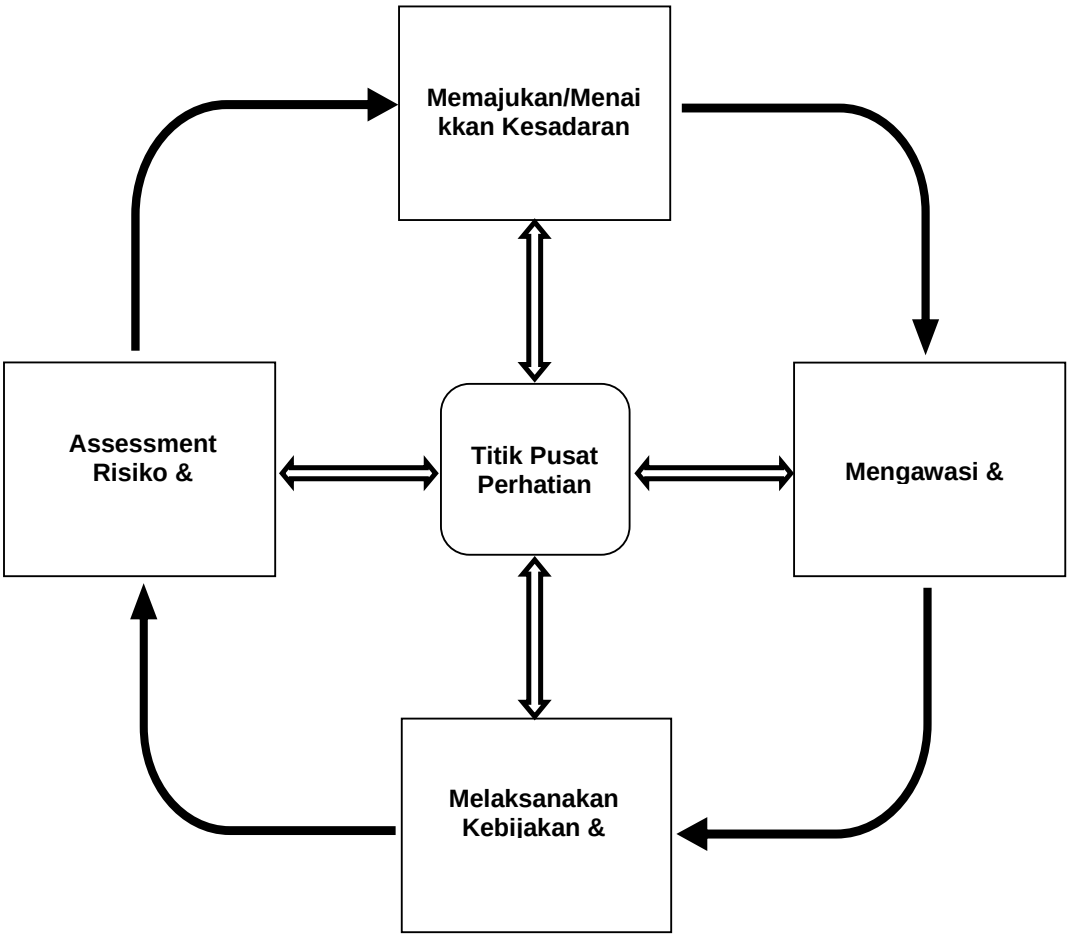
Metode yang digunakan adalah analisis risiko berbasis model bisnis (Suh and Han, 2002), untuk klasifikasi aset informasi mempergunakan metode *University of Nevada of Las Vegas* (UNLV, 2009), penilaian aset kuantitatif mempergunakan pendekatan dari Daniel Moody dan Peter Walsh (1999), analisis kualitatif ancaman dan kerentanan dari NIST 800-30 (Stoneburner at all, 1996) dan tingkat *maturity* keamanan aset informasi kritikal akan mempergunakan *Security Maturity Model* v 0.85 (Aceituno, 2004).

Pengumpulan data sekunder dilakukan dengan **s**tudi dokumentasi dan studi pustaka. Data primer diperoleh dengan observasi, angket, dan wawancara. Analisis data mempergunakan pendekatan kuantitatif (perhitungan penilaian aset informasi setara dengan nilai uang) dan kualitatif (perhitungan persentase sederhana).

2. MANAJEMEN DAN *ASSESSMENT* RISIKO

Manajemen risiko adalah proses identifikasi risiko, *assessment* risiko dan tahapan-tahapan untuk mengurangi risiko sampai pada tingkat yang dapat diterima

(Stoneburner at all, 2002). Manajemen risiko relatif tetap, yang berubah adalah organisasi, yang mengakibatkan perubahan ancaman dan kerentanan, sehingga *assessment* risiko harus dilakukan secara berkesinambungan membetuk sebuah siklus.



Gambar 1. Siklus Manajemen Risiko

Risiko adalah suatu fungsi dari kemungkinan sumber dan ancaman yang berpotensi mengancam kerentanan, dan dampak yang dihasilkan dari peristiwa tersebut yang dapat merugikan organisasi (Rainer at all, 1991).

Assessment risiko merupakan proses pertama dalam manajemen risiko yang menghasilkan data dasar bagi pengambilan keputusan yang tepat dan efektif untuk melindungi dari ancaman (GAO, 2009). *Assessment* risiko harus dilakukan dengan prosedur yang terstruktur dan sistematis, identifikasi yang benar dan penilaian risiko yang tepat, sehingga bermanfaat untuk pengendalian dan cara menghindarinya.

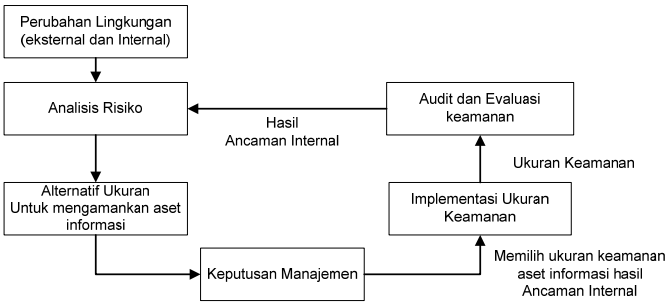
Penelitian tentang metode *assessment* perlu terus dilakukan, karena sistem berbeda akan berbeda pula deskripsi, identifikasi acaman dan peluang-peluang,

penilaian risiko, dan ukuran rekomendasinya (Nicolic and Ruzic-Dimitrijevic, 2009). Diantara perbedaan, ada tiga tahapan yang sama yaitu (Stoneburner, 2001):

1 Menentukan ruang lingkup *Assessment* dan Metodologi.
2 Mengumpulkan dan menganalisis data.
3 Menafsirkan hasil penilaian risiko.

