

RISK ASSESSMENT SISTEM PENGIRIMAN DAN PENGOLAHAN DATA PUSAT TEKNOLOGI DATA DAN PENGINDERAAN JAUH LEMBAGA PENERBANGAN DAN ANTRIKSA NASIONAL

Winarni
Pusat Pengkajian Kedirgantaraan
Lembaga Penerbangan dan Antariksa Nasional

ABSTRACT

Presidential Instruction Number 6 Year 2012 has mandated LAPAN as the agency in charge of providing data high resolution satellite remote sensing with Indonesian government license. With the tasks, the system security in the transfer and processing of data becomes important, so the required for assessment (risk assessment) of the current system and measures to mitigate the risks. This study aims to identify and assess the risks that exist in the delivery system and data processing satellite remote sensing imagery. The methodology used is the Microsoft Security Assessment Tools (MSAT). The results showed that (1) a vital asset in the delivery system and satellite image data processing is the satellite image data (raw data), data processing software, and the data have been processed, (2) aspects that have the greatest risk are operations and Infrastructures.

Key word : Risk Assessment , MSAT , Satellite Image Data , Remote Sensing

ABSTRAK

Instruksi Presiden No. 6 Tahun 2012 telah mengamanatkan LAPAN sebagai lembaga yang berwenang dalam menyediakan data satelit penginderaan jauh resolusi tinggi dengan lisensi pemerintah Indonesia. Dengan tugas tersebut maka sistem keamanan dalam proses pengiriman dan pengolahan data menjadi hal yang penting, sehingga diperlukan penilaian (*risk assessment*) terhadap sistem yang ada saat ini dan langkah memitigasi risiko. Penelitian ini bertujuan untuk mengidentifikasi dan menilai risiko yang ada pada sistem pengiriman dan pengolahan data citra satelit penginderaan jauh. Metodologi yang digunakan adalah *Microsoft Security Assesment Tools* (MSAT). Hasil penelitian menunjukkan bahwa (1) asset vital dalam sistem pengiriman dan pengolahan data citra satelit adalah data citra satelit (raw data), software pengolah data, dan data yang telah diolah; (2) aspek yang memiliki resiko terbesar adalah *operations* dan *infrastructures*.

Kata kunci : Risk Assessment , MSAT, Data Citra Satelit, Penginderaan Jauh

1. Pendahuluan

1.1 Latar Belakang

Lembaga Penerbangan dan Antariksa Nasional (Lapan) sebagai salah satu Lembaga Lembaga Pemerintah Non Kementrian (LPNK) mempunyai tugas melaksanakan tugas pemerintahan di bidang penelitian dan pengembangan serta pemanfaatannya sesuai dengan ketentuan perundang-undangan yang berlaku.¹ Secara srtuktur organisasi, Lapan dipimpin oleh seorang Kepala, yang membawahi tiga Deputi (Deputi Bidang Penginderaan Jauh, Deputi Bidang Teknologi Dirgantara, dan Deputi Sains, Pengkajian dan Informasi Kedirganatraan) dan satu Sekretariat Utama. Salah satu tugas Deputi Bidang Penginderaan Jauh (Deinderaja) tersebut adalah melaksanakan perumusan dan pelaksanaan kebijakan penginderaan jauh.² Untuk penyelenggaraan tugas tersebut, salah satu fungsi Deinderaja adalah melakukan penelitian dan pengembangan teknologi sistem akuisisi dan stasiun bumi, pengolahan data dan pengembangan bank data penginderaan jauh.³ Pengembangan kemampuan Lapan saat ini difokuskan pada pengembangan Bank Data Penginderaan Jauh Nasional untuk melayani kebutuhan data penginderaan jauh seluruh Indonesia, pengembangan model-model pemanfaatan untuk pengelolaan sumber daya alam dan mitigasi bencana, serta pembangunan pusat informasi pemantauan bumi dan atmosfer untuk membantu penanganan bencana dan pengelolaan sumber daya alam nasional.⁴

Terkait dengan pengembangan Bank Data Penginderaan Jauh Nasional tersebut, pada tahun 2013 Lapan telah menegaskan bahwa salah satu sasaran yang akan dicapai Lapan pada tahun 2014 adalah Bank Data Inderaja Nasional telah bekerja secara penuh dengan ditunjang oleh akuisisi secara kontinu data MTSAT, Terra/Aqua, NPP, NOAA, Feng Yung, LDCM/ Landsat-8, Landsat-7, SPOT 5 dan SPOT 6 dan lain-lain⁵. Stasiun Bumi Penginderaan Jauh di Parepare didukung oleh stasiun bumi Rumpin dan Stasiun Bumi Biak menjadi fasilitas akuisisi yang sangat handal dengan didukung oleh sistem pengoperasian yang tidak terputus oleh kerusakan alat dan kendala operasional⁶. Hal tersebut selaras dengan Inpres No.6 Tahun 2012 tentang Penyediaan, Penggunaan, Pengendalian Kualitas, Pengolahan, dan Distribusi Data Satelit Penginderaan Jauh Resolusi Tinggi⁷ serta UU Nomor 21 tahun 2013 tentang Keantariksaan yang telah menjadi tulang punggung legal Operasi Bank Data Penginderaan Jauh Nasional. Bank Data Penginderaan Jauh Nasional telah menjadi sumber data penginderaan jauh nasional serta rujukan dalam pengembangan perekayasaan stasiun bumi dan pengolahan data penginderaan jauh⁸.

Dalam operasionalnya, Bank Data Penginderaan Jauh Nasional dilaksanakan oleh Pusat Teknologi Data dan Penginderaan Jauh⁹. Dengan salah satu sasaran capaian kemampuan operasional Bank Data Penginderaan Jauh Nasional Tahun 2013 adalah implementasi dari Inpres No. 6 Tahun 2012. Untuk menindaklanjuti Inpres tersebut, Lapan perlu: (1) melakukan akuisisi data satelit penginderaan jauh resolusi tinggi untuk seluruh wilayah Indonesia dengan lisensi Pemerintah Indonesia; (2) melaksanakan koreksi radiometrik dan pengendalian kualitas data satelit penginderaan jauh resolusi tinggi; dan (3) pelayan data satelit penginderaan jauh resolusi tinggi ke seluruh Kementrian/ Lembaga, TNI, Kepolisian dan Pemerintah Daerah¹⁰.

