Strategi Identifikasi Resiko Keamanan Informasi Dengan Kerangka Kerja ISO 27005:2018

W Yustanti[1], A Qoiriah[2], R Bisma[3], A Prihanto[4]

[1,2,3,4] (Jurusan Teknik Informatika, Universitas Negeri Surabaya)
[1]wiyliyustanti@unesa.ac.id

***Abstrak*— Penelitian ini membahas hasil kajian penerapan ISO 27001:2013 dengan melihat aspek manajemen resiko yang diatur dalam standar ISO 27005:2018. Namun demikian , karena pada dokumen standar tidak dijelaskan secara rinci bagaimana metodologi penilaian resiko sebagai proses yang harus dilakukan untuk mencapai tujuan dari apa yang telah dinyatakan dalam kontrol sistem manajemen keamanan informasi (SMKI), maka digunakan pendekatan operasional dalam penilaian resiko yang disebut sebagai *Factor Analysis Information Risk* (FAIR). Kesimpulan yang didapatkan adalah bahwa dengan menggunakan metode FAIR, maka proses penilaian resiko yang ditetapkan dalam ISO 27005:2018 sebagai bentuk kelengkapan untuk SMKI klausul 6 pada ISO 27001:2013 dapat dilakukan dengan lebih mudah.**

***Kata Kunci*— ISO 27001:2013, ISO 27005:2018, Sistem Manajemen Keamanan Informasi , metode FAIR**

I. PENDAHULUAN

Sejak tahun 2017, pemerintah khususnya dibawah lingkungan Kemenristekdikti mengeluarakan peraturan menteri no. 62 tahun 2017 terkait Tata Kelola Teknologi Informasi (TI) di lingkungan kementrian ristek dikti. Maksud dan tujuan dikeluarkan peraturan ini adalah sebagai pedoman dalam penyelenggaraan tata kelola pemerintah yang baik melalui e-government pada setiap unit organisasi pemerintah. Ruang lingkup dari peraturan ini meliputi struktur tata kelola TI, *enterprise architecture*, tata kelola pengembangan, tata kelola layanan dan tata kelola pengawasan. Untuk melaksanakan apa yang menjadi himbauan pemerintah maka pada tahun 2017 telah dilakukan audit keamanan informasi dengan menggunakan standart ISO 27001. Dalam bagian dari audit keamanan informasi ini, dibutuhkan sebuah pemahaman mengenai konsep manajemen resiko dari keamanan informasi itu sendiri. Oleh karena itu, selain mengenai kelengakapan standart juga perlu memahami jenis-jenis resiko berdasarkan ISO 27005. ISO 27005 merupakan standar yang digunakan untuk memberikan pedoman bagi kebutuhan tata kelola manajemen risiko keamanan informasi. ISO 27005 mendukung konsep umum yang dijelaskan dalam ISO 27001 dan dirancang untuk membantu penerapan keamanan informasi yang tepat berdasarkan pendekatan manajemen risiko. ISO 27005 tidak merinci, merekomendasikan atau bahkan secara khusus menunjukkan metode analisis risiko, meskipun didalamnya ada penjelasan terstruktur, sistematis, dan ketat dari awal hingga analisis risiko untuk menciptakan perlakuan risiko.

Permasalahan yang akan dibahas dalam tulisan ini adalah bagaimana melakukan identifikasi resiko TI untuk memenuhi standart ISO 27001:2013 dengan pendekatan metodolofi yang telah di atur dalam ISO 27005:2018.

II. TATA KELOLA TEKNOLOGI INFORMASI

Konsep tata kelola teknologi informasi merupakan sebuah kerangka bagaimana manajemen TI dapat menyediakan struktur untuk menyelaraskan strategi TI dengan strategi bisnis. Dengan mengikuti kerangka kerja formal, organisasi dapat menghasilkan hasil yang terukur untuk mencapai strategi dan tujuannya. Program formal juga memperhitungkan kepentingan para pemangku kepentingan, serta kebutuhan staf dan proses yang mengikuti. Secara umum, tata kelola TI adalah bagian integral dari tata kelola bisnis umum.

