Penerapan Standar Keamanan Informasi Menggunakan Framework ISO/IEC 27005:2011 di Lapan Bandung

http://dx.doi.org/10.28932/jutisi.v4i1.770

Radiant Victor Imbar[1] , Asa Ednatry Ayala[2]

Jurusan S1 Sistem Informasi Universitas Kristen Maranatha
Jl. Prof. Drg. Suria Sumantri no. 65 Bandung
[1]radiant.vi@it.maranatha.edu
[2]asaednatryayala@gmail.com

Abstract— **Information Security standard help to ensure security consistency across the business and usually contain security controls relating to the implementation of specific technology, hardware or software. It is important that a company understands standards so the company can choose the standard that are the most relevant to their organization. ISO 27000 is the international standard for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within an organization. ISO/IEC 27005:2011 provides guidelines for information security risk management. It supports the general concepts specified in ISO/IEC 27001 and is designed to assist the satisfactory implementation of information security based on a risk management approach. Risk Management is one of the cornerstones of a mature and functional information security program that provides business value to an organization. The object of this research in LAPAN Bandung is to conduct risk assessment and analysis infrastructure LAPAN RDSA in Bandung. This study uses qualitative and semi-quantitative analysis with the case study method. This risk analysis using the approach of the standard ISO / IEC 27005: 2011.**

Keywords— **Risk Management, ISO/IEC 27005:2011, Information Security.**

I. PENDAHULUAN

A. Latar Belakang

Lembaga Penerbangan dan Antariksa Nasional(LAPAN) adalah Lembaga Pemerintahan Non Kementrian Indonesia yang melaksanakan tugas pemerintahan di bidang penelitian dan pengembangan kedirgantaraan dan pemanfaatannya.

Pengelolaan informasi di LAPAN sudah terkomputerisasi. Implementasi infrastruktur teknologi informasi memiliki risiko yang dapat mengganggu kinerja organisasi maupun operasional. Risiko ini disebabkan oleh manusia atau sistem itu sendiri. Karena itu, organisasi dituntut untuk memiliki manajemen risiko, dimana manajemen risiko merupakan suatu pengelolaan yang melihat potensi-potensi atau hal-hal apa saja yang harus dilakukan agar dapat meminimalkan risiko sekecil mungkin yang dapat terjadi sewaktu-waktu pada organisasi.

Penelitian ini menggunakan *framework* ISO/IEC 27005:2011 sebagai metode penelitian risikonya. Penelitian ini hanya mencakup proses manajemen risiko yang dilakukan pada klausul *context establishment* (klausul 7), *risk assessment* (klausul 8), berupa *risk identification* (klausul 8.1), *risk estimation* (klausul 8.2), *risk evaluation* (klausul 8.3).

B. Ruang Lingkup

Berikut ini adalah ruang lingkup kajian dalam pembuatan penelitian ini:

1. Penelitian dilakukan pada divisi IT LAPAN Bandung.
2. Penilaian risiko teknologi informasi ini terkait aset teknologi informasi untuk infrastruktur RDSA di LAPAN bandung.
3. Pembahasan akan mengacu pada penggunaan ISO 27005:2011.

II. KAJIAN TEORI

Sistem informasi adalah kombinasi antar prosedur kerja, informasi, orang, dan teknologi informasi yang diorganisasikan untuk mencapai tujuan dalam sebuah organisasi [1].

Ada beberapa konsep manajemen resiko yaitu manajemen risiko merupakan proses terstruktur dan sistematis dalam mengidentifikasi, mengukur, memetakan, mengembangkan alternatif penanganan risiko, dan memonitor dan mengendalikan penanganan risiko [2]

Manajemen risiko adalah perbuatan (praktik) dengan manajemen risiko, menggunakan metode dan peralatan untuk mengelola risiko sebuah proyek [3]

Manajemen risiko adalah suatu bidang ilmu yang membahas tentang bagaimana suatu organisasi menerapkan

ukuran dalam memetakan berbagai permasalahan yang ada dengan menempatkan berbagai pendekatan manajemen secara komprehensif dan sistematis [4]

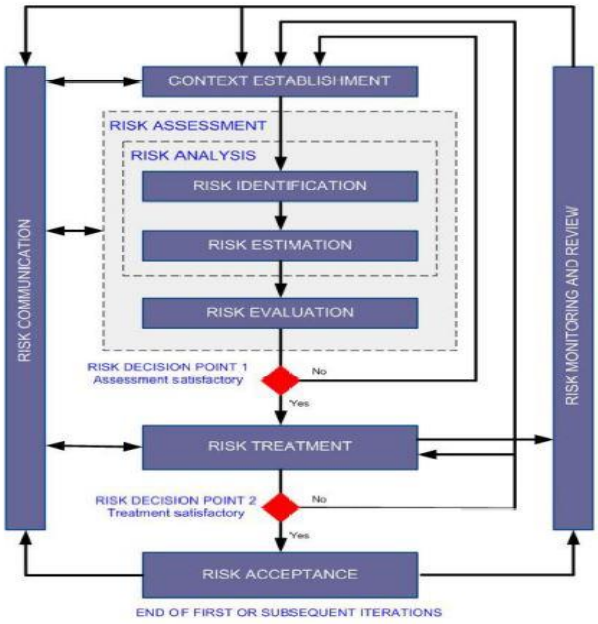
Risiko adalah ketidakpastian (*uncertainty)* yang mungkin melahirkan peristiwa kerugian [5].

Keamanan informasi adalah untuk melindungi kerahasiaan, integritas, dan ketersediaan aset informasi baik dalam penyimpanan, pengolahan, atau transmisi. Hal ini dicapai melalui penerapan kebijakan, pendidikan, pelatihan dan kesadaran, dan teknologi [6].