2.1. ANALISIS RISIKO

Analisis adalah suatu proses menafsirkan ancaman (*threat*), kerentanan (*vulnerability*) dan kemunginan-kemungkinan yang mungkin muncul. Hal ini harus dilakukan berulang-ulang dan berkesinambungan karena ancaman dan kerentanan selalu berubah seiring perubahan dalam organisasi. Proses analisis risiko ini digambarkan dalam sebuah siklus analisis risiko (Rainer, 1991).



Gambar 2. Siklus Analisis Risiko

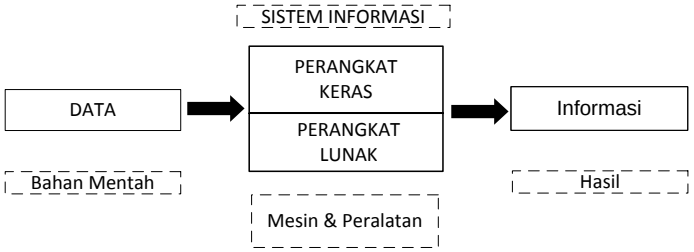
Elemen penting yang harus dilakukan saat proses analisis risiko adalah identifikasi dan valuasi aset, penilaian ancaman dan kerentanan, identifikasi risiko dan evaluasi.

2.1.1. ANALISIS ANCAMAN (*THREAT*) DAN KERENTANAN (*VULNERABILITY*)

Ancaman adalah sumber ancaman yang berpotensi dan berhasil memanfaatkan peluang yang ada untuk diserang (Stoneburner, 2002). Sumber ancaman bisa disengaja atau tidak yang dapat memicu risiko terjadinya kegagalan atau kerugian Sistem Informasi. Kerentanan adalah cacat atau kelemahan dalam prosedur keamanan sistem, disain, implementasi, atau kontrol internal dan dapat mengganggu keamanan sistem(Stoneburner, 2002).

2.1.2. ASET INFORMASI (*INFORMATION ASSET*) DAN ASET INFORMASI KRITIKAL (*CRITICAL INFORMATION ASSET*)

Informasi adalah data yang telah diolah sedemikian rupa menjadi lebih berguna, memberikan gambaran nyata tentang sesuatu keadaan atau peristiwa sehingga membantu penerima dalam proses pengambilan keputusan (Syafrizal, 2005). Informasi merupakan hasil dari proses pengolahan data dengan bantuan Teknologi Informasi, menjadi sesuatu yang bermanfaat (gambar 3) .



Gambar 3. Proses Produksi Informasi (Moody and Walsh, 1999)

Aset informasi memiliki satu sifat atau lebih dari beberapa karakter yaitu bernilai bagi organisasi, tidak mudah dipindahkan bila tanpa biaya, keahlian, waktu, sumber daya atau kombinasinya, dan merupakan bagian dari identitas organisasi. Adapun aset informasi kritikal adalah suatu aset yang memiliki peranan sangat penting dan tanpa aset tersebut tujuan organisasi tidak akan tercapai, atau bahkan akan berhenti sama sekali.

2.1.3. ANALISIS KUANTITATIF DAN KUALITATIF

Analisis risiko tradisional biasanya didasarkan pada peristiwa, peluang dan dampak. Metode ini memiliki kelemahan yaitu kompleks, memakan waktu lama, dan biayanya mahal, dan keterbatasan jumlah dan kualitas data. Pendekatan kuantitatif dengan perkiraan biaya (*moneter*) didasarkan pada tiga aspek yaitu:

1. Kemungkinan bahwa peristiwa yang ada akan merusak
2. Potensi biaya yang harus dikeluarkan untuk mengganti kerusakan
3. Biaya tindakan mitigasi yang dapat diambil.

Data kuantitatif memiliki kelemahan yaitu kesalahan estimasi, yang menyebabkan tidak lengkapnya data tersebut. Bila data tentang biaya tidak tersedia, pendekatan kualitatif dapat dipakai, yaitu dengan cara mendefinisikan risiko secara subjektif dan umum. Kelemahan metode ini adalah lebih bergantung pada keahlian, pengalaman, dan penilaian dari mereka yang melakukan penilaian.

2.1.4. ANALISIS RISIKO BERDASARKAN MODEL BISNIS

Metode analisis risiko berdasarkan model bisnis merupakan analisis dengan mempergunakan pendekatan kuantitatif. Prinsipnya adalah menentukan penting tidaknya peranan fungsi bisnis dalam sebuah model bisnis dan penting tidaknya aset sistem informasi. Memiliki kesamaan dengan proses analisis risiko tradisional. Perbedaannya hanya pada tahap penelitian organisasional dan mempertimbangkan aspek kesinambungan operasional (Suh and Han, 2002).

2.2. PENGELOLAAN DAN PENGAMANAN ASET INFORMASI

Keamanan adalah suatu kualitas atau keadaan yang terbebas dari upaya-upaya yang mengancam keberadaannya dan suatu tindakan yang diambil organisasi untuk melindungi diri dari ancaman (NIST, 1995). Jadi keamanan informasi fokusnya pada ‘data’ dan ‘informasi’ milik perusahaan, dengan cara merencanakan, mengembangkan serta mengawasi semua kegiatan agar tidak disalahgunakan oleh pihak-pihak yang tidak berkepentingan (Syafrizal, 2005).

2.3. *MATURITY* SISTEM KONTROL KEAMANAN

Merupakan seperangkat alat yang dipergunakan organisasi untuk mengukur cara mengamankan dari risiko yang berpotensi mengancam aset yang dimiliki (Homeland Security, 2009). Tujuannya adalah meningkatkan kepercayaan konsumen dan pemangku kepentingan terhadap organisasi, memaksimalkan pengembalian modal investasi pengamanan aset, dan menghidari risiko keamanan. Salah satu modelnya adalah *Security Maturity Model* v 0.85 (SMM v0.85). Model ini mengukur sejauh mana manajemen menerapkan paradigma PDCA (Plan, Do, Check and Act) ketika mendefinisikan dan cara mencapai sebuah target dalam lingkungan organisasinya (Aceituno, 2004).

<table>
<tr><th>Plan</th><th>Do</th><th>Check</th><th>Act</th></tr>
<tr><td>Ruang lingkup: Inventory</td><td rowspan="2">Perlindungan terhadap Siklus Hidup Sistem Informasi</td><td>Tes</td><td rowspan="4">Manajemen Insiden</td></tr>
<tr><td>Target: Kebijakan</td><td rowspan="2">Pengawasan</td></tr>
<tr><td>How to : Prosedur-prosedur</td><td rowspan="2">Manajemen Ukuran Keamanan</td></tr>
<tr><td>Komitmen: Agreement</td><td>Audit</td></tr>
<tr><td colspan="4">Manajemen Anggaran</td></tr>
<tr><td colspan="4">Manajemen Personil</td></tr>
<tr><td colspan="4">Struktur Organisasi & Proses</td></tr>
</table>

Pada prinsipnya model ini membagi tingkat *maturity* kontrol keamanan menjadi lima, yaitu *Initial, Managed, Defined, Quantitatify Managed dan Optimizing.*

3. METODOLOGI DAN PROSES PENELITIAN

Langkah-langkah penting yang akan dilaksanakan dalam penelitian meliputi pra-penelitian, pengumpulan, pengolahan, dan analisis data.