Pada era saat ini, wilayah otoritas TI semakin kompleks dan berisiko. Munculnya teknologi seluler, media sosial, dan cloud semakin memperluas bisnis di luar sistem keamanan perusahaan, yang memungkinakan untuk terbentuknya departemen TI bayangan (pihak ketiga). Sementara itu, data adalah aset bisnis yang juga sangat meningkatkan manajemen risiko dan tekanan kepatuhan. Meningkatnya ketergantungan pada pihak ketiga semakin memperumit model operasi.Pada kondisi seperti ini, terjadilah ketergantungan yang belum pernah terjadi sebelumnya pada teknologi, sehingga terdapat konsekuensi besar ketika gagal. Untuk itu diperlukan Tata kelola TI yang efektif untuk mengatasi tantangan yang kompleks ini. Dengan mengelola kinerja yang dapat menciptakan nilai dengan lebih baik melalui system pendukung keputusan berbasis TI , maka organisasi dapat mencapai sasaran strategisnya. Kerangka kerja tata kelola TI akan membantu mengidentifikasi mekanisme yang diperlukan untuk menciptakan nilai dan mengelola risiko yang terkait dengan TI.

III. MANAJAMEN RESIKO KEAMANAN INFORMASI

A. *ISO 27001:2013*

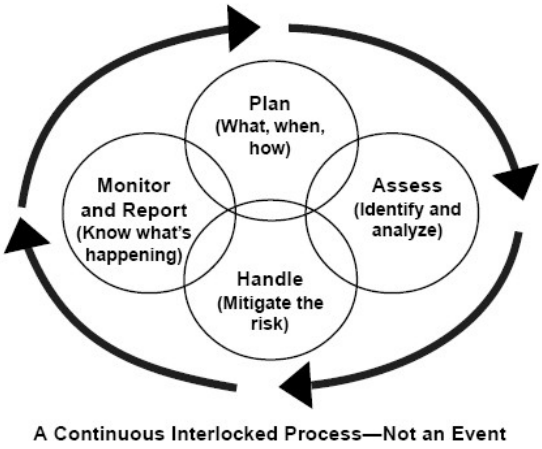
ISO / IEC 27001 merupakan standar keamanan informasi, versi terbaru diterbitkan pada tahun 2013 dengan beberapa

pembaruan kecil. Standar ini diterbitkan oleh Organisasi Internasional untuk Standardisasi (ISO) dan Komisi Listrik Internasional (IEC) di subkomite ISO dan IEC, ISO / ICC JTC3 / SC3. ISO / IEC 27001 berisi konsep dalam menetapkan sistem manajemen yang terkait dengan keamanan informasi dalam manajemen dan memenuhi persyaratan tertentu serta dinyatakan lulus audit oleh sebuah lembaga audit.

Keangka ISO 27001: 2013 ini merupakan dokumen yang berisi :

1) Lingkup standar
2) Dokumen rujukan
3) Persyaratan dan definisi ISO / IEC 27000
4) Konteks organisasi dan pemangku kepentingan
5) Keamanan informasi dan dukungan kebijakan tingkat tinggi
6) Merencanakan sistem manajemen keamanan informasi , penilaian risiko dan pengelolaan risiko
7) Faktor pendukung sistem manajemen keamanan informasi
8) Implementasi sistem manajemen keamanan informasi
9) Evaluasi kinerja sistem keamanan informasi
10) Tindakan korektif
11) Lampiran A: daftar kontrol dan tujuan

Pada tulisan ini akan lebih difokuskan bagaimana merencanakan manajemen keamanan informasi berdasarkan penilaian resiko dan pengelolaannya.