ISO/IEC 27005 berfokus kepada analisis risiko,untuk selanjutnya tahapan menuju pemilihan kontrol keamanan. ISO/IEC 27001 dan ISO/IEC 27002 lebih eksplisit kepada perencanaan, pelaksanaan dan operasi terhadap kontrol keamanan. Kebijakan perusahaan mengenai keamanan informasi memberikan arahan untuk manajemen keamanan informasi[13].

Manajemen risiko mengacu pada budaya, proses, dan struktur yang diarahkan pada pengelolaan ketidakpastian [7] Proses pada manajemen risiko terjadi secara sistematis, terus menerus, dan diterapkan dalam segala aspek [8]

Proses manajemen risiko keamanan informasi pada gambar 1 terdiri dari *context establishment, risk assessment, risk treatment, risk acceptance, risk communication, risk monitoring and review.*



Gambar 1. Proses Manajemen Risiko [9]

A. *Context Establishment*

Konteks manajemen risiko keamanan informasi harus ditetapkan yang melibatkan sebagai berikut [9]:

1. Pertimbangan Umum

   Untuk menentukan tujuan dari manajemen risiko keamanan informasi karena ini akan mempengaruhi keseluruhan proses dan pembentukan konteks tertentu, tujuan ini dapat berupa mendukung SMKI, kepatuhan hokum dan bukti *due diligence* (uji tuntas), penyusunan rencana respon insiden, persiapan rencana respon insiden, deskripsi tentang persyaratan keamanan informasi untuk suatu produk, layanan atau mekanisme.

2. Kriteria Dasar

   Sebuah pendekatan manajemen risiko yang tepat harus dipilih atau dikembangkan yang membahas kriteria dasar seperti: kriteria evaluasi risiko, kriteria dampak, kriteria penerimaan risiko.

3. Ruang Lingkup dan Batasan

   Ketika mendefinisikan ruang lingkup dan batas-batas, organisasi harus mempertimbangkan informasi seperti tujuan, strategi, proses bisnis, dan lain-lain.

4. Organisasi Manajemen Risiko Keamanan Informasi

   Organisasi dan tanggung jawab untuk proses manajemen risiko keamanan informasi harus dibentuk dan dipelihara

B. *Identifikasi dan Penilaian Ancaman, Kerentanan, dan Existing Control*

Menurut ISO/IEC 27005:2011, ancaman memiliki potensi untuk membahayakan aset seperti informasi, proses, sistem, dan organisasi. Ancaman mungkin berasal dari alam atau manusia, dan bisa tidak sengaja atau disengaja. Sumber ancaman, baik tidak disengaja maupun disengaja harus diidentifikasi. Ancaman mungkin timbul dari dalam atau dari luar organisasi. Ancaman harus diidentifikasi secara umum dan menurut jenisnya (misalnya tindakan yang tidak sah, kerusakan fisik, kegagalan teknis) serta ancaman individu.

Selanjutnya, sebuah kerentanan dari sebuah ancaman dipengaruhi oleh kontrol yang dilaksanakan. Perlu dicatat bahwa penerapan kontrol yang tidak tepat atau tidak berfungsinya pengendalian atau pengendalian tersebut digunakan secara tidak benar bisa menjadi kerentanan. Kontrol bisa saja efektif atau tidak efektif tergantung pada lingkungan di mana kontrol tersebut beroperasi. Sebaliknya, ancaman yang tidak memiliki kerentanan yang sesuai mungkin tidak menimbulkan risiko [10].

C. *Analisis Risiko Keamanan Informasi*

1. Penilaian Risiko

   Proses penilaian risiko keamanan informasi secara terperinci melibatkan identifikasi dan penilaian mendalam pada aset, penilaian ancaman terhadap aset tersebut dan penilaian kerentanan. Hasil dari penilaian ini kemudian digunakan untuk menilai risiko dan kemudian mengidentifikasi penanganan risiko [7]

   Nilai aset, tingkat ancaman, dan kerentanan untuk setiap jenis konsekuensi dicocokkan dalam matriks seperti yang ditunjukkan dibawah ini, untuk mengidentifikasi setiap kombinasi ukuran risiko yang relevan pada skala 0

sampai 8. Nilai-nilai ditempatkan dalam matriks dengan cara terstruktur. Adapun baris yang sesuai dalam matriks diidentifikasi oleh nilai aset, dan kolom yang sudah diidentifikasi oleh kemungkinan terjadinya ancaman dan kemudahan eksploitasi. Ukuran matriks, dalam hal jumlah kategori kemungkinan ancaman, kategori kemudahan eksploitasi, dan jumlah kategori penilaian aset, bisa disesuaikan dengan kebutuhan organisasi. Tabel I merupakan tabel matriks yang digunakan untuk menentukan *level* risiko dari nilai aset, kemungkinan terjadi ancaman, dan kemudahan eksploitasi:

TABEL I.

MATRIKS *LEVEL* RISIKO

	Kemungkinan terjadi ancaman	***Low* (L)**			***Medium* (M)**			***High* (H)**		
	Kemudahan Eksploitasi	**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
Nilai Aset	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Berdasarkan Tabel I dapat dilihat bahwa matriks ISO/IEC 27005:2011 yang digunakan untuk menentukan *level* atau tingkat risiko dari masing-masing kelompok aset infrastruktur RDSA. Adapun kriteria skala yang digunakan dari setiap *level* risiko diatas, dikelompokkan menjadi tiga kategori *level* risiko, yaitu:

1. 0-2 termasuk kedalam kategori *low risk* (risiko rendah) yang berarti tidak menimbulkan kerugian besar bagi perusahaan.
2. 3-5 termasuk kedalam kategori *medium risk* (risiko sedang) yang berarti menimbulkan kerugian bagi perusahaan.
3. 6-8 termasuk kedalam kategori *high risk* (risiko tinggi) yang berarti menimbulkan kerugian besar bagi perusahaan.