3.1. PENGUMPULAN DATA

Teknik pengambilan datanya ada dua, yaitu pengumpulan data sekunder (diperoleh dengan studi literatur dan dokumentasi) dan pengumpulan data primer (mempergunakan Survei dan Wawancara). Subyek penelitian ini adalah pimpinan departemen yang terkait dengan pengelolaan aset informasi kritikal, yaitu Departemen Computer dan Sistem Aplikasi (CSA), Divisi Integrasi Usaha (BE) dan Manajemen Suberdaya (RE), Departemen Manajemen Konfigurasi, *Quality Management System* (QMS) dan *Quality Assurance* (QA).

3.2. METODE ANALISIS RISIKO BERDASARKAN MODEL BISNIS

Sebagai kerangka dasar penelitian, akan mempergunakan analisis risiko berdasarkan model bisnis.

Table 1. Proses Metode Analisis Risiko berdasarkan Model Bisnis

Tahapan	Methodologi dan Rumus
1. Penelitian Organisasional	
a. identifikasi misi organisasi	Kajian terhadap Rencana Strategis Wawancara dengan Manajer Senior
b. identifikasi tujuan organisasi	Kajian terhadap Rencana Strategis Wawancara dengan Manajer Senior
c. mengembangkan model bisnis	Memecah menjadi model-model bisnis yang lebih kecil
d. identifikasi tujuan masing-masing fungsi bisnis	Wawancara dengan Line Manajer
e. menentukan tingkat kepentingan masing-masing fungsi bisnis	Perbandingan pasangan Menghitung skala prioritas dengan *Analytic Hierarchy Process* (AHP)
2. Identifikasi dan Evaluasi Aset	
a. identifikasi Aset	Kajian seluruh spesifikasi Sistem Informasi
b. menentukan aset berdasarkan fungsi bisnis	Menentukan fungsi masing-masing aset dalam tabel Wawancara dengan Line Manager
c. menentukan aset-aset penting	Membandingkan pasangan aset $AI_i=\sum_{all\,j} (NijxFij)$
d. identifikasi keterkaitan antar aset	Diagram ketergantungan aset
e. menentukan tingkat kepenting aset	AI_i= max(AI_i; AI_j; AI_k; AI_l; . . .) ketika aset *i* sifatnya independen dengan aset lainnya *j, k, l,*

3. *Assessment* ancaman dan kerentanan	Teknik Delphi; *Brainstorming;* Pendekatan Scenario Ancaman; Pendekatan Statistik
4. Perhitungan ALE	$IL_{ij} = AI_i$ x (l/BD) x RT_{ij} $ALE_{ij} = (RC_{ij} + IL_{ij})$ x P_j
Catatan: FI_i: relatif pentingnya fungsi bisnis tingkat terendah $_i$ AI_i: relatif pentingnya aset $_i$ N_{ij}: relatif pentingnya aset $_i$ untuk tujuan fungsi bisnis $_j$ IL_{ij}: pendapatan yang hilang ketika aset $_i$ rusak sebagai akibat ancaman $_j$; I: perkiraan pendapatan tahunan organisasi; BD: jumlah hari kerja (operasional) per tahun; RT_{ij}: perkiraan waktu yang dibutuhkan untuk memperbaiki aset $_i$ ketika ancaman $_j$ berhasil; ALE_{ij}: kemungkina biaya hilang bila aset $_I$ terkena ancaman $_j$; RC_{ij}: biaya yang dikeluarkan untuk mengganti aset $_i$ ketika ancaman $_j$ berhasil; P_j: kemungkinan terjadi bila ancaman $_j$ berhasil.	

3.3. METODE KASIFIKASI ASET INFORMASI

Tahap klasifikasi aset mempergunakan metode UNLV (University of Nevada of Las Vegas.Untuk lebih jelasnya dapat dilihat pada tabel 2.

Tabel 2. Metode Klasifikasi Aset Informasi

Tahapan	Keterangan
1. Merancang Tingkat Sensitivitas	Klasifikasi sensitivitas data dibutuhkan untuk melindungi data dari upaya pengungkapan oleh pihakyang tidak berkepentingan.
2. Merancang Tingkat Kritikalitas	Kemampuan operasional dalam kondisi kritikal adalah suatu *assessment* yang saat beroperasi mengalami gangguan
3. Standar Tingkat Keamanan Informasi	Manajer sistem harus menentukan tingkat keamanan yang tepat berdasarkan: *Confidentiality, integrity dan availability* informasi, sensitivitas dan kritikalitas data sesuai dengan misi organisasi

3.4. PENGEMBANGAN PROSES KLASIFIKASI ASET INFORMASI KRITIKAL

Penelitian ini lebih menekankan pada aset informasi kritikal yang akan mempengaruhi kesinambungan operasi.

Gambar 4. Proses Klasifikasi Aset Informasi

3.5. METODE *ASSESSMENT* RISIKO (*RISK ASSESSMENT*)

Assessment risiko disesuaikan dengan karakter dan kebutuhan organisasi, tergantung pada ruang lingkup dan ketersediaan data agar dapat diidentifikasi faktor-faktor risiko.

3.6. MENGUKUR TINGKAT *MATURITY* KEAMANAN DARI ASET INFORMASI KRITIKAL DENGAN *SECURITY MATURITY MODEL* V 0.85 (SMM V0.85)

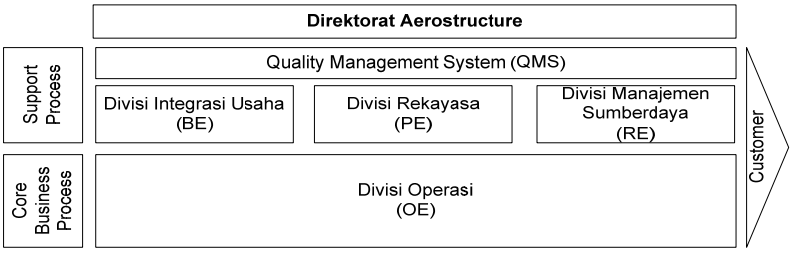
Pengukuran tingkat *maturity* berdasarkan Model Manajemen Plan, Do, Check, Act dan Organizational Structure & Process Security (S & P Security).