Gbr 1. Elemen manajemen resiko

B. ISO 27005:2018

ISO 27005 merupakan kerangka yang menjelaskan metodologi manajemen risiko. Dimana , manajemen resiko merupakan salah satu konsep kunci dari ISO 27001 khususnya untuk mengidentifikasi risiko (bagian ke-6) dan kemudian menggabungkannya dengan risiko yang berpotensi dihadapi. Standar ISO 27005 ini terdiri dari 55 halaman, dan berlaku untuk semua jenis organisasi [2]

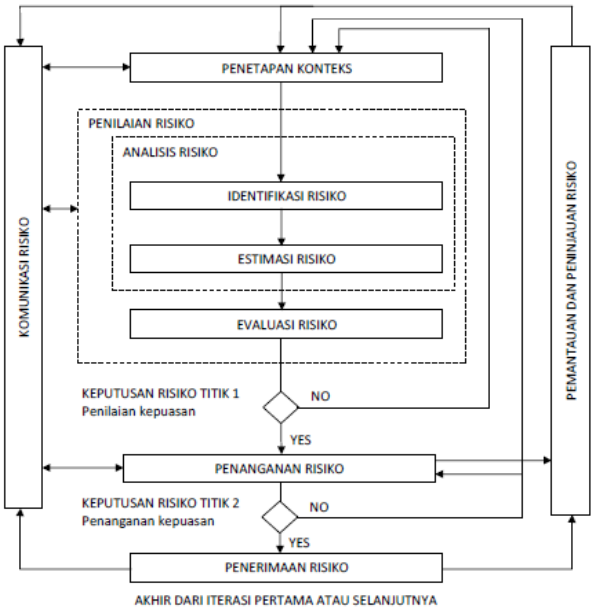
ISACA [1] mendefiniskan bahwa manajemen risiko TI adalah penerapan metode manajemen risiko pada teknologi informasi untuk mengelola risiko TI, yaitu risiko bisnis yang terkait dengan penggunaan, kepemilikan, operasi, keterlibatan, pengaruh dan adopsi TI dalam suatu perusahaan atau organisasi. Manajemen risiko TI merupakan komponen dari sistem manajemen risiko perusahaan yang lebih luas. Kegiatan melakukan identifikasi, pemeliharaan, dan peningkatan berkelanjutan dari Sistem Manajemen Keamanan Informasi (SMKI) merupakan sebuah bukti bahwa perusahaan telah menggunakan metode yang sistematis untuk mengidentifikasi, menilai, dan mengelola risiko keamanan informasi.

Resiko TI tidak hanya mencakup resiko yang memiliki dampak negatif dari operasi dan layanan yang dapat menyebabkan kehancuran atau devaluasi organisasi akan tetapi juga resiko yang memiliki manfaat yang dapat menciptakan perbaikan organisasi akibat tidak dimanfaatkannya peluang dalam pembaruan teknologi untuk kegiatan pengelolaan bisnis atau proyek TI seperti kelebihan pengiriman atau keterlambatan, yang mungkin bias memicu perusahaan untuk melakukan inovasi teknologi. Dalam dokumen OHSAS 18001:2007 didefinisikan bahwa resiko adalah kombinasi dari kemungkinan suatu peristiwa atau paparan berbahaya dan tingkat keparahan cedera atau masalah kesehatan yang mungkin timbul dari peristiwa atau paparan tersebut. Jika dikaitkan dengan asset teknologi informasi maka resiko IT merupakan gambaran komprehensif tentang semua risiko yang terkait dengan penggunaan teknologi informasi di bidang TI, dan menyediakan pendekatan umum untuk manajemen risiko, mulai dari hilir hingga masalah budaya dan operasional. Secara umum dapat diformulasikan :

