Perancangan Manajemen Risiko Keamanan Informasi pada Penyelenggara Sertifikasi Elektronik (PSrE)

Wawan Hermawan

Badan Pengkajian dan Penerapan Teknologi, Republik Indonesia
wawan.hermawan@bppt.go.id

Abstrak
Badan Pengkajian dan Penerapan Teknologi (BPPT) merupakan Penyelenggara Sertifikasi Elektronik (PSrE) untuk instansi pemerintah. Berdasarkan Peraturan Pemerintah No.82 Tahun 2012 Penyelenggara Sertifikasi Elektronik (PSrE) BPPT dikategorikan sebagai Penyelenggara Sistem Elektronik yang termasuk dalam Penyelenggara Sistem Elektronik strategis dan tinggi sehingga diwajibkan untuk memiliki sistem manajemen keamanan informasi. Dalam penelitian ini, untuk mendukung Penyelenggara Sertifikasi Elektronik (PSrE) BPPT memiliki sistem manajemen keamanan informasi maka dilakukan perancangan manajemen risiko keamanan informasi. Rancangan manajemen risiko pada Penyelenggara Sertifikasi Elektronik (PSrE) BPPT menggunakan *framework* ISO/IEC 27005 seperti penentuan konteks, kriteria dasar pengelolaan risiko, penentuan ruang lingkup, penilaian risiko, penanganan dan penerimaan risiko itu sendiri, aset utama dan aset pendukung pada Penyelenggara Sertifikasi Elektronik (PSrE) BPPT semua dilakukan penilaian risikonya dan untuk menghitung nilai risiko menggunakan NIST SP 800-30. Kemudian pada tahapan penanganan risiko menggunakan ISO/IEC 27002. Dari hasil penelitian ini, dapat disimpulkan bahwa terdapat terdapat 51 skenario risiko yang dilakukan pengurangan risiko (*reduction*) dan 10 skenario risiko yang dilakukan penerimaan risiko (*accept*) dengan mengaplikasikan kontrol yang direkomendasikan berdasarkan kepada ISO/IEC 27002.

Keywords: Penyelenggara Sertifikasi Elektronik; Manajemen Risiko; ISO 27005; ISO 27002; Manajemen Keamanan Informasi

DOI: 10.22441/incomtech.v9i2.6474

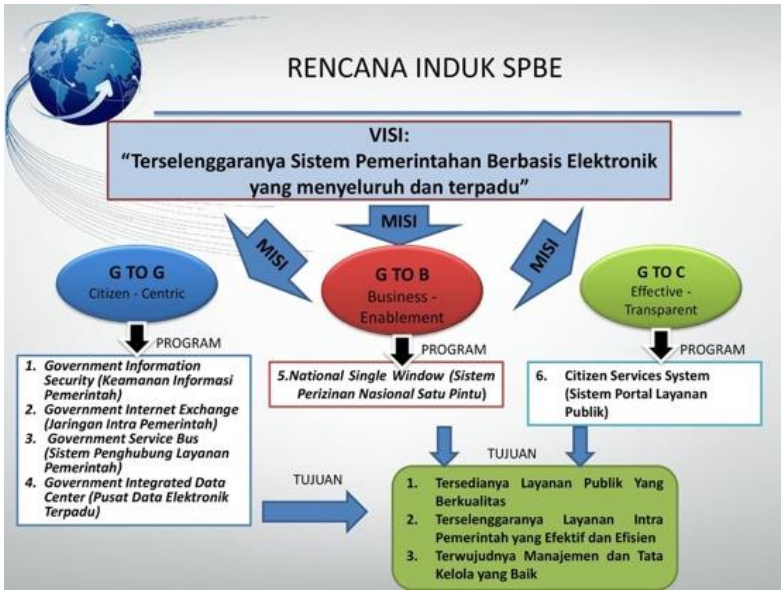
1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi (TIK) yang sangat cepat mempengaruhi segala sektor kehidupan, baik yang berhubungan dengan sektor personal, ekonomi, sosial maupun pemerintahan. Penggunaan teknologi informasi

dan komunikasi di lingkungan pemerintahan dalam rangka meningkatkan kualitas layanan publik secara efektif- dan efisien dikenal dengan sebutan *e-Government*.

Undang-Undang Tentang Informasi dan Transaksi Elektronik (ITE) No 11 Tahun 2008 [1] dan PP 61/2010 menjamin bahwa transaksi elektronik telah memiliki payung hukum yang jelas. Amanah *e-Government* semakin jelas dari pasal 4 butir c UU ITE yang menyebutkan bahwa pemanfaatan teknologi informasi dan transaksi elektronik dilaksanakan dengan tujuan untuk meningkatkan efektifitas dan efisiensi pelayanan publik.