Hasil dari pertimbangan kemungkinan skenario insiden, dipetakan terhadap dampak bisnis yang diperkirakan. Risiko yang timbul diukur pada skala 0 sampai 8 yang dapat dievaluasi terhadap kriteria penerimaan risiko. Skala risiko ini juga bisa dipetakan ke peringkat risiko keseluruhan yang sederhana, misalnya seperti : risiko rendah (0-2), risiko sedang (3-5), dan risiko tinggi (6-8). Matriks ini akan digunakan untuk membantu dalam proses analisis risiko untuk menentukan tingkat suatu risiko suatu ancaman di perusahaan.

2. Evaluasi Risiko

Evaluasi risiko dari sebuah daftar risiko dengan tingkat dan nilai yang diberikan yaitu dengan melakukan perbandingan tingkat risiko dan kriteria penerimaan risiko [10]. Melakukan evaluasi risiko, organisasi harus membandingkan estimasi risiko menggunakan matriks dengan kriteria evaluasi risiko yang ditentukan selama penetapan konteks Identifikasi dan Penilaian Ancaman, Kerentanan, dan *Existing Control*[12].

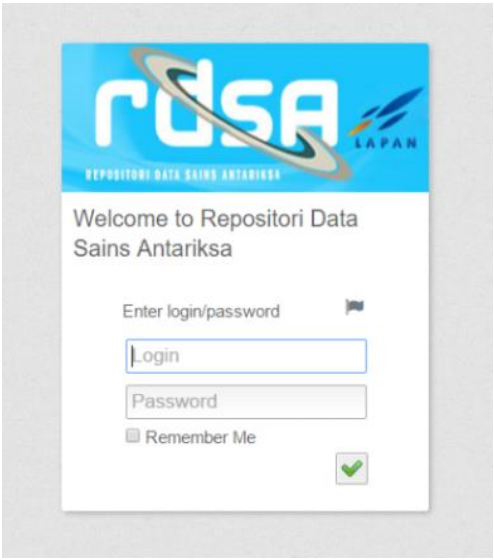
Menurut ISO/IEC 27005:2011, ancaman memiliki potensi untuk membahayakan aset seperti informasi, proses, sistem, dan organisasi. Ancaman mungkin berasal dari alam atau manusia, dan bisa tidak sengaja atau disengaja. Sumber ancaman, baik tidak disengaja maupun disengaja harus diidentifikasi. Ancaman mungkin timbul dari dalam atau dari luar organisasi. Ancaman harus diidentifikasi secara umum dan menurut jenisnya (misalnya tindakan yang tidak sah, kerusakan fisik, kegagalan teknis) serta ancaman individu[13].

Selanjutnya, sebuah kerentanan dari sebuah ancaman dipengaruhi oleh kontrol yang dilaksanakan. Perlu dicatat bahwa penerapan kontrol yang tidak tepat atau tidak berfungsinya pengendalian atau pengendalian tersebut digunakan secara tidak benar bisa menjadi kerentanan. Kontrol bisa saja efektif atau tidak efektif tergantung pada lingkungan di mana kontrol tersebut beroperasi. Sebaliknya, ancaman yang tidak memiliki kerentanan yang sesuai mungkin tidak menimbulkan risiko.

III. ANALISIS DAN EVALUASI

A. *Website RDSA*

RDSA (Repositori Data Sains Antariksa) adalah *website* internal LAPAN yang berfungsi sebagai media/wadah peneliti LAPAN dalam mendapatkan data hasil pengamatan yang berasal dari peralatan di setiap balai/stasiun secara *near realtime.* Gambar 2 adalah tampilan login *website* RDSA:



Gambar 2. Halaman Login

B. Identifikasi Aset Infrastruktur RDSA

Hasil wawancara dan *form checklist* dengan narasumber didapatkan hasil berupa daftar aset infrastruktur RDSA yang ada di LAPAN Bandung. Tabel II adalah daftar aset infrastruktur RDSA.

TABEL II

DAFTAR ASET INFRASTRUKTUR RDSA

Kategori Aset	**No.**	**Nama Aset**	***Asset Valuation* (0-4)**
Hardware	1.	*Server*	4 (*Very high)*
	2.	*Storage Enclosure*	4 (*Very high)*
	3.	PC (*Personal Computer*)	0 (*Very low)*
Kategori Aset	**No.**	**Nama Aset**	***Asset Valuation* (0-4)**
Hardware	4.	Alat Penelitian	4 (*Very high*)
Software	5.	*Website* RDSA	3 (*High*)
	6.	Linux	3 (*High*)
	7.	*Rsync*	2 (*Medium)*
	8.	FTP *Server*	2 (*Medium)*
	9.	FTP *Client*	2 (*Medium)*
	10.	*Open* SSH	2 (*Medium)*
	11.	*Windows*	2 (*Medium)*
Jaringan	12.	*Router*	3 (*High)*
	13.	*Switch*	3 *(High)*
	14.	Kabel UTP	4 (*Very high)*
	15.	*Access Point*	4 (*Very high)*
	16.	*Vsat*	4 (*Very high)*
Informasi/Data	17.	Data hasil penelitian (*raw data)*	4 (*Very high)*
Supporting Facilities	18.	Gedung	3 (*High)*
	19.	CCTV	0 (*Very low)*
	20.	AC	0 (*Very low)*
Human Resources	21.	*Staff* jaringan dan *transfer data*	3 (*High)*

Berdasarkan identifikasi aset infrastruktur RDSA yang ditunjukkan pada tabel II maka dapat dilihat ada 21 daftar aset infrastruktur RDSA yang dilakukan penilaian aset berdasarkan tingkat kritikalitasnya didalam mendukung layanan RDSA.