$$Risk = Threat\ Likelihood * Magnitude\ of\ Impact \quad (1)$$

Dalam kerangka kerja ISO 27005:2018 , proses manajemen resiko dapat digambarkan seperti Gambar 2.[2] Seperti yang ditunjukkan pada Gambar 2, proses manajemen risiko keamanan informasi dapat diulang untuk menilai risiko dan/atau melakukan tindakan manajemen risiko. Pendekatan berulang penilaian risiko ini dapat meningkatkan kedalaman dan detail penilaian di setiap iterasi. Pendekatan iteratif ini memberikan keseimbangan dalam mengurangi waktu dan upaya yang dihabiskan untuk mengidentifikasi tindakan pengendalian serta penilaian risiko yang tepat. Ketika konteks masalah sudah ditentukan sebelumnya, maka penilaian risiko dalam dilakukan kemudian. Jika proses ini sudah dapat memberikan informasi yang cukup dan efektif untuk melakukan tindakan yang diperlukan dalam mengurangi risiko ke level yang dapat diterima, maka tugas dapat diselesaikan dan perlakuan risiko dapat ditentukan. Jika tidak ada informasi yang cukup, maka iterasi lain harus dilakukan.

ISSN : 2549-869X



Gbr 2. Proses Manajemen Resiko Keamanan Informasi

TABEL I
KESESUAIAN ANTARA KERANGKA ISO 27001:2013 DENGAN ISO 27005:2018

ISO 27001 :2013	ISO 27005:2018
Plan	• Menetapkan konteks • Penilaian risiko • Mengembangkan rencana penanganan risiko • Penerimaan risiko
Do	Penerapan rencanan penanganan risiko
Check	Pemantauan dan peninjauan berkala terhadap risiko
Action	Meningkatkan dan memelihara Proses Manajemen Risiko Keamanan Informasi

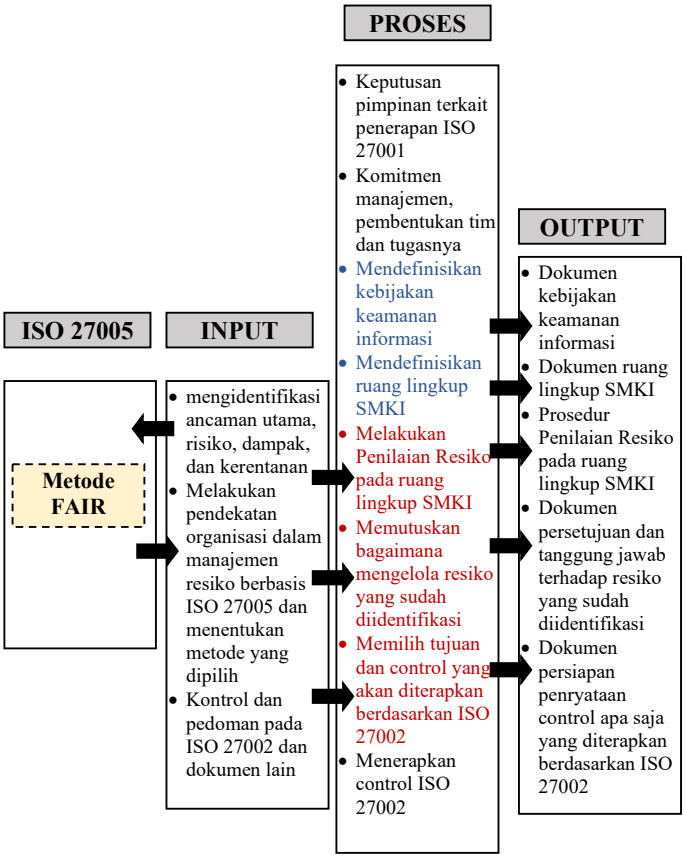
IV. METODOLOGI PENILAIAN RESIKO TI

Pada ISO / IEC 27001, tidak menyediakan metodologi khusus untuk manajemen risiko yang terkait dengan keamanan informasi. Sehingga setiap organisasi dapat menentukan pendekatan yang dipilih berdasarkan perjanjian internal organisasi berdasarkan ruang lingkup manajemen keamanan informasi, konteks manajemen risiko, atau jenis sektor organisasi. Untuk alasan ini, maka penelitian ini menggunakan analisis faktor risiko informasi (FAIR) sebagai metode identifikasi resiko. Dengan demikian kaitan antara ISO 27001, ISO 27005 dan FAIR adalah jika didalam 27001 dijelaskan deskripsi proses untuk sistem manajemen keamanan informasi dan ISO / IEC 27005 menyediakan metodologi analisis risiko, maka metode FAIR digunakan untuk menganalisis risiko dalam konteks ISO / IEC 27005 dan SMKI. Secara model dapat digambarkan seperti pada gambar