Tabel 3. Pemetaan Model Manajemen Keamanan Aset Informasi

Level	Plan	Do	Check	Act	S & P Security
Level 1	Tidak	Tidak	Tidak	Tidak	Mungkin
Level 2	Tidak	Ya	Mungkin	Mungkin	Mungkin
Level 3	Ya	Ya	Ya	Ya	Mungkin
Level 4	Ya	Ya	Ya	Ya	Tdk
Level 5	Ya	Ya	Ya	Ya	Ya

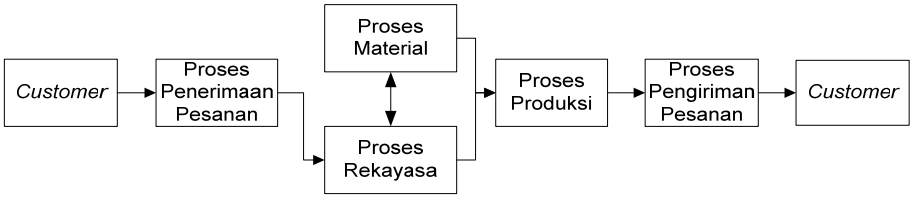
4. HASIL KAJIAN ANALISIS RISIKO DAN TINGKAT MATURITY BERDASARKAN ASET INFORMASI KRITIKAL

PT. X, pada tahun 2004 melalui program efisiensi sumber daya manusia telah mencapai kondisi ideal yaitu memiliki komposisi 44% *non-technical profesional & industrial related*, 35% *engineering*, dan 21% *support*. Melalui program tersebut telah dilakukan restrukturisasi dan mampu menyumbangkan pendapatan terbesar pada organisasi dalam rangka meningkatkan nilai ekonomi perusahaan. Direktorat Aerostructure hanya memfokuskan pada proses bisnis yang sesuai dengan *core competency* yaitu *tool design and component manufacture*. Sedangkan berdasarkan misi organisasinya adalah meningkatkan *value creation* dengan cara peningkatan *lead time* dan penjualan komponen.Kajian proses bisnis untuk mengkaji proses bisnis dengan mempergunakan diagram rantai nilai (*value chain*).



Gambar 5. Rantai Nilai di Direktorat Aerostructure

Dari rantai nilai dan visi organisasi, dapat dipecah lagi menjadi beberapa proses bisnis yang lebih kecil yaitu:



Gambar 6. Proses Bisnis di Direktorat Aerostructure

4.1. KAJIAN FUNGSI BISNIS

Ada lima fungsi bisnis yaitu:

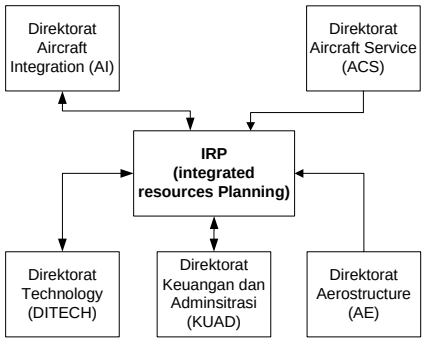
1. Proses Penerimaan Order adalah proses penerimaan order dari *customer* yang dilakukan secara sistem dengan *Integrated Resources Planning* (IRP).
2. Proses Rekayasa adalah proses penyiapan dokumen untuk membuat *work order* (WO). WO adalah sebutan dokumen dari *customer* internal, sedangkan dari luar disebut *purchase order* (PO).
3. Proses Material merupakan tahapan melengkapi *process sheet* dengan dokumen-dokumen kebutuhan material komponen yang akan diproduksi.
4. Proses Produksi mempunyai kegiatan melakukan produksi komponen sesuai dengan *process sheet*, yang di dalamnya terdapat *Work Center Number* (WCN) dan *Job Identification Number* (JIDNO). Operator mesin dan kontrol produksi harus mengikuti prosedur tetap yang sudah ada dalam *process sheet*. Setelah selesai, QC melakukan mengecek *process sheet* dan selanjutnya menerbitkan dokumen *order completion* dan *material ticket* untuk selanjutnya diserahkan ke RE yang akan diproses lebih lanjut.
5. Proses Pengiriman Pesanan adalah mengirimkan komponen yang telah jadi ke *customer*.

4.2. IDENTIFIKASI DAN EVALUASI ASET INFORMASI

Kajian terhadap spesifikasi sistem informasi, akan menentukan jenis-jenis aset sesuai dengan fungsi bisnisnya yang disajikan dalam tabel, dan menentukan tingkat kritikalitas aset.

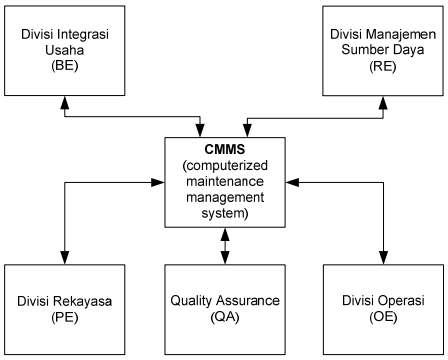
Sistem yang mengelola semua sumber daya disebut *Integrated Resources Planning* (IRP). Kelemahan sistem ini adalah belum mampu menutupi kelemahan

karyawan yaitu rendahnya *up date* data, karena relatif rendah layanan informasi mempengaruhi *confidentiality*, *integrity dan availability* (CIA) aset informasi yang dimiliki organisasi. Data yang di-*input* adalah duplikasi data hasil dokumentasi beberapa tahun yang lalu, sehingga layanan informasinya kurang tepat. Hal ini berakibat pada kesalahan dalam pembuatan estimasi dan proyeksi ke depan.



Gambar 7. Sistem IRP(*Integrated Resources Planning*)

CMMS(*computerized maintenance management system*), yaitu sistem yang dipergunakan untuk mengelola kebutuhan-kebutuhan *maintenance* fasilitas, agar mampu menyiapkan mesin agar bisa dipergunakan pada saat dibutuhkan. Sistem ini memiliki kelemahan yaitu kurangnya *update*, sehingga belum mampu melayani informasi *maintenance* dengan baik, selanjutnya berakibat pada kesalahan pada dokumen *loadplant*, *maintenance plant* dan *configuration plant.*



Gambar 8. Sistem CMMS(*Computerised Maintenance Management System*)

Beberapa sumber kesalahan yang menyebabkan rendahnya layanan informasi *maintenance* peralatan adalah rendahnya *update* informasi *request for maintenance* (RFM), perencanaan *maintenance* dan penjadwalan, *predictive*, *preventive dan*

corrective maintenance report (PR, PM& CM), work order control, work order history, purchasing & inventory control report, dan *cost tracking and analysis.*

4.3. IDENTIFIKASI ASET INFORMASI BERDASARKAN FUNGSI BISNIS

Untuk mengidentifikasi aset informasi maka dilakukan kajian berdasarkan jenis aset dan fungsi aset di tiap proses bisnis.