C. Identifikasi Ancaman, Kerentanan, dan Existing Control

Hasil wawancara dan *form checklist* dengan narasumber menunjukkan jenis-jenis potensi ancaman terhadap setiap aset infrastruktur RDSA dan tingkatannya, kerentanan, atau kemudahan eksploitasi dan tingkatannya serta *existing control* yang sudah diimplementasikan akan disajikan pada tabel III dan tabel IV sebagai berikut:

TABEL III

DAFTAR ASET, JENIS ANCAMAN, DAN TINGKATANNYA

No.	**Nama Aset**	**Jenis Ancaman**	***Level* Ancaman (L), (M), (H)**
1.	*Server*	a.Petir	(M)
		b.Debu/kotoran	(L)
		c.Human error	(L)
		d.Kurangnya SDM	(M)
		e.Pembagian tugas tidak jelas	(M)
		f.Tidak dijalankannya tata kelola	(L)
		g.Kegagalan/kerusakan *hardware*	(M)
		h.Server down	(M)
		i.Koneksi jaringan terputus	(H)
		j.Backup failure	(L)
		k.Kurang baiknya kualitas jaringan	(H)
		l.Hilangnya pasokan listrik	(H)
2.	*Website* RDSA	a.Hilangnya data	(L)
		b.Kurangnya SDM	(L)
		c.Pembagian tugas tidak jelas	(L)
		d.Tidak dijalankannya tata kelola	(L)
		e.Server down	(M)
		f.Koneksi jaringan terputus	(M)
		g.Sistem *crash*	(M)
		h.Overcapacity	(L)
		i.Overload	(L)
		j.Backup failure	(L)

		k.Kurang baiknya kualitas jaringan	(M)
3.	*Router*	a.Petir	(L)
		b.Pencurian perangkat	(L)
		c.Kurangnya SDM	(L)
		d.Pembagian tugas tidak jelas	(L)
		e.Tidak dijalankannya tata kelola	(L)
		f.Overheat	(L)
		g.Koneksi jaringan terputus	(H)
		h.Sistem *crash*	(M)
		i.Kurang baiknya kualitas jaringan	(H)
		j.Hilangnya pasokan listrik	(H)
		k.Sistem keamanan yang kurang handal	(L)
4.	Data Hasil Penelitian	a.Hilangnya data	(L)
		b.Human error	(L)
		c.Tidak dijalankannya tata kelola	(L)
		d.Koneksi jaringan terputus	(M)
		e.Backup failure	(L)
		f.Kurang baiknya kualitas jaringan	(M)
5.	Gedung	a.Debu/kotoran	(L)
		b.Koneksi jaringan terputus	(H)
		c.Kurang baiknya kualitas jaringan	(H)
		d.Hilangnya pasokan listrik	(H)
		e.Sistem keamanan yang kurang handal	(L)
6.	*Staff* Jaringan dan *Transfer Data*	a.Kurangnya SDM	(L)
		b.Pembagian tugas tidak jelas	(L)
		c.Tidak dijalankannya tata kelola	(L)

Berdasarkan identifikasi jenis ancaman untuk setiap infrastruktur RDSA yang ditunjukkan pada tabel III maka dapat dilihat *level* ancaman berdasarkan tingkat kemungkinan terjadinya.

Setelah dilakukan identifikasi tingkat atau *level* ancaman dari setiap aset, maka selanjutnya melakukan identifikasi tingkatan atau *level* kerentanan dari masing-masing jenis ancaman yang telah disebutkan. Hasil identifikasi kerentanan beserta daftar perlindungan yang telah diimplementasikan akan disajikan pada tabel IV sebagai berikut:

TABEL IV

DAFTAR ASET, JENIS ANCAMAN, KERENTANAN, DAN TINGKATANNYA

Aset-Ancaman	**Kerentanan**	***Level* kerentanan (L), (M), (H)**	***Existing Control***
1-a	Sistem *grounding* tidak bagus	(H)	Pasang penangkal petir, memper baharui sistem *grounding*
1-b	Lokasi terbuka	(L)	Dibersih kan secara berkala
1-c	Beban tugas yang berlebih	(M)	Pem bagian tugas
1-d	Beban tugas yang berlebih	(M)	Penambahan SDM
1-e	Belum ada prosedur pembagian tugas	(M)	Penambahan SDM
1-f	Belum ada prosedur	(H)	N/A
1-g	Perangkat keras baru/belum matang	(M)	Diperbaiki,apa bila tetap tidak bisa dikembalikan ke pihak ketiga
1-h	Banyak proses yang berjalan	(L)	*Maintena nce*
1-i	Perangkat kabel rusak	(L)	Perbaikan/peng gantian perangkat, menghubungi pihak ketiga
1-j	Mati listrik	(L)	*Backup* ulang
1-k	Banyak pihak yang mengakses jaringan	(M)	Menambah *bandwith*

Aset-Ancaman	**Kerentanan**	***Level* kerentanan (L), (M), (H)**	***Existing Control***
1-l	Jaringan listrik tidak stabil	(H)	*Backup* listrik/*genset*
2-a	*Human error*	(L)	Mengambil dari *backup data*
2-b	Beban tugas yang berlebih	(M)	Penambahan SDM
2-c	Belum ada prosedur pembagian tugas	(M)	Penambahan SDM
2-d	Belum ada prosedur	(H)	N/A
2-e	Mati listrik, jaringan internet terputus	(L)	*Genset*, cek ke lokasi
2-f	Perangkat kabel rusak	(L)	Perbaikan/penggantian perangkat, menghubungi pihak ketiga
2-g	Banyak proses yang berjalan	(L)	*Restart*
2-h	Data kepenuhan	(L)	Menghapus *temporary file*
2-i	Terlalu banyak menjalankan *script* penarikan data	(M)	
2-j	Mati listrik, jaringan terputus	(L)	*Backup* ulang
2-k	Banyak pihak yang mengakses jaringan	(L)	Menambah *bandwith*