Rencana Induk Sistem Pemerintahan Berbasis Elektronik (SPBE) Nasional [2] disusun dengan mengacu pada arah kebijakan RPJP Nasional 2005 - 2025, Grand Design Reformasi Birokrasi 20l0 - 2025, dan RPJM Nasional 20I4 - 20I9. Pencapaian visi SPBE yang terpadu dan menyeluruh memiliki peran yang sangat penting di dalam penyelenggaraan pemerintahan untuk mewujudkan birokrasi pemerintahan yang terpadu dan berkinerja tinggi, meningkatkan kualitas pelayanan publik, mewujudkan tata kelola pemerintahan yang bersih, efektif, efisien, transparan, dan akuntabel, dan pada akhirnya mampu mewujudkan bangsa yang berdaya saing. Rencana induk Sistem Pemerintahan Berbasis Elektronik (SPBE) dapat dilihat pada Gambar. 1 dibawah ini :



Gambar. 1 Rencana Induk SPBE

Hal mengenai SPBE tertuang dalam Peraturan Presiden No. 95 Tahun 2018 Tentang Sistem Pemerintahan Berbasis Elektronik dimana pada pasal 40 ayat (1) mengenai Keamanan Sistem Pemerintahan Berbasis Elektronik mencakup penjaminan kerahasiaan, keutuhan, ketersediaan, keaslian, dan kenirsangkalan (nonrepudiation) sumber daya terkait data dan informasi, Infrastruktur SPBE, dan Aplikasi SPBE. Dan sebagai penjaminan kenirsangkalan (nonrepudiation) sebagaimana dimaksud pada pasal 40 ayat (1) dilakukan melalui penerapan tanda tangan digital dan jaminan pihak ketiga terpercaya melalui penggunaan sertifikat elektronik.

Pihak ketiga terpercaya yang dimaksud tersebut adalah Penyelenggara Sertifikasi Elektronik (PSrE) . Penyelenggara Sertifikasi Elektronik (PSrE)

sebagai *trusted third party* adalah entitas yang menerbitkan sertifikat elektronik berdasarkan standar *ITU-T X509*, bertugas melakukan pengecekan validitas dan melacak sertifikat yang telah dicabut atau kadaluarsa [3]. Di dalam sertifikat tersebut, tercantum informasi pemilik kunci publik (*public key*) yang otentik dan informasi Penyelenggara Sertifikasi Elektronik (PSrE) sebagai penerbit sertifikat. Pasangan kunci publik dan kunci privat (*private key*) dipakai untuk melakukan tanda tangan digital dan *secure communication* melalui https atau email dengan sistem enkripsi asimetrik.

Penyelenggara Sertifikasi Elektronik (PSrE) sebagai *Trusted Trust Party* (TTP) merupakan Penyelenggara Sertifikasi Elektronik (PSrE) sebagaimana dinyatakan dalam Peraturan Pemerintah No.82 Tahun 2012 [4]. PSrE dikategorikan sebagai penyelenggara sistem elektronik yang termasuk dalam penyelenggara sistem elektronik strategis dan tinggi sehingga diwajibkan untuk memiliki sistem manajemen keamanan informasi.

Badan Pengkajian dan Penerapan Teknologi (BPPT) saat ini sudah terdaftar sebagai Penyelenggara Sertifikasi Elektronik (PSrE) untuk instansi pemerintah di Kementerian Komunikasi dan Informatika sesuai dengan Keputusan Menteri Komunikasi dan Informatika No.969 Tahun 2018. Ketidaktergantungan terhadap institusi luar negeri mengenai keamanan adalah faktor yang mendorong BPPT membangun organisasi Penyelenggara Sertifikasi Elektronik (PSrE) untuk mempercepat kemandirian bangsa dalam mengelola sistem keamanan informasinya. Usaha yang dilakukan untuk mencapai kemandirian ini adalah dengan meningkatkan kemampuan mengoperasikan sebuah Penyelenggara Sertifikasi Elektronik (PSrE) di pemerintahan, baik dari sisi teknis maupun sisi manajemennya.

Menurut Peraturan Menteri Kementrian Komunikasi dan Informatika Republik Indonesia No.11 Tahun 2018 pasal 12 [5], jika BPPT ingin meningkatkan status pengakuan dari terdaftar menjadi berinduk sebagai Penyelenggara Sertifikasi Elektronik (PSrE), maka harus memenuhi persyaratan sebagai PSrE berinduk yang salah satu syaratnya harus mendapatkan tanda daftar Penyelenggara Sistem Elektronik (PSE).