3. Pada klausul 4.2.1 dalam dokumen ISO / IEC 27001 disebutkan point penting untuk bagian manajemen risiko dari SMKI yaitu [4] :

a) Menentukan pendekatan penilaian risiko organisasi
b) Identifikasi risiko
c) Menganalisis dan mengevaluasi risiko
d) Mengidentifikasi dan mengevaluasi opsi untuk perawatan risiko
e) Pilih tujuan kontrol dan kontrol untuk perawatan risiko
f) Dapatkan persetujuan manajemen dari risiko residual yang diusulkan

Poin ini menguraikan proses umum untuk mengelola risiko pada level manajemen tingkat atas dalam perusahaan. Sementara itu ISO / IEC 27005 menetapkan secara lebih rinci pengelolaan risiko tanpa memberikan spesifikasi atau mengidentifikasi metodologi untuk menentukan tingkat risiko. Sehingga FAIR dapat digunakan sebagai metodologi untuk mencapai proses yang dijelaskan dalam dokumen ISO baik 27001 dan 27005 khususnya mengidentifikasi risiko dan menganalisis serta mengevaluasi risiko. [6]



Gbr 3. Penggunaan ISO / IEC 27005 dan FAIR dalam Proses Pengembangan SMKI berbasis ISO / IEC 27001

Berdasarkan gambar 2 tentang gambaran detil tentang proses manajemen resiko, metode FAIR berada pada kegiatan

penilaian resiko yang terdiri dari tahapan identifikasi resiko, estimasi resiko dan evaluasi resiko. Secara taksonomi dapat dijelaskan dalam table 2.

TABEL II
METODE FAIR DALAM PENILAIAN RESIKO BERBASIS ISO 27005:2018

ISO 27005:2018	FAIR
Analisis Resiko	Keseluruhan komponen dalam taksonomi FAIR
Identifikasi Resiko	Tahap 1.Tahapan ini mencakup kegiatan mengidentifikasi skenarion komponen resiko yang beupa" • Mengidentifikasi aset yang beresiko • Menidentifikasi ancaman
Evaluasi dan Estimasi Kapan terjadinya Resiko	Tahap 2 , yaitu : • Mengevaluasi *Loss Event Frequency* (LEF) • Memperkirakan *Threat Event Frequency* (TEF) • Memperkirakan *Threat Capability* (TCap) • Memperkirakan *Control Strength* (CS) • Menurunkan *Vulnerability* (Vuln) • Menurunkan *Loss Event Frequency* (LEF)
Evaluasi dan Estimasi Berapa besar kerugian jika terjadi Resiko	Tahap 3 , yaitu : • Mengevaluasi *Probable Loss Magnitude* (PLM) • Memperkirakan *worst-case loss* • Memperkirakan *Probable Loss Magnitude (PLM)*
Keputusan	Tahap 4 , yaitu menurunkan dan menjelaskan semua resiko

V. PEMBAHASAN

Dalam bagian ini akan dijelaskan bagaimana strategi penggunaan metode FAIR untuk sistem manajemen keamanan informasi (SMKI). Berdasarkan tahapan yang dijelaskan pada tabel 2, maka langkah-langkah yang dilakukan dalam proses penilaian resiko adalah sebagai berikut :

a. Tahap 1
Dalam tahapan ini akan dilakukan identifikasi komponen resiko yang berupa aset dan ancaman. Dalam mengidentifkasi aset maka harus dapat menjawab pertanyaan :
(1) Aset apa yang beresiko?. Untuk menjawabnya maka dapat berupa sistem, aplikasi perangkat lunak, database, jaringan atau data center disesuaikan dengan ruang lingkup SMKI.
(2) Ancaman apa yang terkait dengan resiko?. Untuk menjawabnya dapat dimulai dari karakteristik organisasi dan komunitas apa yang mungkin terlibat. Misalnya komunitas hacker, pihak internal, pihak ketiga yang berkaitan dengan TI atau kasus kriminalitas lain.