Aset-Ancaman	**Kerentanan**	***Level* kerentanan (L), (M), (H)**	***Existing Control***
3-a	Sistem *grounding* tidak bagus, penataan kabel kurang baik	(H)	Ganti *router*
3-b	Keamanan kurang	(L)	CCTV
3-c	Beban tugas yang berlebih	(M)	Penambahan SDM
3-d	Belum ada prosedur pembagian tugas	(M)	Penambahan SDM
3-e	Belum ada prosedur	(H)	N/A
3-f	Pendingin mati	(L)	Perbaikan AC dan penambahan AC
3-g	Perangkat kabel rusak	(M)	Perbaikan/penggantian perangkat, menghubungi pihak ketiga
3-h	Banyak proses yang berjalan	(L)	*Restart*
3-i	Banyak pihak yang mengakses jaringan	(L)	Menambah *bandwith*
3-j	Jaringan listrik tidak stabil	(H)	*Backup* listrik/*genset*
3-k	Rentan terhadap pencurian	(L)	Menambah sistem keamanan
4-a	*Human error*	(L)	Mengambil dari *backup data*
4-b	Beban tugas yang berlebih	(M)	Pembagian tugas
4-c	Belum ada prosedur	(H)	N/A
4-d	Perangkat kabel rusak	(M)	Perbaikan/penggantian perangkat, menghubungi pihak ketiga

Aset-Ancaman	Kerentanan	*Level* kerentanan (L), (M), (H)	*Existing Control*
4-e	Mati listrik, jaringan terputus	(L)	*Backup* ulang
4-f	Banyak pihak yang mengakses jaringan	(L)	Menambah *bandwith*
5-a	Lokasi terbuka	(L)	Dibersihkan secara berkala
5-b	Perangkat kabel rusak	(M)	Perbaikan/penggantian perangkat, menghubungi pihak ketiga
5-c	Banyak pihak yang mengakses jaringan	(L)	Menambah *bandwith*
5-d	Jaringan listrik tidak stabil	(H)	*Backup* listrik/*genset*
5-e	Rentan terhadap pencurian	(L)	Menambah sistem keamanan
6-a	Beban tugas yang berlebih	(L)	Penambahan SDM
6-b	Belum ada prosedur pembagian tugas	(L)	Penambahan SDM
6-c	Belum ada prosedur	(L)	N/A

Berdasarkan identifikasi kerentanan untuk setiap kemungkinan ancaman yang dapat terjadi pada aset infrastruktur RDSA yang ditunjukkan pada tabel IV maka dilihat tingkat atau *level* ancaman berdasarkan letak atau lokasi aset ditempatkan ditempat yang mudah tereksploitasi atau tidak.

D. Risk Estimation

Analisis risiko berarti melakukan penilaian risiko terhadap aset-aset RDSA dengan menggunakan matriks pendekatan ISO/IEC 27005:2011 untuk dapat menentukan risiko berdasarkan nilai aset, tingkat ancaman, dan tingkat kerentanan yang dapat dilihat pada tabel matriks risiko yang akan digunakan untuk menetukan *level* risiko dapat dilihat pada tabel V berikut:

TABEL V

MATRIKS LEVEL RISIKO

	Kemungkinan terjadi - ancaman	*Low* (L)			*Medium* (M)			*High* (H)		
	Kemudahan Eksploitasi	**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
Nilai Aset	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

Untuk setiap aset, kerentanan, dan ancaman yang relevan dipertimbangkan. Jika ada kerentanan tanpa ancaman yang sesuai, atau ancaman tanpa kerentanan yang sesuai, saat ini belum ada risiko (tetapi perawatan harus dilakukan seandainya situasi ini berubah). Adapun baris yang sesuai dalam matriks diidentifikasi oleh nilai aset, dan kolom yang sesuai diidentifikasi oleh kemungkinan terjadinya ancaman dan kemudahan eksploitasi. Sebagai contoh, jika aset memiliki nilai 3, ancamannya adalah *"high"* dan kerentanannya "*low"*, maka ukuran risiko adalah 5. Asumsikan aset memiliki nilai 2, misalnya untuk modifikasi, tingkat ancaman "*low"* dan kemudahan eksploitasi adalah "*high",* maka ukuran risiko adalah 4.

Berdasarkan tabel V, dapat dilihat merupakan matriks ISO/IEC 27005:2011 yang digunakan untuk menentukan *level* atau tingkat risiko diatas, dikelompokkan menjadi tiga kategori *level* risiko yaitu:

1. 0-2 termasuk kedalam kategori *low risk* (risiko rendah) yang berarti tidak menimbulkan kerugian besar bagi perusahaan.
2. 3-5 termasuk kedalam kategori *medium risk* (risiko sedang) yang berarti menimbulkan kerugian besar bagi perusahaan.
3. 6-8 termasuk kedalam kategori *high risk* (risiko tinggi) yang berarti menimbulkan kerugian besar bagi perusahaan.