Untuk memenuhi syarat Penyelenggara Sistem Elektronik (PSE) dan memiliki tanda daftar Penyelenggara Sistem Elektronik (PSE), maka BPPT harus memenuhi persyaratan seperti tercantum di Peraturan Menteri Kementrian Komunikasi dan Informatika Republik Indonesia No.7 Tahun 2018 [6] yang salah satu syaratnya harus mempunyai sertifikat keamanan informasi dengan menerapkan sistem manajemen pengamanan informasi berdasarkan atas risiko. Selain itu BPPT sebagai instansi pemerintah harus memenuhi kepatuhan terhadap Peraturan Menteri Komunikasi dan Informatika No.4 Tahun 2016 [7] yang mengatur mengenai pencegahan, penanggulangan ancaman dan serangan yang dapat menimbulkan gangguan berdasarkan risiko yang sudah dianalisis serta memenuhi kepatuhan terhadap standard ISO/IEC 27001.

Kondisi Penyelenggara Sertifikasi Elektronik (PSrE) BPPT saat ini belum memiliki sistem manajemen keamanan informasi yang menjadi salah satu syarat apabila BPPT mau menjadi Penyelenggara Sertifikasi Elektronik (PSrE) Berinduk. Untuk itu pada penelitian ini akan dirancang manajemen risiko keamanan informasi berdasarkan panduan ISO/IEC 27005:2013 yang secara spesifik dan komprehensif untuk melakukan *assestment* terhadap keamanan informasi [8]. Dan juga akan

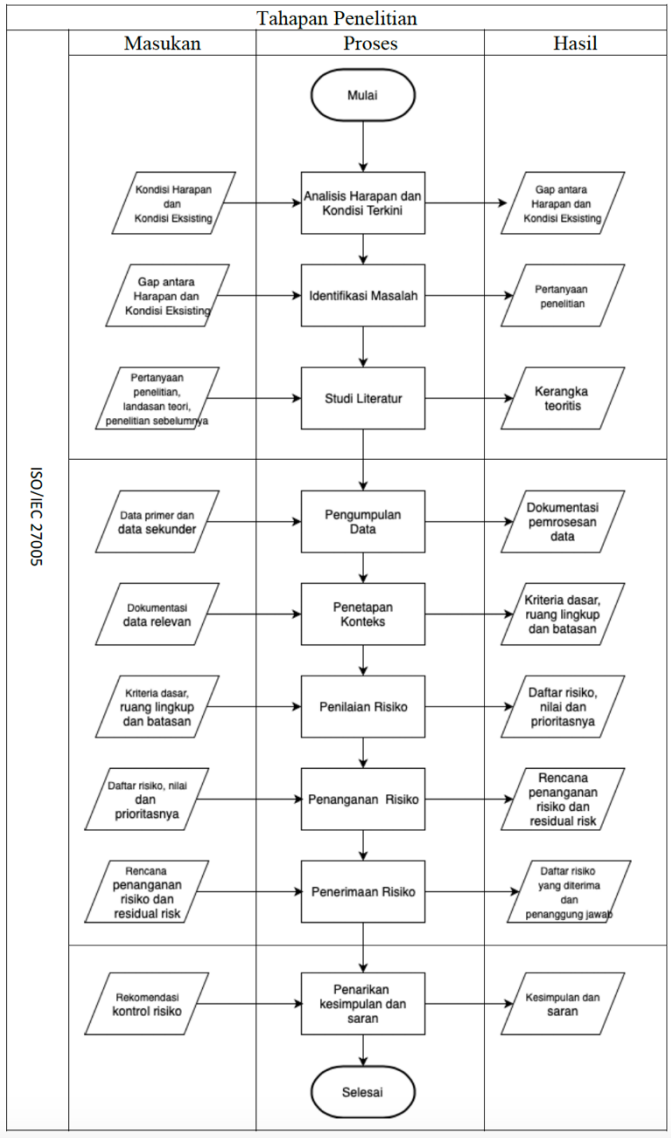
dibuat kontrol keamanan informasi Penyelenggara Sertifikasi Elektronik (PSrE) BPPT dalam mendukung penerapan sistem manajemen keamanan informasi. Perancangan kontrol keamanan informasi pada penelitian ini disusun suatu rancangan kontrol keamanan informasi Penyelenggara Sertifikasi Elektronik (PSrE) berdasarkan ISO/IEC 27002:2014 [9].

2. METODE PENELITIAN

Pada bagian ini membahas mengenai tahapan penelitian yang dilakukan untuk melakukan perencanaan manajemen risiko keamanan informasi.