Kondisi layanan data satelit resolusi tinggi ke berbagai instansi yang membutuhkan tersebut adalah sangat rentan terhadap keamanan data maupun informasi yang ada di dalamnya. Banyak kemungkinan yang dapat terjadi seperti data hilang atau rusak, untuk itu keamanan terhadap data dan informasi dalam pengiriman maupun pengolahan data citra satelit menjadi sangat penting. Selain itu, agar data dan informasi terjamin baik dari sisi *confidentiality, integrity, availability dan accountability*.

1.2 Permasalahan

Berdasarkan latar belakang tersebut, terlihat bahwa ternyata kualitas dan keamanan data dan informasi menjadi kebutuhan yang mendesak dalam pengiriman dan pengolahan data citra satelit resolusi tinggi, sehingga diperlukan manajemen risiko untuk mengurangi kemungkinan risiko yang terjadi. Padahal penilain itu diperlukan untuk mengetahui tingkat resiko yang dimiliki pada setiap tahapan pengiriman dan pengolahan data agar dapat dilakukan *risk mitigation* yang tepat terhadap setiap objek atau proses pengiriman dan pengolahan data yang dilakukan. Manajemen risiko untuk keamanan data dan informasi merupakan suatu proses yang dimulai dengan *risk assessment, risk mitigation dan continuous evaluation*. Manajemen risiko biasanya mengadopsi standar yang sudah ada atau mengikuti regulasi yang berlaku. Permasalahannya adalah bagaimana *risk assessment* dalam proses pengiriman dan pengolahan data yang dilakukan oleh Lapan tersebut dilakukan terhadap setiap proses bisnis yang dilakukan.

1.3 Tujuan Penelitian

Tujuan dari penelitian ini adalah mengidentifikasi dan menilai risiko yang ada pada sistem pengiriman dan pengolahan data citra satelit penginderaan jauh di Lapan Pekayon.

2. TINJAUAN LITERATUR

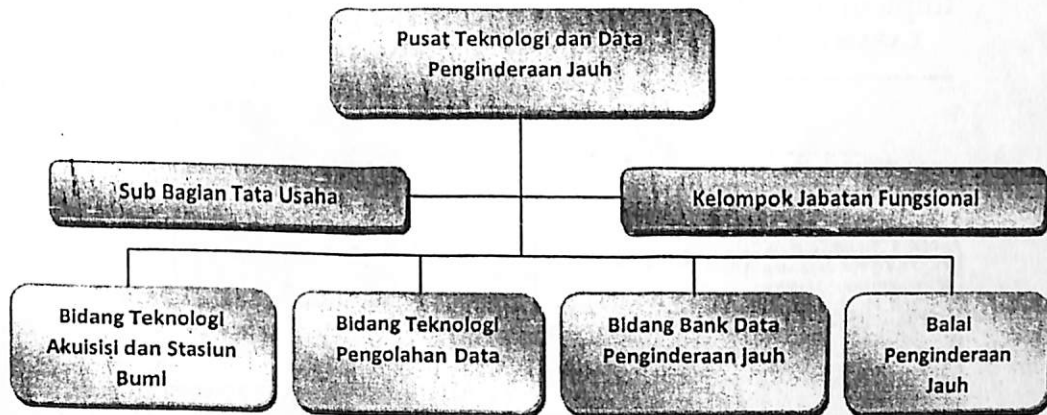
2.1 Risk Assesment

Menurut Whitman (2010)¹¹, *Risk Assesment* adalah proses mengidentifikasi, memprioritasi dan memitigasi risiko. Dalam bukunya tersebut dikemukakan juga bahwa *risk assessment* mencakup orang, proses dan teknologi yang terlibat dalam proses bisnis. Tahapan dalam *risk assessment* meliputi : (1) *Asset Identification*, (2) *Threat and Vulnerability Identification*, (3) *Risk Prioritization*, (4) *Develop Control* and (5) *Monitoring*. Pendekatan Metodologi yang digunakan dalam *risk assessment* adalah pendekatan kualitatif dengan mengestimasi potensi kerugian dan pendekatan kuantitatif dengan pendekatan matematis. Metode yang biasa digunakan adalah NIST-800 yang di rilis oleh NIST dan ISO 27001 yang dirilis oleh ISO¹².

2.2 Tugas Pokok dan Fungsi Pusat Teknologi dan Data Penginderaan Jauh

Berdasarkan Peraturan Kepala Lapan No.2 Tahun 2011 tentang Organisasi dan Tata Kerja Lembaga Penerbangan dan Antariksa Nasional¹³, Pusat Teknologi dan Data Penginderaan Jauh mempunyai tugas melaksanakan penelitian dan pengembangan teknologi sistem akusisi dan stasiun bumi, pengolahan data, serta pengembangan bank data penginderaan jauh. Pusat Teknologi dan Data Penginderaan Jauh menyelenggarakan

fungsi meliputi : (a) penelitian dan pengembangan teknologi sistem akusisi dan stasiun bumi; (b) penelitian dan pengembangan sistem pengolahan data;(c) penelitian dan pengembangan bank data penginderaan jauh; (d) pembinaan teknis di bidang teknologi dan data penginderaan jauh. Struktur organisasinya Pusat Teknologi Data Penginderaan Jauh dapat dilihat pada gambar 2-1.