Selanjutnya dengan menggunakan matriks pada tabel V akan didapatkan hasil *level* risiko untuk setiap aset infrastrukttur RDSA berdasarkan penilaian tingkat ancaman dan kerentanan. Penilaian secara lebih rinci akan dilampirkan pada lampiran dalam penelitian ini. Hasil analisis risiko akan disajikan pada tabel VI sebagai berikut:

TABEL VI

HASIL PENILAIAN RISIKO

Kategori Aset	Kode Aset	*Asset Valuation*	Kode Ancaman	*Level* Ancaman	Kerentanan	*Level* Kerentanan	*Level* Risiko	Kategori Level Risiko
Hardware	1.	4 (*Very high*)	a	(M)	Sistem *grounding* tidak bagus	H	7	*High risk*
			b	(L)	Lokasi terbuka	L	4	*Medium risk*
			c	(L)	Beban tugas yang berlebih	M	5	*Medium risk*
			d	(M)	Beban tugas yang berlebih	M	6	*High risk*
			e	(M)	Belum ada prosedur pembagian tugas	M	6	*High risk*
			f	(L)	Belum ada prosedur	H	6	*High risk*
			g	(M)	Perangkat keras baru/belum matang	M	6	*High risk*
			h	(M)	Banyak proses yang berjalan	L	5	*Medium risk*
		4 (*Very high*)	i	(H)	Perangkat kabel rusak	L	6	*High risk*
			j	(L)	Mati listrik	L	4	*Medium risk*
			k	(H)	Banyak pihak yang mengakses jaringan	M	7	*High risk*
			l	(H)	Jaringan listrik tidak stabil	H	8	*High risk*
Software	2	3 (*high*)	a	(L)	*Human error*	L	3	*Medium risk*
			b	(L)	Beban tugas yang berlebih	M	4	*Medium risk*
			c	(L)	Belum ada prosedur pembagian tugas	M	4	*Medium risk*
Soft war	2.	3	d	(L)	Belum ada prosedur	H	5	*Medium risk*
			e	(M)	Mati listrik, jaringan internet terputus	L	4	*Medium risk*
			f	(M)	Perangkat kabel rusak	L	4	*Medium risk*
			g	(M)	Banyak proses yang berjalan	L	4	*Medium risk*
			h	(L)	Data kepenuhan	L	3	*Medium risk*
			i	(L)	Terlalu banyak menjalankan *scrip*t penarikan data	M	4	*Medium risk*
			j	(L)	Mati listrik, jaringan terputus	L	3	*Medium risk*
			K	(M)	Banyak pihak yang mengakses jaringan	L	4	*Medium risk*
Jaringan	3.	3 (*High*)	a	(L)	Sistem *grounding* tidak bagus, penataan kabel kurang baik	H	5	*Medium risk*
			b	(L)	Keamanan kurang	L	3	*Medium risk*
			c	(L)	Beban tugas yang berlebih	M	4	*Medium risk*
			d	(L)	Belum ada prosedur pembagian tugas	M	4	*Medium risk*
			e	(L)	Belum ada prosedur	H	5	*Medium risk*
			f	(L)	Pendingin mati	L	3	*Medium risk*
Jaring an	3.	3	g	(H)	Perangkat kabel rusak	M	6	*High risk*

Kategori Aset	Kode Aset	*Asset Valuation*	Kode Ancaman	*Level* Ancaman	Kerentanan	*Level* Kerentanan	*Level* Risiko	Kategori Level Risiko
			h	(M)	Banyak proses yang berjalan	L	4	*Medium risk*
			i	(H)	Banyak pihak yang mengakses jaringan	L	5	*Medium risk*
			j	(H)	Jaringan listrik tidak stabil	H	7	*High risk*
			k	(L)	Rentan terhadap pencurian	L	3	*Medium risk*
Informasi/data	4.	4 (*Very high*)	a	(L)	*Human error*	L	4	*Medium risk*
			b	(L)	Beban tugas yang berlebih	M	5	*Medium risk*
			c	(L)	Belum ada prosedur	H	6	*High risk*
			d	(M)	Perangkat kabel rusak	M	6	*High risk*
			e	(L)	Mati listrik, jaringan terputus	L	4	*Medium risk*
			f	(M)	Banyak pihak yang mengakses jaringan	L	5	*Medium risk*
Supporting Facilities	5.	3 (*High*)	a	(L)	Lokasi terbuka	L	3	*Medium risk*
			b	(H)	Perangkat kabel rusak	M	6	*High risk*
			c	(H)	Banyak pihak yang mengakses jaringan	L	5	*Medium risk*
			d	(H)	Jaringan listrik tidak stabil	H	7	*High risk*
			e	(L)	Rentan terhadap pencurian	L	3	*Medium risk*
Human Resources	6.	3 (*High*)	a	(L)	Beban tugas yang berlebih	L	3	*Medium risk*
			b	(L)	Belum ada prosedur pembagian tugas	L	3	*Medium risk*
			c	(L)	Belum ada prosedur	L	3	*Medium risk*

Berdasarkan tabel VI dapat diketahui tingkat risiko berdasarkan tingkat ancaman dan kerentanannya untuk setiap masing-masing kategori aset. Hasil penilaian atau penentuan *level* risiko akan dipetakan ke dalam tabel pemetaan risiko sesuai dengan kategorinya. Pemetaan ini akan membantu melihat tingkat risiko secara keseluruhan untuk aset infrastruktur RDSA dan dievaluasi untuk menentukan kontrol rekomendasi sesuai ISO/IEC 27001:2013. Kontrol rekomendasi akan dipilih berdasarkan *risk acceptance level*, dimana akan dievaluasi pada hasil pemetaan risiko. Namun *acceptance level* harus ditentukan terlebih dahulu agar dapat mengetahui hingga batasan mana sebuah risiko dapat diterima oleh suatu perusahaan. Hasil pemetaan risiko aset RDSA akan ditampilkan pada tabel VII Pemetaan Risiko.

Berdasarkan tabel VII setelah dilakukan pemetaan kita dapat mengetahui bahwa secara keseluruhan aset infrastruktur RDSA berada pada kategori *high risk*, *medium risk*, dan *low risk.* Tabel VII berisi angka-huruf yang merupakan kode aset dengan kombinasi jenis ancamannya masing-masing. Dari tabel VII terlihat bahwa terdapat risiko yang berada dalam area warna biru atau risiko dengan kategori *high* (*high risk)*, dimana semakin gelap warnanya maka semakin tinggi nilai risiko kategorinya.