A. Alur Penelitian

Penelitian ini dilakukan dengan mengadopsi tahapan yang disarankan oleh ISO/IEC 27005:2013. Tahapan penelitian yang akan dilakukan pada penelitian ini dapat dilihat pada Gambar 2



Gambar. 2 Metodologi Penelitian

Tahapan yang dilakukan dalam membuat manajemen risiko keamanan informasi pada Penyelenggara Sertifikasi Elektronik (PSrE) BPPT adalah:

1. Melakukan analisis harapan dan kondisi eksisting untuk melihat *gap* diantara keduanya.
2. Mengidentifikasi masalah berdasarkan *gap* yang telah ditemukan dan menentukan pertanyaan penelitian.
3. Melakukan studi literatur yang berkaitan dengan manajemen risiko keamanan informasi untuk membuat kerangka teoritis
4. Mengumpulkan data primer dan data sekunder untuk didokumentasikan.
5. Context establishment. Penentuan konteks manajemen risiko keamanan informasi dilakukan dengan menetapkan kriteria dasar serta mendefinisikan ruang lingkup dan batasan yang diperlukan untuk manajemen risiko keamanan informasi.
6. Risk assesment. Pada tahap ini risiko akan diidentifikasi, diukur secara kualitatif dan diprioritaskan sesuai dengan kriteria evaluasi risiko yang telah ditetapkan.
7. Risk treatment. Pada tahap ini kontrol untuk mengurangi, mempertahankan, menghindari, atau mentransfer risiko ditetapkan dan direncanakan. Penentuan kontrol dilakukan dengan mengacu ISO/IEC 27002:2014.
8. Risk acceptance. Pada tahap ini keputusan untuk menerima risiko harus didokumentasikan. Pihak yang bertanggung jawab atas keputusan yang telah dibuat harus ditentukan dan didokumentasikan secara resmi.
9. Menarik kesimpulan berdasarkan kontrol risiko keamanan informasi yang telah ditetapkan.

B. Metode Pengumpulan Data

Dalam penelitian ini, data yang dijadikan acuan untuk melakukan evaluasi terhadap manajemen risiko keamanan informasi dibagi menjadi dua, yaitu data primer dan data sekunder.

a. Data primer Data primer merupakan data yang diperoleh langsung dari sumber yang relevan. Dalam penelitian ini, data primer didapat melalui wawancara terhadap pihak terkait, pengisian *assessment checklist*, serta survei dan observasi lapangan.
b. Data sekunder Data sekunder merupakan data yang didapat melalui dokumen organisasi maupun hasil penelitian yang dilakukan oleh orang lain. Dalam penelitian ini, data sekunder didapat dari dokumen arsitektur teknologi sistem Penyelenggara Sertifikasi Elektronik (PSrE) BPPT, dokumen kebijakan organisasi, serta dokumen pendukung studi literatur.

C. Metode Analisis Data

Setelah mendapatkan data yang dibutuhkan maka dilakukan analisis data yaitu antara lain:

a. Analisis perencanaan manajemen risiko keamanan informasi menggunakan metode ISO/IEC 27005:2013;
b. Analisis kontrol keamanan informasi menggunakan ISO/IEC 27002:2014.

3. HASIL DAN PEMBAHASAN

Pada penelitian ini proses perencanaan manajemen risiko keamanan informasi sesuai dengan kerangka kerja ISO/IEC 27005:2013 yang dimulai dengan penetapan konteks dan penilaian risiko, selanjutnya akan dilakukan penanganan risiko dan penerimaan risiko yang sesuai.

A. Penetapan Konteks

Penetapan konteks bertujuan untuk menentukan spesifikasi kriteria dasar yang berupa kriteria dampak, kriteria kemungkinan terjadi, dan kriteria penerimaan risiko. Selain itu penetapan konteks juga bertujuan untuk menentukan ruang lingkup dan batas-batas, dan organisasi untuk proses manajemen risiko keamanan informasi. Ruang lingkup penilaian risiko berupa risiko operasional yang terjadi pada dua proses kritikal Penyelenggara Sertifikasi Elektronik (PSrE) BPPT yaitu proses penerbitan sertifikat elektronik dan proses bisnis validasi sertifikat elektronik.

- Kriteria Dasar Pengelolaan Risiko

Dalam hal ini terdapat kriteria dalam pengelolaan risiko yang terdiri dari kriteria evaluasi risiko, kriteria dampak dan kriteria penerimaan risiko. Adapun penjelasan setiap kriteria sebagai berikut :

a. Kriteria evaluasi risiko

Berdarkan ISO/IEC 27005:2013 bahwa terdapat beberapa macam kriteria evaluasi risiko yang dapat ditentukan dari beberapa faktor antara lain :

1. Nilai strategis dari proses informasi bisnis;
2. Kebutuhan untuk regulasi dan hokum ;
3. Tingkat kekritisan aset informasi yang terkait;
4. Kepentingan operasional bisnis terkait *confidentiality*, *integrity* dan *availability*;
5. Pengaruh terhadap kepentingan stakeholder;
6. Konsekuensi terhadap reputasi organisasi.