Gambar 2-1 Struktur Organisasi Pusat Teknologi Data dan Penginderaan Jauh
 Sumber : <http://www.lapanrs.com>

Pusat Teknologi dan Data Penginderaan Jauh bertanggung jawab terhadap pengambilan data citra satelit dan pengolahan datanya sehingga dapat dimanfaatkan oleh masyarakat yang membutuhkan. Banyak manfaat yang bisa diperoleh dari penginderaan jauh yaitu model pemanfaatan lahan darat, model pemanfaatan pesisir dan laut, pengembangan model zona potensi penangkapan ikan, pengembangan metode analisis dampak kenaikan muka air laut terhadap sumber daya wilayah pesisir, deteksi dan analisis sebaran tumpahan minyak di Laut Timor, menggunakan data satelit penginderaan jauh dan model kebencanaan dan cuaca.

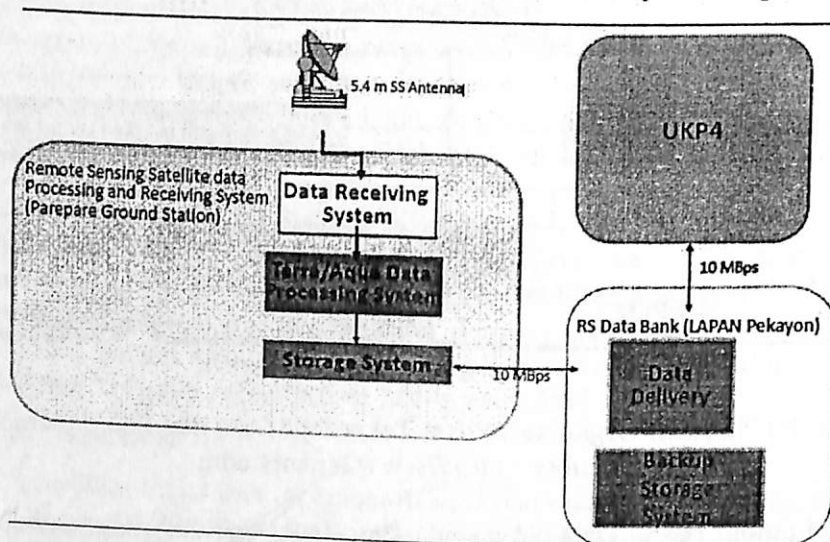
Terkait dengan aktivitas pengolahan data, tentu bisa ditelusuri kerentanan dan celah keamanan yang bisa mengancam kerahasiaan, integritas dan ketersediaan terkait dengan data dan informasi di dalamnya. Dengan kondisi tersebut di atas perlu dilakukan suatu proses yang mengacu kepada mekanisme yang terstruktur dan terstandar dalam rangka mengidentifikasi risiko, celah kerawanan (*vulnerability*) dan langkah-langkah mitigasi yang tepat untuk meminimalisasi dampak terkait dengan keamanan aset-aset informasi.

2.3 Sistem Pengiriman dan Pengolahan Data Citra Satelit

Sistem pengiriman dan pengolahan data citra satelit penginderaan jauh mengacu kepada *Sistem Synthetic Aperture Radar (SAR)*. SAR adalah merupakan salah satu teknik penginderaan jauh sistem aktif yang menggunakan daerah gelombang mikro dari spektrum elektromagnetik antara frekuensi 0.3 GHz sampai 300 GHz (atau bila dinyatakan dengan panjang gelombang, antara 1 m sampai 1 mm)¹⁴. Alur Penerimaan data dan pengolahan data citra satelit dapat dilihat pada Gambar 2-2. Pada gambar tersebut terlihat bahwa data

citra satelit yang diterima melalui stasiun bumi kemudian diterima oleh sistem penerima data, data dilanjutkan pada sistem pemrosesan data Terra/ Aqua yang kemudian dimasukkan dalam sistem *Storage*. Data kemudian dikirim pada bank data yang akan menyimpannya dalam sistem storage atau mengirimkan pada UKP4 serta instansi lain yang membutuhkan.

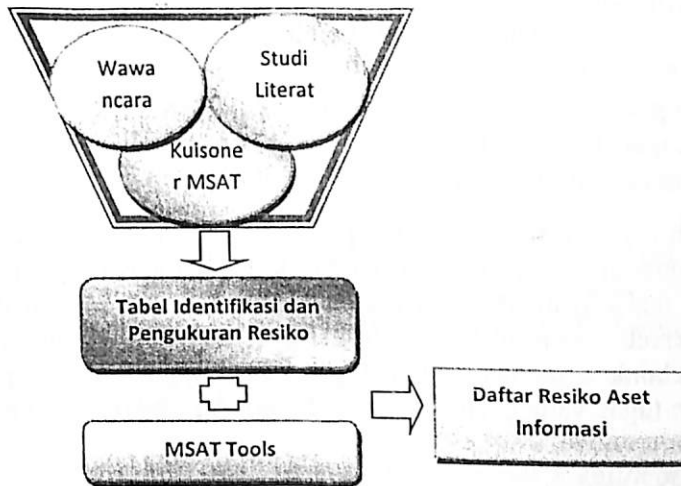
Implementasi Sistem Penerimaan dan Pengolahan Data LAPAN DB Processing System : Communication and system design



Gambar 2-2 Alur Sistem Penerimaan dan Pengolahan Data
(Sumber : Indrajad, Andy)¹⁵