Tabel 4. Fungsi Bisnis dan Aset Informasi

Kategori	Nama Dokumen/Aset Informasi	Keterangan		
		Pemilik	Bentuk Aset	
			HC	SC
Proses Penerimaan Order	– *Purchase Order* (PO)	BE	v	v
	– *Work Order* (WO)		v	v
	– *Load Plant*		-	v
	– *Schedule of Production* (*Schedule Plant*)		-	v
	– *HR Competence Certificate*		v	v
	– Kontrak Kerja		v	v
	– Review Kontrak		v	v
Proses Material	– Kontrak Pengadaan Material	RE	v	-
	– Proposal Pengadaan Material		v	-
	– *Purchase Order Material*		v	v
	– Perhitungan Harga Komponen		-	v
	– *Material Ticket*		v	-
Proses Rekayasa	– *Process Sheet* (PS)	PE	v	v
	– *Drawing Engineering*		v	v
	– Konfigurasi Mesin		-	v
	– Dokumentasi sistem IRP		v	v
	– Dokumentasi sistem CMMS		-	v
	– *Daily maintenance report*		-	v
	– Weekly maintenance report		-	v
	– Annualy maintenance report		-	v
	– Modul dan manual Produk		v	v
	– Modul dan manual layanan		v	v
	– Modul dan panduan Instalasi CNC		-	v
	– Panduan *Update data Daily Maintenance*		-	v
	– Dokumen pengembang perangkat lunak kit(SDK)		v	v
	– Dokumen Pemrograman Aplikasi Interface (API)		-	v
	– Dokumen Platform Layanan Informasi		-	v
Proses Produksi	– *Process Sheet* (PS)	OE	v	v
	– *Maintenance Plant*		-	v
	– *Control Plant*		-	v
	– *Tool Plant*		-	v
	– Modul dan Manual Instalasi CNC		v	-
	– Manual Maintenance CNC		v	-
	– *Order Completion Form*		v	v
Proses Pengiriman Pesanan	– *Delivery Order*	RE	v	V
	– *Invoice*		v	v

4.4. KLASIFIKASI ASET INFORMASI

Semua aset informasi di Dit.AE, berdasarkan SOP sebagian besar dikategorikan ‘terbatas’ (*limited clasification*), atau hanya untuk kepentingan internal organisasi, dan sebagian kecil rahasia. Sedangkan yang yang bersifat ‘umum’ tidak ada, karena untuk kepentingan umum dipublikasikan oleh korporat.

Dalam kajian ini, secara kualitatif diperoleh gambaran bahwa ***process sheet*** (PS) adalah aset informasi paling kritikal di Dit.AE. Beberapa alasan bahwa ***process sheet*** (PS) adalah aset informasi paling kritikal proses kajian yaitu:

1. Merupakan aset informasi selalu menyertai proses produksi komponen sejak persiapan konfigurasi disain sampai dengan komponen dilakukan *finishing*.
2. Tanpa aset informasi tersebut semua proses bisnis di Dit. AE akan terhenti.

Dengan demikian tahapan analisis risiko berdasarkan model bisnis, secara tidak langsung tidak perlu lagi dilakukan kajian terhadap perbandingan tingkat kritikalitas dan pembuatan diagram saling ketergantungan antar aset informasi.

4.5. *ASSESSMENT* ANCAMAN DAN KERENTANAN

Hanya dilakukan pada *process sheet* sebagai aset informasi kritikal. Asumsinya adalah aset informasi kritikal memiliki perilaku yang ‘unik’ saat dipergunakan dalam proses produksi komponen dan nilainya akan meningkat bila semakin banyak dipergunakan. Pemilik aset informasi adalah Direktorat Aerostructure, sedangkan *custodian* atau pihak yang diberi kewenangan untuk mengelola adalah *Quality Assurance* (QA), Departemen *Configuration Management* (CFM), dan *Computer and System Application* (CSA). Adapun berdasarkan *Standard Operating Prosedur* (SOP) *pengelolaan process sheet* yang sudah selesai dipergunakan dalam proses produksi dikelola oleh *Quality Assurance*(*QA*), khususnya di Departemen *Configuration and Verification Data Receiving* (CVDR).

Proses pelaksanaan klasifikasi aset, beberapa kali mengalami perubahan sesuai dengan kepentingan bisnis. Sedangkan sistem keamanan aset telah dibuat *protocol* administratifnya (khususnya aset informasi yang berupa *print out*) dan *protocol* TI (untuk aset informasi elektronik). Cara pengelolaan aset-aset organisasi berdasarkan perilaku aset dan selanjutnya diperlakukan sesuai kebutuhan organisasi. Praktik perlakuan atau perilaku aset informasi ini mempermudah proses identifikasi ancaman dan kerentanan. Untuk itulah, perlu digambarkan dalam *flow diagram* berikut ini:

Gambar 9. Diagram Perilaku dan Perlakuan Aset Informasi

Aset informasi diklasifikasikan dengan mempertimbangkan perilaku dan perlakuan, agar mempermudah proses *assessment* risiko, sehingga akan nampak secara berurutan tahapan analisisnya adalah *labelling*, penyimpanan, transmisi, dan penggunaan (*user*). Berikut ini hasil kajian prosedur pengelolaan aset informasi tersebut:

1. ***Labelling* Aset Informasi**

   Proses *labelling* dilakukan berdasarkan SOP yang gunanya untuk mempermudah proses pengenalan, penyimpanan. Pada pelaksanannya menganut metode yang umum berdasarkan jenis media penyimpanan yang ada.

2. **Penyimpanan informasi**

   Berbagai bentuk atau kelompok *process sheet* disimpan di ruangan (Lantai 3 Gedung Aerostructure di Departemen CVDR), merupakan tempat khusus yang memiliki klasifikasi keamanan cukup tinggi. Keamanan fisik semacam ini cukup mampu mengamankan media penyimpanan sementara selama 3 bulan.

3. **Pemindahan Aset Informasi (*transmitting*)**

   Pemindahan informasi yang diproteksi, rahasia atau terbatas, diberlakukan prosedur khusus oleh organisasi.

4. **Perlindungan Integritas Aset Informasi**

   Dalam kasus tertentu, bila aset informasi file yang berbentuk elektronik disimpan dalam mode ‘*read only*’. Dalam beberapa jenis dokumen diperlakukan kontrol yang ketat seperti enkripsi. Jika enkripsi dipergunakan, biasanya diserta ‘*key escrow*’.

4.6. ANALISIS DAMPAK

Di dalam melakukan analisis dampak, penulis mempergunakan asumsi yaitu dampak akan dianalisis pada saat proses pembuatan dan penggunaan aset informasi kritikal. Untuk kebutuhan analisis, maka perlu dibahas ancaman dan kerentanan, namun dalam penjelasan yang lebih sederhana. Tujuannya adalah agar lebih mudah dalam pembahasan dampak yang mungkin akan timbul.