Begitu pula dengan area warna hijau untuk risiko kategori *medium (medium risk)* semakin berwarna hijau gelap maka nilai risiko semakin besar, dan risiko *low (low risk)* ditunjukkan oleh warna kuning, semakin berwarna kuning gelap maka nilai risiko semakin tinggi dengan rentang nilai 0-2. Sehingga dari pemetaan risiko ini kita dapat menentukan *risk acceptance level*. Berdasarkan hasil wawancara dengan narasumber diperoleh untuk *risk acceptance level* yaitu pada kategori risiko *low (low risk)* dengan batas nilai risiko adalah 2 atau pada tabel ditunjukkan oleh area yang berwarna kuning tua, dengan pertimbangan bahwa dampak yang akan ditimbulkan dari nilai aset dan ancamannya dapat diterima oleh perusahaan. Selebihnya tingkat risiko dengan nilai 3 atau diatas *risk acceptance level* pada tabel ditunjukkan oleh area berwarna hijau muda hingga biru gelap tidak dapat diterima oleh perusahaan.

TABEL VII

PEMETAAN RISIKO

	Kemungkinan terjadi - ancaman	***Low* (L)**			***Medium* (M)**			***High* (H)**		
	Kemudahan Eksploitasi	**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
Nilai Aset	0	**3-a, 3-b, 3-g, 3-j, 20-a**	**3-c, 3-d, 3-e, 20-b**				**3-i, 20-c**	**3-f, 19-b**	**3-h, 19-a**	**19-c**
	1									
	2	**7-e, 7-h, 8-e, 8-h, 9-e, 9-h, 10-e, 10-h, 11-e, 11-g, 11-i**	**7-a, 7-b, 8-a, 8-b, 9-a, 9-b, 10-a, 10-b, 11-a, 11-b**	**7-c, 8-c, 9-c, 10-c, 11-c**	**11-f**		**7-g, 8-g, 9-g, 10-g, 11-h**	**7-d, 7-f, 8-d, 8-f, 9-d, 9-f, 10-d, 10-f, 11-d**		
	3	**5-a, 5-h, 5-j, 6-e, 6-g, 6-i, 12-b, 12-f, 12-k, 13-b, 13-h, 18-a, 18-e, 21-a, 21-b, 21-c**	**5-b, 5-c, 5-i, 6-a, 6-c, 6-h, 12-c, 12-d ,13-c, 13-d**	**5-d, 6-b, 12-a, 12-e, 13-e**	**5-e, 5-f, 5-g, 5-k, 6-d, 6-f, 6-j, 12-h, 13-g, 13-j**		**6-k**	**12-i, 13-k, 18-c**	**12-g, 13-f, 13-i, 18-b**	**12-j, 13-a, 13-l, 18-d**
	4	**1-b, 1-j, 2-a, 2-g, 4-c, 4-d, 4-e, 4-f, 4-g, 4-m, 4-p, 16-a, 17-a, 17-e**	**1-b, 4-i, 15-b, 15-c, 17-b**	**1-f, 2-d, 4-j, 15-a, 15-d, 17-c**	**1-h, 2-e, 4-a, 4-l, 14-a, 17-f**	**1-d, 1-e, 1-g, 2-b, 2-c, 2-f, 4-h, 4-o, 17-d**	**1-a**	**1-i, 15-g, 15-h, 15-i, 16-c**	**1-k, 4-k, 4-n, 15-e, 15-f, 16-b**	**1-l, 4-b, 4-q, 15-j, 16-d**

TABEL VIII

KONTROL REKOMENDASI BERDASARKAN ISO 27005:2011

No.	Kontrol Rekomendasi (Klausul)	Kode (Aset-Ancaman)	Ada, Belum diimplementasi	Ada, Sudah diimplementasi dan Sudah efektif	Ada, Sudah diimplementasi dan Belum Efektif	Keterangan
1.	*Equipment sitting and protection* (A.11.2.1)	1-a; 1-b; 2-a; 2-g; 4-a; 4-b; 4-c; 4-d; 4-e; 4-g; 12-a; 13-a; 15-a; 16-a; 18-a; 20-a; 12-b; 13-b;		√		Membuat rangka besi untuk perangkat dengan gembok

No.	Kontrol Rekomendasi (Klausul)	Kode (Aset-Ancaman)	Ada, Belum diimplementasi	Ada, Sudah diimplementasi dan Sudah efektif	Ada, Sudah diimplementasi dan Belum Efektif	Keterangan
2.	*Management responsibilities* (A.7.2.1)	1-e; 1-f; 2-c; 2-d; 4-i; 4-j; 5-c; 5-d; 6-a; 6-b; 7-b; 7-c; 8-b; 8-c; 9-b; 9-c; 10-b; 10-c; 11-b; 11-c; 12-d; 12-e; 13-d; 13-e; 15-c; 15-d; 17-c; 21-b; 21-c;			√	Pelatihan untuk *staff* agar bertanggung jawab dalam pembagian tugas yang ada.
3.	Cabling security (A.11.2.3)	1-k; 2-e; 4-l; 5-f; 6-f; 7-d; 8-d; 9-d; 10-d; 11-d; 12-g; 13-i; 15-f; 16-b; 17-d; 18-b; 19-a;		√		Penggantian kabel yang rusak serta menggunakan kabel dengan kualitas lapisan pelindung yang tebal dan kuat agar tidak rentan rusak
4.	Equipment maintenance (A.11.2.4)	1-i; 1-g; 2-f; 3-h; 4-k; 4-m; 4-n; 4-o; 5-e; 5-g; 5-h; 5-i; 6-c; 6-d; 6-e; 6-f; 6-g; 6-i; 7-f; 8-f; 9-f; 10-f; 11-f; 12-f; 12-h; 12-i; 12-k; 13-f 13-g; 13-h; 13-j; 13-k 14-a; 15-e; 15-g; 15-h; 16-c; 17-e; 17-f; 18-c; 18-d; 19-b; 20-b;		√		Membuat sistem keamanan kunci dan gembok pada perangkat.
5.	*Information backup* (A.12.3.1)	5-a; 6-i; 17-a;		√		Melakukan *backup* data secara berkala
6.	*Information security awareness, education, and training* (A.7.2.2)	1-c 17-b	√			Pelatihan untuk *staff* yang bertanggung jawab terhadap keamanan informasi