Dalam penelitian ini kriteria dibentuk dengan memperhatikan keenam pertimbangan di atas. Namun pertimbangan yang paling utama adalah kepentingan operasional bisnis terkait *confidentiality*, *integrity* dan *availability* dan pengaruh terhadap kepentingan stakeholder yang dapat mempengaruhi proses kinerja Penyelenggara Sertifikasi Elektronik (PSrE) BPPT.

b. Kriteria Dampak

Tahap selanjutnya adalah menentukan kriteria dampak dan kriteria kecenderungan risiko untuk kemudian nanti dipakai pada pengendalian dan penerimaan risiko. Dalam penelitian ini kriteria dampak dan kecenderungan didapatkan dari hasil wawancara dengan berbagai narasumber yang terkait organisasi Penyelenggara Sertifikasi Elektronik (PSrE) BPPT. Kriteria dampak ini mempengaruhi strategi dan operasional organisasi Penyelenggara Sertifikasi Elektronik (PSrE) BPPT dan juga dapat berpengaruh terhadap *stakeholder* terkait.

Tabel 1. Kriteria Dampak

Tingkat Dampak	Keterangan
Tinggi	1. Proses bisnis utama mengalami gangguan total dan berhenti 2. Terdapat data rahasia yang dapat diakses dan/atau dimodifikasi oleh pihak yang tidak berwenang 3. Adanya data yang rusak/hilang dan tidak memiliki backup 4. Hilangnya reputasi dan kepercayaan organisasi PSrE
Sedang	1. Proses bisnis terganggu namun proses bisnis utama tetap dapat berjalan 2. Adanya data yang rusak/hilang dan tidak memiliki backup
Rendah	1. Tidak menyebabkan gangguan pada operasional proses bisnis 2. Adanya data yang rusak/hilang namun terdapat backup

Dan berikut ini adalah kriteria kecenderungan yang ditetapkan oleh Penyelenggara Sertifikasi Elektronik (PSrE) BPPT pada penelitian ini:

Tabel 2. Tingkat Kecenderungan Risiko

Tingkat Kecenderungan	Penjelasan
Tinggi	1. Terjadi lebih dari 12 kali dalam setahun 2. Kontrol tidak berjalan dan/atau tidak memiliki kontrol
Sedang	1. Terjadi 6 sampai 12 kali dalam setahun 2. Memiliki kontrol yang dapat mengurangi ancaman
Rendah	1. Terjadi kurang dari 6 kali dalam setahun 2. Memiliki kontrol yang dapat mengurangi ancaman dan mencegah kerentanan

c. Kriteria Penerimaan Risiko

Dalam penelitian ini ditentukan selera risiko yang bersumber pada selera organisasi dalam mengevaluasi dan memilih penanganan risiko yang ada. Tabel III menjelaskan matriks selera risiko organisasi Penyelenggara Sertifikasi Elektronik (PSrE) BPPT:

Tabel 3. Kriteria Penerimaan Risiko

Dampak / Kecenderungan	Rendah	Sedang	Tinggi
Tinggi	Mitigate	Mitigate	Mitigate
Sedang	Accept	Mitigate	Mitigate
Rendah	Accept	Accept	Mitigate

B. *Penilaian Risiko*

Setelah menetapkan konteks, langkah selanjutnya adalah menilai risiko. Penilaian risiko dilakukan untuk mengidentifikasi serta menilai aset informasi, mengidentifikasi ancaman-ancaman dan kerentanan yang mungkin muncul, mengidentifikasi kontrol yang telah ada, menentukan potensi konsekuensi dan memprioritaskan risiko yang diperoleh dan mengurutkannya berdasarkan kriteria evaluasi risiko yang telah ditetapkan pada pembangunan konteks. Penilaian risiko mencakup kegiatan identifikasi risiko, analisis risiko, dan evaluasi risiko.

C. *Identifikasi Risiko*

Identifikasi risiko dilakukan dengan melakukan *focus group discussion*. Proses yang dilakukan adalah identifikasi aset, identifikasi ancaman, identifikasi kontrol yang telah ada, identifikasi kerawanan serta dampak yang mungkin muncul. Identifikasi aset dilakukan dengan mengelompokkan aset menjadi *primary asset* dan *secondary asset*. Berdasarkan [10], aset yang termasuk primary asset adalah proses bisnis dan informasi. Sementara aset yang termasuk dalam *secondary asset* adalah:

1. Perangkat keras
2. Perangkat lunak
3. Jaringan
4. Sumber Daya Manusia (SDM)
5. *Site*
6. Stuktur organisasi

Tabel 5. Daftar Aset Penyelenggaraa Sertifikasi Elektronik (PSRE) BPPT

	Aspek Keamanan Informasi	Aset
1	Teknologi	Aplikasi Penerbitan Sertifikat Elektronik
2		Aplikasi Validasi Sertifikat Elektronik
3		Database
4		Database Server
5		Storage Server
6		Core Switch
7		Distribution Switch
8		Access Switch
9		Router
10		Kabel Jaringan
11		Firewall
12		HSM
13		PC
14		MariaDB
15		Linux Server
16		Anti Virus
17		VPN
18		Load Balancer
19		EJBCA
20		TSA
21	SDM	CA Administrator
22		RA Administrator
23		Developer
24		Operator RA
25	Proses Bisnis	Proses Penerbitan Sertifikat Elektronik
26		Proses Validasi Sertifikat Elektronik
27	Informasi	Dokumen CP
28		Dokumen CPS
29		Dokumen Business Plan
30		Dokumen BCP

31	Dokumen DRP
32	Data Pemohon Sertifikat Elektronik
33	Daftar Sertifikat Elektronik Aktif
34	Daftar Sertifikat Elektronik Dicabut

D. *Estimasi Risiko*

Setelah dampak dari setiap risiko teridentifikasi, selanjutnya dilakukan estimasi tingkat pengaruh dampak tersebut kepada bisnis Penyelenggara Sertifikasi Elektronik (PSrE) BPPT diidentifikasi. Tingkat dampak diidentifikasi dengan menggunakan kriteria tingkat dampak yang telah ditetapkan pada proses penetapan konteks. Tingkat dampak dibagi menjadi tiga yaitu tinggi, sedang dan rendah. Selain mengidentifikasi dampak, tingkat kecenderungan sebuah ancaman terjadi juga diidentifikasi seperti yang telah ditetapkan pada pada penetapan konteks.

E. *Evaluasi Risiko*

Pada tahap ini dilakukan evaluasi risiko berdasarkan dampak yang dapat terjadi oleh tiap ancaman pada masing-masing aset terhadap kecenderungan atau peluang terjadinya dampak tersebut. Berdasarkan ISO/IEC 27005:2013 terdapat tiga tingkatan dampak dan kecenderungan, dikarenakan tingkatan dampak dan kecenderungan yang dianalisis memiliki tiga tingkatan, oleh karena itu proses evaluasi risiko menggunakan framework dari NIST 800-300 [11]. Adapun evaluasi risiko berdasarkan matriks pada tabel 3.5

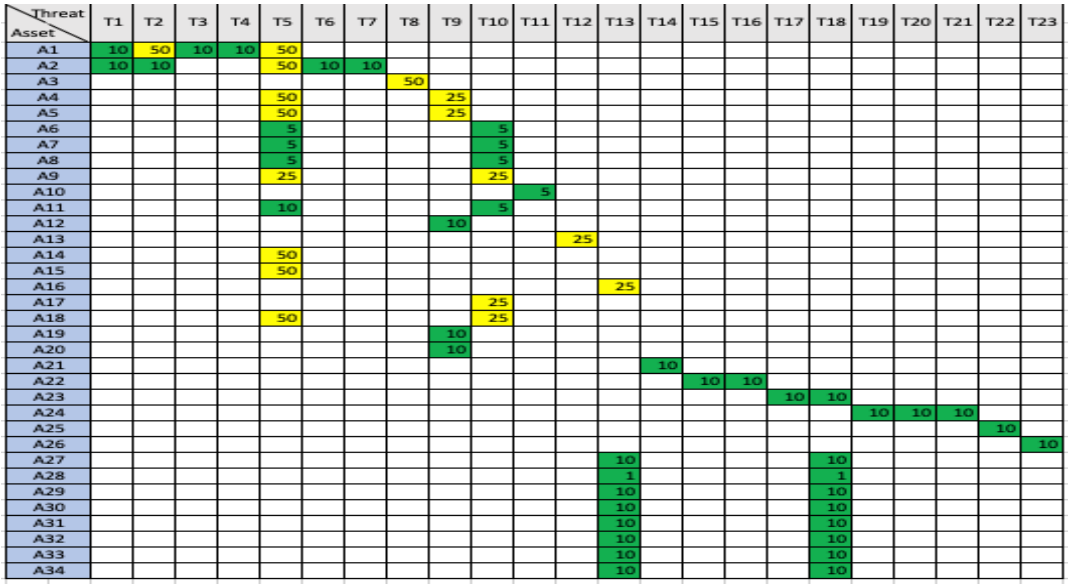
Tabel 5. Matriks Penentuan Tingkatan Evakuasi Risiko