b. Tahap 2
Tahapan ini dilakukan evaluasi dan estimasi terhadap frekwensi terjadinya resiko. Persamaan (1) menyatakan bahwa resiko merupakan perkalian antara peluang terjadinya ancaman (*threat likelihood)* dan besarnya dampak (*magnitude of impact*). Oleh karena itu kedua elemen tersebut harus diubah dalam bentuk kuantitatif. Nilai skala kuantitatif dari elemen kemungkinan terjadinya ancaman dapat dilihat pada tabel 3.

TABEL III
RATING FREKWENSI KEJADIAN ASSET YANG BERESIKO

Rating	Keterangan
Sangat Tinggi (ST)	Lebih dari 100 kali per tahun
Tinggi (T)	Antara 10 sampai 100 kali per tahun
Sedang (S)	Antara 1 sampai 10 kali per tahun
Rendah (R)	Antara 0.1 sampai 1 kali pertahun
Sangat Rendah (SR)	Kurang dari 0.1 kali per tahun

Selanjutnya dilakukan identifikasi ancaman dari semua resiko terhadap asset dikonversi dengan nilai rating pada tabel 3. Kemudian diidentifikasi kemampuan dalam menhadapi ancaman terhadap asset dengan menggunakan tabel 4.

TABEL IV
RATING KEMAMPUAN MENGHADAPI ANCAMAN

Rating	Keterangan
Sangat Tinggi (ST)	Top 2% dibandingkan semua nacaman
Tinggi (T)	Top 16% dibandingkan semua ancaman
Sedang (S)	Antara *top* 16% dan Bottom 16% dari semua ancaman
Rendah (R)	Dibawah *bottom* 16% dibandingkan semua ancaman
Sangat Rendah (SR)	Dibawah *bottom* 2% dari semua ancaman

Kemudian perlu dilakukan pengukuran daya tahan organisasi dalam menghadapi ancaman. Ukurannya dapat menggunakan table 5.

TABEL V
RATING DAYA TAHAN ORGANISASI DALAM MENGAHDAPI ANCAMAN

Rating	Keterangan
Sangat Tinggi (ST)	Mampu melindungi aset dari ancaman kecuali top 2% dari rata-rata ancaman
Tinggi (T)	Mampu melindungi aset dari ancaman kecuali top 16 % dari rata-rata ancaman
Sedang (S)	Mampu melindungi aset dari rata-rata ancaman
Rendah (R)	Hanya melindungi aset dari *bottom* 16% dibandingkan semua ancaman
Sangat Rendah (SR)	Hanya melindungi aset dari *bottom* 2% dibandingkan semua ancaman

Selanjutnya dapat dilakukan analisis skala nilai kerentanan dan frekwensi terjadinya ancaman (*threat likelihood*).

TABEL VI
MATRIX SKALA KERENTANAN

Kerentanan	Daya Tahan menghadapi ancaman					
Kemampuan menghadapi ancaman		SR	R	S	T	ST
	ST	**ST**	**ST**	**ST**	**T**	**M**
	T	**ST**	**ST**	**T**	**M**	**R**
	S	**ST**	**T**	**M**	**R**	**SR**
	R	**T**	**M**	**R**	**SR**	**SR**
	SR	**M**	**R**	**SR**	**SR**	**SR**

TABEL VII
MATRIX SKALA *LIKELIHOOD*

Likelihood	Kerentanan					
Frekwensi terjadinya ancaman		SR	R	S	T	ST
	ST	S	T	ST	ST	ST
	T	R	S	T	T	T
	S	SR	R	S	S	S
	R	SR	SR	R	R	R
	SR	SR	SR	SR	SR	SR

Dimana nilai likelihood yang paling tinggi bernilai 100%.

c. Tahap 3

Setelah itu dilanjutkan dengan penilaian terhadap besarnya dampak kerugian yang disebabkan dari resiko. Skala yang digunakan untuk mengukur dampak kerugian dari sebuah resiko dapat dilihat pada table 8.