3. METODOLOGI PENELITIAN

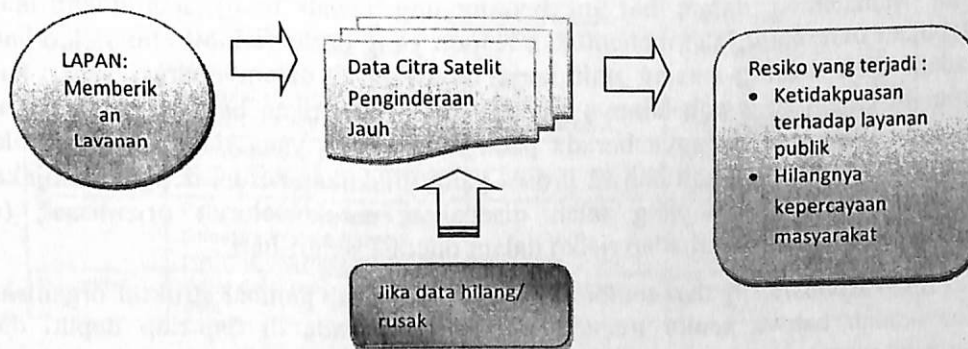
Risk assessment dilakukan dengan menggunakan beberapa metode. Metode pengumpulan data dilakukan dengan wawancara dan kuisioner. Wawancara dilakukan kepada staff dan peneliti di Pusat Teknologi dan Pengolahan Data Penginderaan Jauh. Sedangkan metode analisa yang digunakan adalah *Microsoft Security Assesment Tools (MSAT)*¹⁶. MSAT merupakan sebuah piranti lunak yang dikeluarkan oleh *Microsoft* yang digunakan untuk mengetahui kondisi TI yang ada di lingkungan organisasi saat ini. Data input MSAT didapatkan dengan kuisioner yang mencakup pertanyaan mengenai infrastruktur, aplikasi, operasi, dan sumber daya manusia. Pertanyaan-pertanyaan tersebut merupakan rekomendasi dari standar yang ada seperti ISO 17799 dan NIST – 800x serta bimbingan preskriptif dari *Microsoft Trustworthy Computing Group*. Kerangka *risk assessment* dapat dilihat pada Gambar 3-1.



Gambar 3-1 Kerangka *Risk Assesment*

4. ANALISA DAN PEMBAHASAN

Proses bisnis Lapan yang dijalankan pada Pusat Teknologi Data Penginderaan Jauh yang telah dijelaskan pada sub bab di atas, secara organisasi risiko yang kemungkinan terjadi adalah pelayanan data citra satelit penginderaan jauh kepada masyarakat maupun pelanggan menjadi tidak maksimal. Hal tersebut akan berakibat terhadap tingkat kepercayaan masyarakat terhadap instansi pemerintah menjadi kurang baik. Disamping itu pendapatan Negara bukan pajak yang berasal dari penjualan data citra satelit menjadi berkurang, sehingga *Risk Management in chart* pada proses bisnis tersebut dapat dilihat pada Gambar 4-1.



Gambar 4-1 *Chart Risk Management*

4.1 *Roles and Responsibility*

Struktur Organisasi yang menangani TIK di Pusat Teknologi Data dan Penginderaan Jauh secara kelembagaan belum ada, namun secara fungsional keberadaan

dari pengelola TIK menumpang pada tugas yang lain seperti peneliti yang berada pada tiap-tiap bidang. Sedangkan dalam sebuah manajemen risiko unit pengelola TIK harus berdiri sendiri sebagai sebuah organisasi walaupun secara fungsi bisa beriringan dengan tugas lainnya, sehingga langkah utama dalam manajemen risiko adalah membuat unit pengelola TIK di Lapan secara terpusat dan unit pengelola di masing-masing unit kerja termasuk di Pusat Teknologi data dan Penginderaan Jauh.

Namun dalam organisasi pemerintah, perubahan struktural adalah bukan hal yang fleksibel untuk dilakukan karena banyaknya birokrasi yang perlu di tempuh untuk hal tersebut. Untuk itu maka pengadopsian peran-peran yang dibutuhkan dalam penerapan manajemen risiko tersebut saat ini tidak dilakukan dengan mengubah struktur organisasi yang sudah ada, melainkan menambahkan tugas dan tanggung jawab pada pihak-pihak yang relevan dengan tugas yang perlu diemban. Selain itu diperlukan juga komitmen dari pimpinan untuk penerapannya.

Berdasarkan identifikasi organisasi di Lapan, maka untuk penerapan manajemen risiko ini *roles and responsibility* yang perlu ada adalah sebagai berikut:

1. Komite Risiko

Komite risiko dalam hal ini akan menjalankan fungsinya sebagai penetap kebijakan dan strategi penerapan manajemen risiko untuk seluruh organisasi. Komite akan dikepalai langsung oleh kepala organisasi agar efektif dan akan berisi kepala deputy dan sekretariat utama, juga direktorat. Selain itu komite risiko ini juga akan menjalankan fungsi-fungsi: (a) Identifikasi; evaluasi dan prioritas risiko yang mungkin terjadi terhadap organisasi; (b) Cost benefit dari risiko dan kontrol yang diterapkan; (c) Menjaga efektifitas proses manajemen risiko; (d) Identifikasi implikasi risiko terhadap keputusan pimpinan.

2. Senior Manajemen

Senior Manajemen dalam hal ini bertanggung jawab untuk mengidentifikasi, melakukan *assesment*, dan menentukan respon yang perlu diambil atas risiko yang dihadapi oleh masing-masing unit kerja dibawahnya dalam operasi sehari-hari. Selain itu tanggung jawab lainnya adalah : (a) Memastikan bahwa aktivitas yang dilakukan oleh unit kerjanya berada pada level risiko yang dapat diterima oleh organisasi; (b) Memastikan bahwa proses yang dilakukan sesuai dengan kebijakan atas manajemen risiko yang telah disepakati untuk seluruh organisasi; (c) Promosikan awareness terhadap risiko dalam operasi sehari-hari.

Roles and responsibility dari senior manajemen terhadap gambar struktur organisasi diatas adalah bahwa senior manajemen ini akan ada di tiap-tiap deputy dan sekretariat utama.

3. Risk Management

Risk management dalam hal ini akan dijalankan oleh *single risk champion* mengingat ketersediaan sumber daya yang kurang. Risk manajemen akan ada di biro umum yang akan menjalankan seperti : (a) Membuat kebijakan dan strategi untuk *risk management*; (b) Membangun kultur *risk awareness*; (c) *Review* proses

risk management; (d) Membuat proses respon risiko, termasuk rencana kontingensi dan rencana kontinuitas bisnis; dan (e) Membuat laporan risiko untuk komite.