Dampak yang terbesar sebagai akibat kerentanan dari aset informasi kritikal adalah waktu yang terbuang (*down time*) karena mesin harus *maintenance*

(direncanakan dan tidak direncanakan), mencapai total 51,6 %. *Down time* artinya *process sheet* tidak bisa dipergunakaan dalam proses produksi komponen. Di dalamnya ada komponen *machine hour* dan *man hour*.

Tabel 5. Dampak dari Aset Informasi Kritikal

No.	Department	Dampak		Keterangan
		Kuantitatif	Kualitatif	
1	Kontrol Produksi Aset	2.66%	Tinggi	Kehilangan order produksi sebelum produksi dimulai
2	*Machining*	0.29%	Rendah	Tingkat kerusakan akibat faktor manusia
3	*Metal Forming & H/T*	0.18%	Rendah	Tingkat kerusakan akibat faktor manusia
4	*Bonding, Composite & Surface Treatment*	0.11%	Rendah	Tingkat kerusakan akibat faktor manusia
5	*Sub - Assembly*	0.32%	Rendah	Tingkat kerusakan akibat faktor manusia
6	*Tool Manufacture & Service*	1.28 %	Sedang	
7	*Maintenance* Fasilitas.			
	– waktu produktif yang hilang akibat *maintenance* yang direncanakan (PM dan PR)	1.43 %	Sedang	
	– waktu produktif yang hilang akibat *maintenance* yang tidak direncanakan (CM)	3.73%	Tinggi	Tingkat kerusakan akibat peralatan produksi
	Total	10.0%		
Sumber: Direktorat Aerostructure PT. DI (2011)				

4.7. TINGKAT *MATURITY* DARI ASET INFORMASI KRITIKAL

Data ancaman dan kerentanan dari aset informasi kritikal diperoleh gambaran bahwa perilaku aset informasi kritikal dapat dikaji saat *process sheet* dibuat, dipergunakan dan saat disimpan. Jadi kontrol keamanan aset informasi kritikal akan berbeda di setiap tahapan, karen *process sheet* masih mengalami perubahan-perubahan. Departemen yang berkepentingan secara langsung yaitu *maintenance plant, configuration design, configuration management, quality control.*

Tabel 6. Pemetaan Model Manajemen Keamanan Aset Informasi

No.	Model Manajemen	Jumlah					Kesimpulan
		Menjawab 'Ya'	Pertanyaan	Dept.	Skor Model	Persentase	
1	Plan	13	11	5	55	23.6%	Tidak
2	Do	29	11	5	55	52.7%	Ya
3	Check	22	7	5	35	40.0%	Tidak
4	Act	0	2	5	10	0.0%	Tidak
5	S & P Security	7	7	5	35	20.0%	Tidak

Catatan:
Skor Model Manajemen : (Jumlah jawaban : jumlah pertanyaan) x 100
Asumsi : Jika jawaban $\geq$ 50% = Ya; Jika jawaban < 50% = Tidak

Sebagian besar (52.7%) sumberdaya di lima departemen melakukan praktik-praktik pengecekan sumber daya kritikal untuk dan pelaksanaan pengamanan aset informasi kritikal. Dengan demikian tingkat *maturity* dari keamanan aset informasi kritikal organisasi ini adalah **SMM Level-2: *Acknowledged.*** Hal ini berarti, organisasi telah melakukan tindakan nyata dan menganggap keamanan merupakan sesuatu yang penting dan telah melakukan upaya pengamanan. Namun mereka beranggapan bahwa keamanan aset informasi adalah penting, namun dalam kajian ini diperoleh kenyataan, bahwa tanggung jawab keamanan ada di tangan inspektorat (pengawas internal) dan kesadaran dalam melakukan dokumentasi praktik-praktik pengamanan masih dirasakan sangat kurang, sehingga pihak manajemen mengalami kesulitan saat mengambil keputusan untuk proyeksi pengamanan aset informasi kritikal pada tahun mendatang. Peristiwa-peristiwa kehilangan aset informasi dimulai saat restrukturisasi (tahun 2004). Orang-orang yang berkepentingan dan memiliki kompetensi dalam kontrol keamanan aset rata-rata sudah keluar (PHK), sehingga penanganan dokumentasi saat ini hanya berdasarkan kebutuhan minimum. Jadi pengamanan aset informasi sangat minimal, hanya sebatas dapat dipergunakan untuk persiapan, memproses dan kelancaran produksi komponen. Meskipun *process sheet* bersifat sangat rahasia, namun orang-orang yang tidak berkepentingan dengan mudah memperolehnya.

5. ANALISIS DAN DISKUSI HASIL KAJIAN

Analisis yang dimaksud di sini adalah temuan-temuan selama proses kajian itu sendiri. Berikut ini adalah beberapa pokok bahasan hasil dari proses kajian tersebut:

5.1. PROSES IDENTIFIKASI ASET INFORMASI BERDASARKAN MODEL BISNIS PERLU DILAKUKAN PENYESUAIAN AGAR DAPAT DITERAPKAN DI INDUSTRI KOMPONEN PESAWAT

Analisis risiko berdasarkan model bisnis lebih tepat bila dipergunakan untuk mengkaji proses bisnis tunggal atau unit bisnis kecil dan aset fisik. Untuk industri manufaktur komponen pesawat terbang, yang proses bisnisnya relatif besar dan terdiri dari beberapa unit bisnis, memerlukan proses yang panjang. Dalam pelaksanaan identifikasi aset informasi kritikal, bisa dilakukan hanya sampai pada tahap dua, yaitu *assessment* ancaman dan kerentanan. Hal ini disebabkan karena secara kualitatif aset informasi kritikalnya sudah teridentifikasi. Untuk kebutuhan identifikasi aset pada industri manufaktur dibutuhkan beberapa tahap berikut ini:

1. Analisis rantai nilai (***value chain***): proses ini akan membantu mempermudah memahami proses bisnis dan sistem informasi yang dipergunakan dalam organisasi.
2. Membuat proses bisnis berdasarkan diagram *value chain*.
3. Memecah proses bisnis pada tahap 3 menjadi unit-unit bisnis yang lebih kecil. Cara ini dapat dilakukan beberapa kali sampai ditemukan unit bisnis yang paling kecil.
4. Memilih proses bisnis kritikal di tiap-tiap tahap pemecahan proses bisnis.
5. Melakukan identifikasi aset-aset kritikal di tiap tahapan pemecahan proses bisnis.
6. Setelah teridentifikasi aset-aset informasi kritikal di tiap pemecahan proses bisnis, maka baru bisa melakukan analisis ancaman dan kerentanan (analisis resiko).