TABEL VIII
SKALA DAMPAK DARI KERUGIAN

Rating	Keterangan
Parah (ST)	Lebih dari 100 M
Tinggi (T)	Antara 10 M – 100 M
Signifikan (S)	Antara 1 M – 10 M
Sedang (M)	150 Juta – 1 M
Rendah (R)	10 Juta – 150 Juta
Sangat Rendah (SR)	Dibawah 10 Juta

d. Tahap 4

Pada tahap terakhir dilakukan pengukuran nilai resiko yang ada dengan membuat matrik hubungan antara likelihood dan dampak resiko. Matrik yang digunakan dapat dilihat pada table 9.

TABEL IX
MATRIK RISIKO

Resiko	Frekwensi (*likelihood*)					
Dampak (*Impact*)		SR	R	S	T	ST
	ST	T	T	K	K	K
	T	S	T	T	K	K
	S	S	S	T	T	K
	M	R	S	S	T	T
	R	R	R	S	S	S
	SR	R	R	S	S	S

Sebagai ilustrasi untuk menghitung resiko digunakan data seperti table 10.

TABEL X
CONTOH HASIL PENILAIAN RESIKO KEAMANAN INFORMASI

Pengamat-an	Sumber	Likeli-hood	Impact	Resiko	Rekomendasi
Password pengguna dapat dibobol	Hacker	S	S	T	Kombinasi password sebaiknya dicek kompleksitasnya yang terdiri dari kombinasi huruf, angka dan karakter khusus serta case sensitive untuk huruf besar dan kecil
SQL Injection	Hacker	S	S	T	Dilakukan validasi terhadap semua header , cookies, sintak query serta hiiden fields sebagai upaya untuk melawan adanya operasi sql yang tidak diijinkan.
Database corrupted	Hacker	T	S	T	Memastikan semua parameter divalidasi sebelum digunakan
Server menjalan-kan service yang tidak diperlukan	Service yang tidak perlu/aplikasi mal-ware	S	S	T	Melakukan konfigurasi sistemulang dan mematikan /membuang semua service yang tidak diperlukan
Belum memiliki dokumen Disaster Recovery Plan	Tim personal yang bertang gung jawab terha-dap penang-gulang-an resiko/ bencana	S	T	T	Mengembangkan dan melakukan simulasi oe gujian terhadap dokumen disaster recovery plan

Hasil analisis resiko tersebut akan menjadi input dari proses kebijakan manajemen dalam komitmen mengimpelemtasikan SMKI berdasarkan kerangka 27001:20013.

VI. PENUTUP

Kesimpulan yang diperoleh dari kajian ini adalah bahwa dalam rangka menerapkan tata kelola TI yang salah satunya adalan menajemen resiko TI dapat menggunakan kerangka 27005:2018 yang didalamnya dapat diintegrasikan dengan metode FAIR sehingga membantu dalam mendapatkan prioritas resiko yang akan disiapkan scenario pencegahan dan pemulihannya.

REFERENSI

[1] ISACA, *The Risk IT Framework Excerpt,* Illiniois USA: ISACA,2009.
[2] ISO/IEC, *Information technology -- Security techniques-Information security risk management.* ISO/IEC FIDIS 27005:2018

[3] ISO/IEC, *Information technology — Security techniques — Information security management systems — Requirements*.ISO/IEC FIDIS 27001:2013
[4] Jack Freund, Jack Jones, *Measuring and Managing Information* Risk, Butterworth-Heinemann,2015
[5] James Broad, *Risk Management Framework : A Lab-Based Approach to Securing Information Systems*, 1st Edition, Butterworth-Heinemann, Syngress, Elsevier, 2013
[6] The Open Group, *FAIR – ISO/IEC 27005 Cookbook*, Open Group, United Kingdom, 2010