4. Internal audit

Peran untuk internal audit ini akan berada di Inspektorat. Hal ini tentunya sudah sesuai dengan fungsi dan tugas pokok yang diemban selama ini sebagai internal auditor dari organisasi. Terkait dengan fungsinya dalam manajemen risiko, maka internal audit ini akan bertanggung jawab antara lain : (a) Audit proses *risk management*; (b) Melaporkan kepada komite mengenai hasil identifikasi/*assessment* terhadap kontrol risiko; (c) Secara tidak langsung memberikan jaminan mengenai pengelolaan manajemen risiko.

4.2 Risk Assesment dan Risk Mitigation

Proses *risk assement* diawali dengan melakukan *risk identification* terlebih dahulu. Dalam proses *risk identification* ini kita mencoba mengidentifikasi aset-aset informasi yang dimiliki organisasi dan risiko yang mungkin terjadi pada aset tersebut. Aset-aset tersebut dikelompokkan dalam kategori vital (penting dan berpengaruh langsung pada efektifitas pemeriksaan), *important* (penting namun tidak berpengaruh langsung), dan *secondary* (dapat memberi manfaat tambahan). Tabel 4-1 menunjukkan pengelompokan aset-aset yang dimiliki pada sistem pengiriman dan pengolahan data citra satelit.

Tabel 4-1. *Vulnerability Assessment Matrix*

Kategori Aset	Aset	Highly Probable	Probable	Unlikely
Vital	Data citra satelit (raw data)	Loss of access	Loss of data	
Vital	Software pengolah data	Loss of access	Loss of data Disclosure	
Vital	Data yang telah di olah (citra Satelit)	Loss of access	Loss of data	
Important	Server	Loss of access	Loss of data	Bencana
Important	SDM pengolah data (SDM bidang akuisisi data dan pengolahan data)		Resign, sakit	Bencana
Important	System storage 24 TB	Loss of access	Kehilangan data	Bencana
Important	Username dan password		hacker	
Secondary	Backup Storage system 24TB	Loss of access	Kehilangan data	Bencana
Secondary	Proses pengiriman data pada pelanggan / data delivery (website dan manual)		Loss of data Hacker	
Secondary	Arsip data hasil pengolahan data	Loss of access	Loss of data	

Dari masing-masing aset informasi tersebut selanjutnya hanya akan dilakukan analisis lebih lanjut untuk aset informasi yang vital bagi organisasi. Proses selanjutnya adalah mengasosiasikan antara kelemahan yang ada pada sistem saat ini (*vulnerabilities*), ancaman yang mungkin terjadi (*threat*), pihak yang dapat melakukan ancaman tersebut (*threat agent*), dan tindakan yang dilakukan oleh *threat agent* dalam rangka memanfaatkan *vulnerabilities* yang ada (*threat action*).

Tabel 4-2 *Vulnerability Identification*

Aset	Threat	Management	Threat Agent	Threat Action	Vulnerability		
					People	Process	Technology
Data citra satelit (raw data)	Loss of access		Virus	Komputer dimana data citra satelit (raw data) dalam bentuk softcopy disimpan terkena virus sehingga tidak bisa digunakan			Penggunaan komputer pribadi dalam menyimpan data citra satelit (raw data) dengan keamanan yang tidak memadai seperti anti virus dan akses internet pribadi dapat menyebabkan virus dengan mudah masuk
	Loss of data		Operator penyimpanan (raw data)	Operator melakukan kelalaian dalam menyimpan (raw data)	Kebiasaan meniggalkan data, informasi, perangkat di sembarang tempat sedangkan kendali atas akses masuk masih kurang		
software pengolahan data	Lost of access	Tidak adanya panduan yang jelas apa yang harus dilakukan	Virus	Komputer untuk melakukan pengolahan raw data terkena virus sehingga tidak bisa di gunakan			Penggunaan komputer pribadi dengan keamanan yang tidak memadai seperti anti virus dan akses internet pribadi dapat menyebabkan virus dengan mudah masuk
	Loss of data		Sdm pengolahan data	Sdm pengolahan data melakukan kelalaian dengan menghilangkan software pengolahan data	Kebiasaan meniggalkan data, informasi, perangkat di sembarang tempat sedangkan kendali atas akses masuk masih kurang		
Data yang telah di olah (citra Satelit)	Loss of access	Hilangnya data dapat menimbulkan potensi kerugian	Virus	Komputer dimana data citra satelit dalam bentuk softcopy disimpan terkena virus sehingga tidak bisa digunakan			Penggunaan komputer pribadi dalam menyimpan data citra satelit dengan keamanan yang tidak memadai seperti anti virus dan akses internet pribadi dapat menyebabkan virus dengan mudah masuk
	Loss of data		Sdm pengolah data	Sdm melakukan kelailaian dalam penyimpanan data citra satelit	Kebiasaan meniggalkan data, informasi, perangkat di sembarang tempat sedangkan kendali atas akses masuk masih kurang		