5.2. KLASIFIKASI ASET INFORMASI DIKEMBANGKAN OLEH UNLV PERLU DILAKUKAN PENYESUAIAN APABILA DIPERGUNAKAN KALSIFIKASI ASET INFORMASI KRITIKAL

Klasifikasi aset yang dikembangkan oleh UNLV dipergunakan untuk proses klasifikasi aset informasi yang sudah selesai dipergunakan proses produksi. Untuk klasifikasi saat aset informasi yang masih terlibat langsung dalam proses produksi, perlu pengembangan metode klasifikasi aset baru yang didasarkan pada **sifat** dan **perilaku (perlakuan)** aset informasi tersebut, sesuai dengan tingkat keterlibatan *process sheet* dalam berbagai fungsi bisnis.

Berikut ini adalah tahapan yang dapat membantu proses klasifikasi:

1. Berdasarkan kritikalitas : akan menentukan *cost-effective security control*
2. Berdasarkan kepemilikan : akan mempermudah cara memperoleh data dalam hubungannya dengan kejelasan dan ketepatan informasi.

Tahapan dalam perilaku dan perlakuan, berguna untuk mengidentifikasi ancaman dan kerentanan, karena proses ini berbeda dengan aset–aset lainnya.

5.3. ANALISIS ANCAMAN DAN KERENTANAN ASET TI BERBEDA DENGAN ASET INFORMASI

Aset informasi bersifat mudah dipindahkan, sehingga sifat demikian memiliki ancaman dan kerentanan yang berbeda. Perilaku aset tersebut memiliki risiko ancaman dan kerentanan lebih tinggi dari aset fisik, namun di sisi lain memiliki potensial ekonomi yang lebih tinggi pula. Potensial ekonomi masa depan yang tinggi disebabkan karena semakin banyak dipergunakan semakin tinggi nilainya dan tidak mengalami depresiasi nilai.

Perilaku aset informasi memiliki pengertian proses *labelling*, penyimpanan dan *transmiting* (pemindahan) dan *using*. Masing masing tahapan memiliki ancaman dan kerentanan yang berbeda-beda. Faktor yang menyebabkannya adalah kebijakan dari pemilik, perlakuan dari petugas (*custodian*) dan pengguna (*user*).

Dalam kaitannya dengan produksi komponen, ditemukan beberapa kondisi sebagai berikut:

1. Analisis ancaman dan kerentanan dapat dilakukan pada saat proses pembuatan, proses penggunaan dan proses penyimpanan.
2. Tingginya ketergantungan dan lemahnya layanan aset informasi dari fungsi bisnis terkait, merupakan ancaman paling besar dan menyebabkan rendahnya *integrity* aset informasi kritikal.
3. Analisis ancaman dan kerentanan secara kuantitatif dengan model bisnis sulit untuk dilakukan, sehingga perlu waktu untuk penelitian berikutnya.

5.4. VALUASI ASET INFORMASI ANTARA TEORI DENGAN DI OBYEK KAJIAN BERBEDA

Teori-teori yang membahas proses valuasi aset yang ada saat ini, lebih banyak membahas aset fisik (aset tetap), sedangkan untuk mengukur nilai aset informasi masih relatif sedikit. Untuk proses valuasi aset infromasi, perlu dilakukan tahapan-tahapan sebagai berikut:

1. **Nilai Awal** yaitu nilai proses memproduksi data/aset informasi tersebut. Nilai ini dihitung dengan mempergunakan kaidah ekonomi. Apabila terjadi kehilangan *invoice* (aset informasi kritikal) senilai Rp 10 juta, maka total kehilangan yang

akan terjadi adalah senilai bahan mentah (*raw material*) yang ada di dalam faktur. Cara menghitungnya yaitu :

a. Nilai Raw Material = Nilai Faktur – Profit
b. Nilai Faktur = nilai jual komponen yang akan *didelivery* ke *customer*
c. Profit = nilai jasa yang dikehendaki oleh produsen termasuk di dalamnya *man hour, spent* dan *cost l*ainnya.

2. **Nilai Sejarah** (nilai guna/utilitas) yaitu nilai yang dihitung berdasarkan perkalian dari variabel "jumlah tahapan proses" (dihitung dari jumlah personel yang menandatanganinya) dan "Waktu" (dihitung berdasarkan waktu yang dibutuhkan untuk memproses dokumen di setiap tahapan). Lamanya waktu yang dibutuhkan oleh operator di setiap tahapan produksi akan meningkatkan nilai aset informasi.

5.5. BEBERAPA PENYEBAB PERMASALAHAN CACAT DOMINAN PRODUKSI KOMPONEN

Dampak yang timbul akibat kurangnya *confidentiality, integrity dan availability* (*CIA*) adalah terjadinya *rejected,* s*cratch* (cacat dominan) pada *single parts*. *Scratch* adalah penyebab cacat material *single part* paling dominan pada program A380, Paragon dan Boeing 777 yaitu 71,8%.

CIA disebabkan karena faktor manusia (operator), mesin (*maintenance*), material dan metode yang digunakan. Dampak yang terbesar sebagai akibat kerentanan dari aset informasi kritikal adalah waktu yang terbuang (*down time*) karena mesin harus *maintenance* (direncanakan dan tidak direncanakan, mencapai total 51,6 %. *Down time* artinya *process sheet* tidak bisa dipergunakaan dalam proses produksi komponen. Di dalamnya ada komponen *machine hour, man hour*, keterlambatan *delivery*.

5.6. PENGUKURAN TINGKAT MATURITY DARI KEAMANAN ASET INFORMASI KRITIKAL TIDAK BISA DILAKUKAN SECARA TERPISAH DENGAN ANALISIS ANCAMAN DAN KERENTANAN

Analisi ancaman dan kerentanan aset informasi kritikal merupakan bagian yang tidak terpisahkan dengan proses pengukuran tingkat *maturity* dari aset informasi kritikal. Dari proses kajian diketemukan tahapan-tahapan yang perlu dilakukan agar proses pengukuran tingkat *maturity* aset informasi lebih mudah yaitu:

1. Proses analisis ancaman dan kerentanan dilakukan pada setiap proses pembuatan *process sheet*, penggunaan dan penyimpanan.

2. Identifikasi masing-masing fungsi bisnis.
3. Mempersiapkan daftar pertanyaan menurut model manajemen.
4. Pengolahan data sesuai model manajemen PDCA (*Plan. Do, Check, Act and S & P*).
5. Membuat formulasi berdasarkan jumlah kriteria di setiap model manajemen PDCA.
6. Membuat tabel pemetaan sesuai kriteria yang sudah ada.
7. Menyesuaikan tabel hasil pemetaan dengan kriteria *SMM Level of Maturity v0.85*.

6. KESIMPULAN

Teknik penilaian aset secara kualitatif yang ada saat ini, belum dapat dipergunakan untuk menilai aset informasi secara efektif. Hal ini disebabkan karena kesulitan dalam mengembangkan suatu pendekatan yang tepat untuk mengukur informasi sebagai aset ekonomi. Informasi menganut hukum-hukum ekonomi seperti aset lainnya, sehingga sulit untuk menerapkan metode penilaian yang umum dipakai.