Dampak / Kecenderungan	**Rendah (10)**	**Sedang (50)**	**Tinggi (100)**
Tinggi (1.0)	Rendah 10 x 1.0 = 10	Sedang 50 x 1.0 = 50	Tinggi 100 x 1.0 = 100
Sedang (0.5)	Rendah 10 x 0.5 = 5	Sedang 50 x 0.5 = 25	Sedang 100 x 0.5 = 50
Rendah (0.1)	Rendah 10 x 0.1 = 1	Rendah 50 x 0.1 = 5	Rendah 100 x 0.1 = 10

Tabel 5 menjelaskan terdapat tiga tingkatan evaluasi risiko yang merupakan hasil matriks dari tingkat dampak terhadap kecenderungan pada masing-masing aset dan ancaman yang menyertai. Cara mengetahui tingkatan risiko yaitu :

- Rendah (1 sampai 10)
- Sedang (>10 sampai 50)
- Tinggi (>50 sampai 100)

Berikut adalah rangkuman keseluruhan nilai evaluasi risiko pada tiap skenario risiko yang ditunjukan pada Gambar 3:



Threat / Asset	T1	T2	T3	T4	T5	T6	T7	T8	T9	T10	T11	T12	T13	T14	T15	T16	T17	T18	T19	T20	T21	T22	T23
A1	10	50	10	10	50																		
A2	10	10			50	10	10																
A3								50															
A4					50				25														
A5					50				25														
A6					5					5													
A7					5					5													
A8					5					5													
A9					25					25													
A10											5												
A11					10					5													
A12									10														
A13												25											
A14					50																		
A15					50																		
A16													25										
A17										25													
A18					50					25													
A19									10														
A20									10														
A21														10									
A22															10	10							
A23																	10	10					
A24																			10	10	10		
A25																						10	
A26																							10
A27													10					10					
A28													1					1					
A29													10					10					
A30													10					10					
A31													10					10					
A32													10					10					
A33													10					10					
A34													10					10					

Gambar. 4 Perhitungan Nilai Risiko

Berdasarkan hasil perhitungan nilai risiko pada Gambar 3 maka dapat dilakukan prioritas penanganan risiko dari nilai risiko tertinggi sampai dengan nilai risiko terendah pada Tabel 6 :

Tabel 6. Matriks Penentuan Tingkatan Evaluasi Risiko

Prioritas	Skenario	Nilai Risiko
1	A1 dan T2	Sedang (50)
2	A1 dan T5	Sedang (50)
3	A2 dan T5	Sedang (50)
4	A3 dan T8	Sedang (50)
5	A4 dan T5	Sedang (50)
6	A5 dan T5	Sedang (50)
7	A14 dan T5	Sedang (50)
8	A15 dan T5	Sedang (50)
9	A18 dan T5	Sedang (50)
10	A4 dan T9	Sedang (25)
11	A5 dan T9	Sedang (25)
12	A9 dan T5	Sedang (25)
13	A9 dan T10	Sedang (25)
14	A13 dan T12	Sedang (25)
15	A16 dan T13	Sedang (25)
16	A17 dan T10	Sedang (25)
17	A18 dan T10	Sedang (25)
18	A1 dan T1	Rendah (10)
19	A1 dan T3	Rendah (10)
20	A1 dan T4	Rendah (10)
21	A2 dan T1	Rendah (10)
22	A2 dan T6	Rendah (10)
23	A2 dan T7	Rendah (10)
24	A11 dan T5	Rendah (10)
25	A12 dan T9	Rendah (10)
26	A19 dan T9	Rendah (10)
27	A20 dan T9	Rendah (10)
28	A21 dan T14	Rendah (10)
29	A22 dan T15	Rendah (10)

30	A22 dan T16	Rendah (10)
31	A23 dan T17	Rendah (10)
32	A23 dan T18	Rendah (10)
33	A24 dan T19	Rendah (10)
34	A24 dan T20	Rendah (10)
35	A24 dan T21	Rendah (10)
36	A25 dan T22	Rendah (10)
37	A26 dan T23	Rendah (10)
38	A27 dan T13	Rendah (10)
39	A27 dan T18	Rendah (10)
40	A29 dan T13	Rendah (10)
41	A29 dan T18	Rendah (10)
42	A30 dan T13	Rendah (10)
43	A30 dan T18	Rendah (10)
44	A31 dan T13	Rendah (10)
45	A31 dan T18	Rendah (10)
46	A32 dan T13	Rendah (10)
47	A32 dan T18	Rendah (10)
48	A33 dan T13	Rendah (10)
49	A33 dan T18	Rendah (10)
50	A34 dan T13	Rendah (10)
51	A34 dan T18	Rendah (10)
52	A6 dan T5	Rendah (5)
53	A6 dan T10	Rendah (5)
54	A7 dan T5	Rendah (5)
55	A7 dan T10	Rendah (5)
56	A8 dan T5	Rendah (5)
57	A8 dan T10	Rendah (5)
58	A10 dan T11	Rendah (5)
59	A11 dan T10	Rendah (5)
60	A28 dan T13	Rendah (1)
61	A28 dan T18	Rendah (1)