Tabel 4-3 Risk Assessment Risiko Inheren

Aset	Penanggung Jawab	Risiko	Kerawanan terhadap Aset (<i>vulnerabilities</i>)	Ancaman	Inheren			Kontrol yang ada
					Dampak	Probabilitas	Nilai risiko	
Data citra satelit (raw data)	Balai penginderaan jauh (parepare)	Kerahasiaan Ketersediaan Integritas Kelengkapan data	<ul style="list-style-type: none"> - Data rusak - Data tidak lengkap - Data hilang/ di curi 	<ul style="list-style-type: none"> - Data yang didapat dari satelit (raw data) rusak dikarenakan virus - Terjadi kehilangan data ketika disimpan kedalam komputer - Terjadi gangguan pengiriman raw data dari satelit 	Tinggi	Sedang	Tinggi	<ul style="list-style-type: none"> - Penunjukan personel untuk pengambilan data - Akses menggunakan password - Data disimpan dalam sebuah storage system - Pengamanan secara fisik
software pengolah data	bidang akuisisi data bidang pengolahan data	Ketersediaan Integritas	<ul style="list-style-type: none"> - Software tidak terupdate - Diakses oleh orang yang tidak berwenang - Software rusak - Software hilang 	<ul style="list-style-type: none"> - software pengolah hilang karena teruninstall oleh pengguna - Software Rusak karena terkena virus - Komputer yang terinstall software pengolah diakses oleh orang yang tidak berhak - adanya celah keamanan di software yang dapat dimanfaatkan oleh hacker 	Tinggi	Sedang	Tinggi	<ul style="list-style-type: none"> - Penggunaan password untuk akses - Penunjukan personel dalam pengolahan data dan akses pada aplikasi
Data yang telah di olah (citra Satelit)	Bidang pengolahan data	Kerahasiaan Integritas Ketersediaan	<ul style="list-style-type: none"> - Data hilang/ di curi - Data rusak 	<ul style="list-style-type: none"> - Data yang sudah diolah rusak dikarenakan virus - Terjadi kehilangan data ketika disimpan kedalam komputer 	Tinggi	Sedang	Tinggi	<ul style="list-style-type: none"> - Akses menggunakan password - Data disimpan dalam sebuah storage system - Pengamanan secara fisik - Penunjukan personel untuk pengambilan data

Tabel 4-3 Risk Assessment Risiko Inheren

Aset	Penanggung Jawab	Risiko	Kerawanan terhadap Aset (<i>vulnerabilities</i>)	Ancaman	Inheren			Kontrol yang ada
					Dampak	Probabilitas	Nilai risiko	
Data citra satelit (raw data)	Balai penginderaan jauh (parepare)	Kerahasiaan Ketersediaan Integritas Kelengkapan data	<ul style="list-style-type: none"> - Data rusak - Data tidak lengkap - Data hilang/ di curi 	<ul style="list-style-type: none"> - Data yang didapat dari satelit (raw data) rusak dikarenakan virus - Terjadi kehilangan data ketika disimpan kedalam komputer - Terjadi gangguan pengiriman raw data dari satelit 	Tinggi	Sedang	Tinggi	<ul style="list-style-type: none"> - Penunjukan personel untuk pengambilan data - Akses menggunakan password - Data disimpan dalam sebuah storage system - Pengamanan secara fisik
software pengolah data	bidang akuisisi data bidang pengolahan data	Ketersediaan Integritas	<ul style="list-style-type: none"> - Software tidak terupdate - Diakses oleh orang yang tidak berwenang - Software rusak - Software hilang 	<ul style="list-style-type: none"> - software pengolah hilang karena teruninstall oleh pengguna - Software Rusak karena terkena virus - Komputer yang terinstall software pengolah diakses oleh orang yang tidak berhak - adanya celah keamanan di software yang dapat dimanfaatkan oleh hacker 	Tinggi	Sedang	Tinggi	<ul style="list-style-type: none"> - Penggunaan password untuk akses - Penunjukan personel dalam pengolahan data dan akses pada aplikasi
Data yang telah di olah (citra Satelit)	Bidang pengolahan data	Kerahasiaan Integritas Ketersediaan	<ul style="list-style-type: none"> - Data hilang/ di curi - Data rusak 	<ul style="list-style-type: none"> - Data yang sudah diolah rusak dikarenakan virus - Terjadi kehilangan data ketika disimpan kedalam komputer 	Tinggi	Sedang	Tinggi	<ul style="list-style-type: none"> - Akses menggunakan password - Data disimpan dalam sebuah storage system - Pengamanan secara fisik - Penunjukan personel untuk pengambilan data

Tabel 4-4 Risk Assessment Risiko Residual

Aset	Residual			Strategi mitigasi	Rencana kerja	Target penyelesaian	PIC
	Dampak	Probabilitas	Nilai risiko				
Data citra satelit (raw data)	Sedang	Jarang	Sedang	Kendalikan Risiko-Accept	Implementasi SOP penerimaan data satelit (raw data) dan penyimpanannya	Tahun berikutnya	
software pengolahan data	Rendah	Jarang	Rendah	Kendalikan Risiko-Accept	Selalu melakukan update software untuk menutup celah keamanan	Segera	
Data yang telah diolah (citra Satelit)	Rendah	Jarang	Rendah	Kendalikan Risiko-Accept	Implementasi SOP untuk management data citra satelit	Tahun berikutnya	

4.3 Specific Trends (Current)

Berdasarkan dampak yang mungkin dirasakan oleh Lapan dan kecenderungan *threat agent* dapat memanfaatkan *vulnerabilities* yang ada, dilakukan penilaian atas level risiko yang ada. Penilaian atas dampak dilakukan dengan pengumpulan data yang dilakukan dengan metode wawancara dan kuisioner. Kuisioner dibutuhkan untuk menjawab 200 (dua ratus) pertanyaan *audit* MSAT. Hasil Audit Lapan dengan MSAT menunjukkan beberapa kondisi kritis pada *operations* dan *infrastructure*. Hasil Analisa MSAT dapat dilihat pada Gambar 4-5.