Tahapan-tahapan memecah proses bisnis menjadi unit yang lebih kecil, membuat proses identifikasi aset semakin mudah dan jelas arahnya. *Assessment* secara bertahap, memudahkan organisasi melakukan *assessment* secara berkesinambungan, karena diidentifikasi aset informasi kritikal dan kontrol keamanan oleh pihak manajemen semakin efektif. Hambatan terbesar pengukuran risiko dan kerentanan aset informasi, adalah sifat aset informasi memiliki perilaku yang unik, berbeda dengan aset lainnya.

PT. X memiliki infrastruktur teknologi informasi dan sistem informasi yang sangat baik, dengan *standar operating prosedur* yang terdokumentasi. Setelah restrukturisasi, perhatian karyawan dan manajemen dalam melakukan *update* aset informasi relatif rendah, sehingga mempengaruhi integritas dan ketersediaan data. Kondisi ini telah berpengaruh pada kemampuan organisasi dalam memanfaatkan peluang-peluang bisnis dan mengantisipasi perubahan persaingan bisnis.

Analisis risiko berdasarkan model bisnis, relevan menganalisis proses bisnis tunggal atau unit bisnis kecil dan aset fisik. Dalam produksi komponen, analisis ancaman dan kerentanan dapat dilakukan saat proses pembuatan, proses penggunaan dan proses penyimpanan. Lemahnya layanan informasi dari fungsi bisnis lain merupakan ancaman paling besar terhadap *integrity* aset informasi kritikal. Analisis ancaman dan kerentanan secara kuantitatif berdasarkan model bisnis sulit untuk

dilakukan, sehingga perlu dilakukan penelitian lanjutan. Klasifikasi aset yang dikembangkan oleh UNLV lebih tepat untuk klasifikasi aset informasi yang sudah selesai digunakan. Penilaian aset informasi di Dit.AE hampir diabaikan baik dalam audit, penelitian dan praktek. Tingkat *maturity* dari keamanan aset informasi kritikal Direktorat Aerostructure adalah **SMM Level-2: *Acknowledged.*** Hal ini berarti, organisasi telah melakukan tindakan nyata dan menganggap keamanan merupakan sesuatu yang penting dan telah melakukan upaya pengamanan.

7. DAFTAR PUSTAKA

[1]. Aceituno, V. ***Security Model Draft v0.85 : An ISECOM Project***. [Online]. Tersedia: http://www.isecom.org/mirror/Security_Maturity_Model_v0.85.pdf. [25 September 2011]

[2]. Aljafari, R. and Sanikar S., ***A Risk Assessment Framework for Inter-Organization Knowledge Sharing***, University of Nebraska at Omaha, USA, 2007

[3]. CIAO, ***Practical for Securing Critical Information Assets***, Critical Infrastructure Assurance Office, Washington D.C. 2000

[4]. COA, ***Information Classification***, Jericho Forum-COA Service Paper, http://www.opengroup.org/jericho/publications.htm,Version 1.0, January 2009

[5]. Gaol, S. and Chen, V. ***Information Security Risk Analysis: A Matrix-Based Approach***, University at Albany, School of Business University at Albany, SUNY. New York, 2009

[6]. GAO,***Implementation Security Risk Assessment***, 2009

[7]. Kindinger, J.P. and Darby J.L., ***Risk Analysis-A new Qualitative Risk Management Tool***, proceeding of the project management Institute Annual Seminars & Symposium, September7-6, 2000.

[8]. Kamat, M. ***ISO 27001. Guideline for Information Asset Valuation***. ISO27K Implementer's Forum, www.ISO 27001 security.com, 2009

[9]. Homeland Security, ***Information Technology Sector Baseline Risk Assessmen*t**, August 2009,

[10]. Moteff, John***, Risk Management and Critical Infrastructure Protection: Assesing, Integrating, and Managing Threats, Vulnarabilities and Consequences,*** CRS Report for Congress, September2, 2004

[11]. Moody, D,.and Walsh P. ***Measuring The value of Information: An Asset Valuation Approach***, European Conference on Information Systems (ECIS'99), Copenhagen Business School, 23-25 June 1999

[12]. NIST***, An Introduction to Computer Security: The NIST Handbook***, NIST Special Publication 800-12**,** US Department of Commerce,1995

[13]. Nikolic, B., and Ruzic-Dimitrijevic, L. ***Risk Assessment of Information Technology Systems,*** The Higher Education Technical School of Professional Studies, Novi Sad, Serbia, Issue in Informing Science and Information Technology, Volume 6, 2009

[14]. Newman, D. E., Nkei, Bertrand, Carreras, B. A., Dobson, I., Lynch, V. E. Paul Gradney. ***Risk Assessment in Complex Interacting Infrastructure Systems,*** Thirthty-Eight Hawaii International Conference on System Science , January 2005, Bid Island, Hawaii, copyright 2004, IEEE.

[15]. Rayner, R. K., Snyder, C.A. and Carr, H.H. ***Risk Analysis for Information Technology***, Journal of Management Information Systems/Summer 1991, Vol. 8 No. 1, M.E. Sharpe Inc., 1991

[16]. Stoneburner, G., Goguen, A., and Feringa, A. ***NIST, Special Publication 800-30: Risk Management Guide for Information Technology Systems,*** US Department of Commerce, 2002

[17]. Stoneburner. G., Hayden, C., and Feringa, A. ***Enginering Principles for Information Technology Security (A Baseline for Achieving Security),*** NIST, Special Publication 800-27, US Department of Commerce, 2001

[18]. Swanson, M. ***Security Self-Assessment Guide for Information Technology Systems,*** NIST, Special Publication 800-26, US Department of Commerce

[19]. Suh, B. and Han, I.,***The Risk Anaysis Based on A Business Model,***Science Direct Journal, 26 Sepetember 2002

[20]. Swiss CTI-Project.***Risk Analysis of Information Systems by Agent-based Modeling of Business Process***,

[21]. Swanson, M., Bartol, N., Sabato, J., Hash, J., and Graffo, L. ***Security Metrics Guide for Information Technology Systems,*** NIST, Special Publication 800-55

[22]. Swanson, M. and Guttman, B. ***NIST : Generally Accepted principles and Practices for Securing Information Systems***, US Department of Commerce, 1996

[23]. Syafrizal, M.***Information Security Management System (ISMS) Menggunakan Standar ISO/IEC 27001:2005***, STMIK AMIKOM Yogyakarta

[24]. Taubenberger, S. and Jurjens, J. ***IT Security Risk Analysis based on Business Process Model enhanced with Security Requirements***, Open University, Computing Department, UK, 2011

[25]. USAID, ***Risk Assessment Guidelines : A Mandatory Reference for ADS Chapter 545***, M/DCIO, 06/01/2006[26].