Tabel VIII adalah tabel kontrol rekomendasi berdasarkan ISO 27005:2011 dimana ada 6 rekomendasi yang diusulkan kepada LAPAN sebagai perbaikan agar risiko yang mungkin terjadi dapat diminimalkan.

IV. SIMPULAN DAN SARAN

A. *Simpulan*

Dari hasil analisis penilaian risiko menggunakan matriks *level* risiko dari pendekatan ISO/IEC 27005:2011 pada infrastruktur RDSA di LAPAN Bandung maka dapat diperoleh kesimpulan sebagai berikut:

1. Hasil identifikasi aset RDSA diperoleh 21 daftar aset yang dilakukan penilaian dan analisis risiko. Hasil identifikasi aset menunjukkan bahwa aset yang bernilai 3 dan 4 (*high* dan *very high)* cenderung aset perangkat keras.
2. Hasil identifikasi kerentanan pada set RDSA menunjukkan jenis kerentanan dibagi kedalam tiga kategori yaitu kerentanan *low* (L), kerentanan *medium* (M), dan kerentanan *high* (H), dimana satu aset memiliki beberapa kerentanan yang sama jenisnya dan juga berbeda jenisnya. Satu jenis kerentanan bisa menimpa satu aset dan beberapa aset lainnya. Sehingga dari hasil identifikasi diperoleh jenis kerentanan dengan rincian berikut 81 kerentanan dengan tingkat *low* (L), 50 kerentanan dengan tingkat *medium* (M), 53 kerentanan dengan tingkat *high* (H). Hal ini menunjukkan aset infrastruktur RDSA cenderung memiliki tingkat kerentanan *low* (L).
3. Hasil penilaian risiko berdasarkan analisis menunjukkan *level* risiko cenderung berada pada *risk acceptance level*,namun ada beberapa aset yang memiliki *level* risiko diantara 6-8 (*high risk*) seperti hilangnya pasokan listrik, kerusakan pada perangkat keras, sehingga harus dilakukan penanganan yang sesuai.

B. *Saran*

Berdasarkan simpulan yang ada, maka terdapat beberapa saran yang dapat dijadikan bahan masukan yaitu:

1. Adanya peningkatan ancaman yaitu ancaman hilangnya pasokan listrik, maka untuk mencegah ancaman tersebut sebaiknya LAPAN perlu melakukan kerja sama kepada PLN untuk tidak melakukan pemutusan listrik di daerah-daerah stasiun pengambilan data sehingga pengambilan data tidak terhambat atau dapat membeli UPS untuk mencegah kehilangan data dan kerusakan *hardware*.
2. Terdapat ancaman lain yang mengalami peningkatan yaitu ancaman pencurian perangkat keras dan kerusakan fisik perangkat keras, maka sebaiknya LAPAN perlu melakukan kerjasama dengan pihak ketiga dalam hal ini adalah melakukan pengamanan dengan satpam atau kepolisian agar ancaman kehilangan dapat diminimalkan.
3. Untuk ancaman dari sisi sumber daya manusia maka perlu dianggarkan untuk pelatihan SDM untuk mengoperasikan komputer dan kemampuan *troubleshooting* jaringan sehingga apabila ada masalah dapat ditangani langsung oleh staf yang bertugas.

DAFTAR PUSTAKA

[1] A. Kadir and T. Ch. Triwahyuni, Pengantar Teknologi Informasi, Yogyakarta: ANDI Yogyakarta, 2013.

[2] T. Sutabri, Analisis Sistem Infromasi, Yogyakarta: ANDI Yogyakarta, 2012.

[3] H. Siahaan, Manajemen Risiko, Jakarta: PT. Elex Media Komputindo, 2007.

[4] I. Fahmi, SE, Msi., Manajemen Risiko, Bandung: Alfabeta, 2010.

[5] S. Djojosoedarso, Prinsip-prinsip Manajemen Risiko Ansuransi, Jakarta: Salemba Empat, 2005.

[6] M. E. Whitman and H. J. Mattord, Principles of Information Security, United States: Course Technology, 2012.

[7] C. D, G. S, R. G and W. P, Project Risk Management Guidelines: Managing Risk in Large Projects and Complex Procurements, Chichester, West Sussex: John Wiley & Sons Ltd, 2004.

[8] G. M. Husein and R. V. Imbar, "Analisis Manajemen Resiko Teknologi Informasi Penerapan Pada Document Management System di PT. Jabar Telematika (JATEL," *Jurnal Teknologi Informasi Sistem Informasi* , vol. 1, no. 2, p. 2, 2015.

[9] "ISO/IEC 27001," *ISO/IEC 27001,* 2013.

[10] "ISO 27005," *ISO 27005,* 2011.

[11] H. P, Fundamentals of Risk Management:Understanding, Evaluating, and Implementing Effective Risk Management, London: Kogan Page, 2010.

[12] Peltier, Informatin Security Risk Analysis Third Edition, Boston USA: Auerbach publications, 2014.

[13] J. A. Cazemier and P. O. Et Al, Information Security Management with ITIL, Netherlands: Van Haren Publishing, 2010.