Results:

Areas of Analysis	Risk-Defense Distribution	Security Maturity
People		
Operations	●	●
Applications	●	
Infrastructure	●	●

Gambar 4-2 Hasil Risk Assesment dengan MSAT

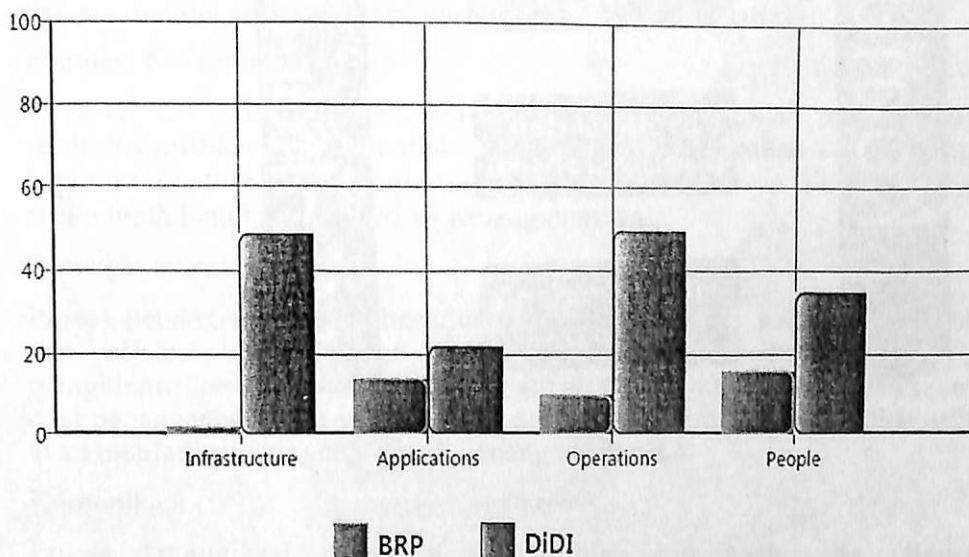
Pada hasil yang lebih rinci (terlampir) terlihat beberapa risiko yang harus segera diatasi yaitu : *Remote Access*, keamanan secara fisik, *security requirement*, *remote access users* dan perjanjian dengan pihak ketiga.

High Priority	Medium Priority	Low Priority
<ul style="list-style-type: none"> • Remote Access • Physical Security • Security Requirements • Remote-Access Users • Third-party independent software vendor (ISV) 	<ul style="list-style-type: none"> • Patch Management • Segmentation • Security Awareness • Third-Party Relationships • Logging 	<ul style="list-style-type: none"> • Management Host - Servers • Protocols & Services • Acceptable Use • Backup • Anti-virus - Desktops

Gambar 4-3 Saran Inisiatif Kendali MSAT

Adanya risiko besar pada *operations* dan *infrastructure* dimungkinkan karena hasil kuisioner MSAT menunjukkan *operation* memiliki *Business Risk Profile* 10 dan ini merupakan hal yang tidak mungkin. Selanjutnya pada *infrastructure* teridentifikasi celah yang besar antara *Business Risk Profile* dengan *Defense Index Dept Index (DiDI)*. Celah besar BRP dan DiDI ini menunjukkan terlalu besar kendali yang diterapkan untuk risiko yang cukup kecil.

Risk-Defense Distribution

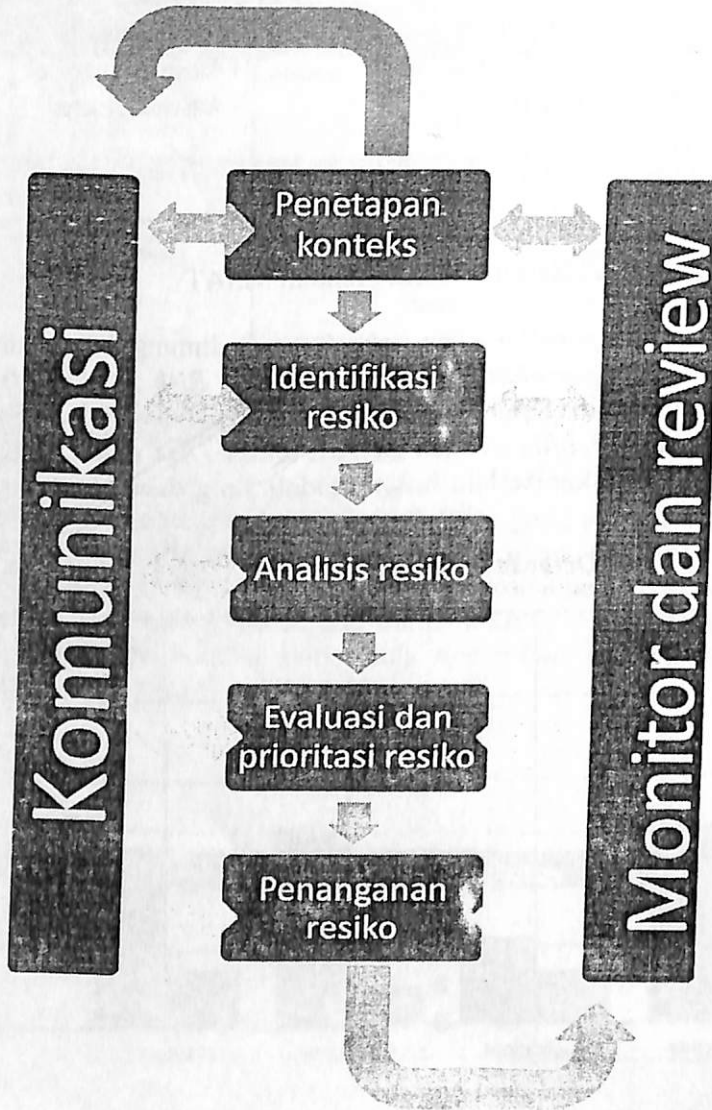


Gambar 4-4 Risk Defense Distribution dengan MSAT

4.4 Proses Risk Management

Proses *risk management* belum diterapkan di Lapan, termasuk pada sistem pengiriman dan pengolahan data citra satelit penginderaan jauh. Namun demikian terdapat sejumlah kendali yang telah diterapkan untuk mengurangi sejumlah risiko dalam proses

operasinya. Bentuk kendali yang dilakukan tersebut umumnya baru sebatas kendali yang sudah umum, baik dari sisi teknologi, proses dan sumber daya manusia. Untuk itu diusulkan adanya proses *risk management* terstruktur yang dapat diterapkan di Lapan. Adapun proses *risk management* yang kami usulkan adalah sebagai berikut:



Gambar 4-5 Proses *Risk Management*

Proses *Risk Management* pada Gambar 4-5 meliputi :

1. Penetapan konteks

Penetapan konteks bertujuan untuk mengidentifikasi dan menganalisis Lapan sebagai lingkungan tempat manajemen risiko akan diterapkan. Dalam proses ini diidentifikasi pihak-pihak yang paling berkepentingan dengan proses penerapan manajemen risiko, ruang lingkup dan tujuan proses, kondisi yang membatasi, serta hasil yang diharapkan dari penerapan manajemen risiko. Aspek definisinya antara lain: sasaran manajemen risiko, komposisi fungsi manajemen risiko, stakeholder, regulasi, kriteria risiko.