F. *Penanganan Risiko*

Menurut ISO/IEC 27005:2013 terdapat empat macam penanganan risiko yaitu kontrol untuk mengurangi (*reduction*), mempertahankan (*retention*), menghindari (*avoidance*) atau mentransfer (*transfer*). Kontrol harus dipilih dan kemudian mempersiapkan rencana penanganan risiko tersebut. Pemilihan kontrol harus disesuaikan dengan risiko residual yang diharapkan. Apabila sudah sesuai dengan risiko residual yang diharapkan maka sebaiknya tidak perlu dilakukan kontrol tambahan, apabila nilai risiko lebih tinggi dari risiko residual yang diharapkan maka harus dilakukan kontrol tambahan.

Berdasarkan hasil wawancara yang dilakukan dengan tim dari Penyelenggara Sertifikasi Elektronik (PSrE) BPPT bahwa risiko residual yang diharapkan adalah risiko yang mempunyai:

- Maksimal mempunyai nilai dampak dengan tingkat sedang dan mempunyai nilai kecenderungan dengan tingkat rendah;
- Maksimal mempunyai nilai risiko dengan tingkat rendah atau bernilai 5.

G. *Penerimaan Risiko*

Pada penerimaan risiko berdasarkan ISO/IEC 27005:2013 pihak yang bertanggung jawab sebagai personal incharge (PIC) untuk melakukan kontrol akan setiap ancaman terhadap aset ditentukan. PIC bertanggung jawab untuk membuat dan me-monitor kontrol terhadap aset. Seluruh risiko pada kelompok yang bukan termasuk kelompok risiko rendah akan ditangani.

4. KESIMPULAN

Pada penelitian ini dapat disimpulkan kerangka kerja yang digunakan adalah ISO/IEC 27005:2013 dengan rancangan kontrol penanganan risiko ISO/IEC 27002:2014. Untuk tahap penilaian risiko kerangka kerja yang digunakan adalah NIST SP 800-30, hal tersebut dipilih karena NIST mempunyai langkah-langkah yang baik dan mempunyai panduan teknis dan identifikasi yang rinci seperti *checklist* dan matriks risiko yang sangat membantu dalam penyelesaian penelitian ini. Dari hasil penelitian ini terdapat terdapat 51 skenario risiko yang dilakukan pengurangan risiko (*reduction*) dan 10 skenario risiko yang dilakukan penerimaan risiko (*accept*) dengan mengaplikasikan kontrol yang direkomendasikan berdasarkan kepada ISO/IEC 27002:2014.

REFERENCES

[1] Presiden Republik Indonesia, & Dewan Perwakilan Rakyat Republik Indonesia. (2008). Undang-Undang No.11 tahun 2008 tentang Informasi dan Transaksi Elektronik. Jakarta, Indonesia.

[2] Peraturan Presiden Nomor 95 (2018): Tentang Sistem Pemerintah Berbasis Elektronik. Jakarta, Indonesia.

[3] Black, P. and Layton, R. (2014) '*Be Careful Who You Trust: Issues with the Public Key Infrastructure*'.

[4] Peraturan Pemerintah Nomor 82 (2012): Tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Jakarta, Indonesia.

[5] Peraturan Menteri Komunikasi dan Informatika Nomor 11 (2018): Tentang Penyelenggaraan Sertifikasi Elektronik. Jakarta, Indonesia.

[6] Peraturan Menteri Komunikasi dan Informatika Nomor 7 (2018): Tentang Pelayanan Perizinan Berusaha Terintegrasi Secara Elektronik Bidang Komunikasi dan Informatika. Jakarta. Indonesia.

[7] Peraturan Menteri Komunikasi dan Informatika Nomor 4 (2016): Tentang Manajemen Pengamanan Informasi. Jakarta, Indonesia.

[8] *International Standard Organization (2013). ISO/IEC 27005:2013 – Information Technology – Security Techniques – Information Security Risk Management. Switzerland*.

[9] *International Standard Organization (2014). ISO/IEC 27002:2014 – Information Technology – Information Security Risk Management System – Requirement.. Switzerland*.

[10] Liao, K. and Chueh, H. (2012) '*Medical Organization Information Security Management Based on ISO 27001 Information Security Standard*'.

[11] D, D. G. L. W. et al. (2017) '*Design of Information Security Risk Management using ISO/IEC 27005 and NIST SP 800-30 Revision 1 : A Case Study at Communication Data Applications of XYZ Institute*', International Conference on Information Technology Systems and Innovation (ICITSI).