2. Identifikasi risiko

Identifikasi risiko bertujuan untuk mengidentifikasi seluruh jenis risiko yang berpotensi mengganggu operasi sehari-hari terutama pada sistem pengiriman dan pengolahan data citra satelit penginderaan jauh. Proses ini dilakukan dengan cara mengidentifikasi proses terjadinya peristiwa (*what*), lokasi (*where*), waktu (*when*) dan sebab (*how*) risiko yang dapat terjadi.

3. Analisis risiko

Analisis risiko bertujuan untuk mengetahui profil dari risiko-risiko yang ada dan akan digunakan dalam proses evaluasi risiko. Proses analisis risiko dilakukan dengan melihat sumber risiko dan tingkat pengendalian yang ada serta dilanjutkan dengan menilai risiko dari sisi dampak dan kecendrungan terjadinya.

4. Evaluasi dan prioritas risiko

Evaluasi dan prioritas risiko bertujuan untuk menetapkan prioritas risiko yang telah diidentifikasi dan dianalisis. Evaluasi risiko dilakukan agar para pengambil keputusan/komite bisa mempertimbangkan perlu tidaknya dilakukan penanganan risiko lebih lanjut serta prioritas penanganannya.

5. Penanganan risiko

Proses penanganan risiko bertujuan menentukan jenis penanganan yang efektif dan efisien untuk suatu risiko. Penanganan risiko dilakukan dengan mengidentifikasi berbagai opsi penanganan risiko yang tersedia dan memutuskan opsi penanganan risiko yang terbaik dalam proses ini juga ditentukan pihak yang akan menjadi penanggung jawab penanganan risiko.

6. Komunikasi

Proses komunikasi bertujuan memperoleh informasi yang relevan serta mengkomunikasikan setiap tahapan proses Manajemen Risiko sehingga pihak-pihak yang terkait dapat menjalankan tanggungjawabnya dengan baik. Adapun faktor-faktor agar komunikasi ini dapat berjalan dengan baik diantaranya: kualitas informasi, arah komunikasi dan media komunikasi.

7. Monitor dan evaluasi

Monitoring bertujuan untuk melakukan pemantauan atas penerapan manajemen risiko pada seluruh organisasi. Proses monitoring bisa dilakukan secara terus menerus maupun terpisah dengan cara memantau efektivitas rencana penanganan risiko, strategi, dan sistem manajemen risiko.

5. PENUTUP

Sistem pengiriman dan pengolahan data penginderaan jauh merupakan proses bisnis yang dilakukan oleh Lapan sebagai lembaga kedirgantaraan. Dalam proses tersebut sangat rentan terhadap risiko data yang hilang maupun rusak sehingga perlu dilakukan *risk assessment* terhadap asset-aset yang terkait dengan sistem.

Hasil *risk assessment* menunjukkan bahwa : (1) asset vital dalam sistem pengiriman dan pengolahan data citra satelit adalah data citra satelit (raw data), software pengolah data, dan data yang telah diolah; (2) berdasarkan analisa MSAT, kondisi resiko terbesar dari 4 aspek yaitu *people, operations, application* dan *infrastructure* terdapat pada *operations* dan *infrastructures*. Sehingga rekomendasi yang diberikan terkait dengan dua hal tersebut pada: *Remote Access*, keamanan secara fisik, *security requirement, remote access users* dan perjanjian dengan pihak ketiga.

DAFTAR RUJUKAN

- ¹ LAPAN. 2011. *Peraturan Kepala LAPAN No.2 Tahun 2011 tentang Organisasi dan Tata Kerja Lembaga Penerbangan dan Antariksa Nasional*. Jakarta.
- ² Ibid, pasal 61.
- ³ Ibid, pasal 62
- ⁴ Lapan. 2013. *Sasaran Kegiatan Lembaga Penerbangan dan Antariksa Nasional Tahun 2013*. Jakarta. hal 3
- ⁵ Ibid, hal 5
- ⁶ Ibid, hal 5
- ⁷ Instruksi Presiden No.6 Tahun 2012 tentang *Penyediaan, Penggunaan, Pengendalian Kualitas, Pengolahan, dan Distribusi Data Satelit Penginderaan Jauh Resolusi Tinggi*, Jakarta.
- ⁸ Ibid, hal 5
- ⁹ LAPAN. 2011. Loc Cit
- ¹⁰ Lapan. 2013. Op Cit.hal 13
- ¹¹ Whitman, M. E., & Mattord, H. J. (2010). *Principles of information security*. Cengage Learning
- ¹² Jones, A., & Ashenden, D. (2005). *Risk management for computer security: Protecting your network & information assets*. Butterworth-Heinemann.
- ¹³ LAPAN. (2011). *Peraturan Kepala LAPAN No.2 Tahun 2011 tentang Organisasi dan Tata Kerja Lembaga Penerbangan dan Antariksa Nasional*. Jakarta.
- ¹⁴ Indrajad, Andi. 2012. *Desain Sistem Otomatisasi Pengolahan Data Modis*. Jakarta.
- ¹⁵ Ibid
- ¹⁶ MSAT sumber <http://www.microsoft.com/en-us/download/details.aspx?id=12273>