Manajemen Risiko Teknologi Informasi Pada Penerapan E-Recruitment Berbasis ISO 31000:2018 Dengan FMEA (Studi Kasus PT Pertamina)

Hanafi Indra Pribadi[a,*], Ernastuti[b]

[a] Jurusan Sistem Informasi Bisnis, Program Magister Manajemen Sistem Informasi, Universitas Gunadarma, Jalan Kenari I, Kenari, Kec. Senen, Kota Jakarta Pusat, DKI Jakarta.
[b] Fakultas Teknologi Industri Universita Gunadarma, Jalan Margonda Raya No. 100, Depok, Jawa Barat.

Naskah Diterima : 31 Desember 2019; Diterima Publikasi : 21 Februari 2020
DOI : 10.21456/vol10iss1pp28-35

Abstract

Increasing the efficiency of time and human resources in the process of recruiting PT. Pertamina (Persero) to carry out its business processes that are spread throughout Indonesia is very much needed by implementing a website-based online recruitment system. Increased efficiency is obtained from a system that runs without constraints, while the weaknesses (vulnerabilities) in a system will cause great threats to the company, then the risk management of information technology on the application of the E-Recruitment system needs to be done by referring to ISO 31000: 2018 and risk assessment to get a Risk Priority Number (RPN), which is the priority of risk treatment for each risk attribute using the FMEA (Failure Modes and Effects Analysis) method based on ISO 31010: 2009 with the aim of knowing and assessing how much the threats and risks in an information system can become consideration of company stakeholders in implementing the system. Risks obtained in this study are 3 types of potential risks and 28 risk attributes, after a risk assessment has been obtained, the results are obtained that 7 risk attributes require special attention in the process of implementing the system so that it can run well in the future.

Keywords : Risk Management; ISO 31000; FMEA; Risk Reduction.

Abstrak

Peningkatan efisiensi waktu dan sumber daya manusia dalam proses perekrutan pegawai PT. Pertamina (Persero) untuk melaksanakan proses bisnisnya yang tersebar di seluruh wilayah Indonesia sangatlah dibutuhkan yakni dengan menerapkan sistem rekrutmen *online* berbasis *website*. Peningkatan efisiensi didapatkan dari sistem yang berjalan tanpa kendala, adapun kelemahan (*vulnerabilities*) pada sebuah sistem akan menimbulkan ancaman (*threats*) yang besar bagi perusahaan, maka manajemen risiko teknologi informasi pada penerapan sistem *E-Recruitment* perlu dilakukan dengan mengacu pada ISO 31000:2018 serta penilaian risiko untuk mendapatkan *Risk Priority Number* (RPN) yakni priotitas perlakuan risiko pada setiap atribut risiko dengan metode FMEA (*Failure Modes and Effects Analysis*) berbasis ISO 31010:2009 dengan tujuan mengetahui dan menilai seberapa besar ancaman dan risiko pada sebuah sistem informasi hingga dapat menjadi pertimbangan *stakeholder* perusahaan dalam menerapkan sistem tersebut. Risiko yang didapatkan pada penelitian ini adalah sebanyak 3 jenis potensial risiko dan 28 atribut risiko, setelah dilakukan penilaian risiko maka didapatkan hasil bahwa 7 atribut risiko memerlukan perhatian khusus dalam proses penerapan sistem agar dapat berjalan dengan baik untuk kedepannya.

Keywords : Manajemen Risiko; ISO 31000; FMEA; Perlakuan Risiko.

1. Pendahuluan

PT. Pertamina (Persero) merupakan perusahaan negara yang melakukan kegiatan usaha migas pada Sektor Hulu hingga Sektor Hilir, melalui UU No.8 tahun 1971, pemerintah mengatur peran Pertamina untuk menghasilkan dan mengolah migas dari ladang-ladang minyak serta menyediakan kebutuhan bahan bakar dan gas di Indonesia.

Pelaksanaan proses bisnis yang membutuhkan pegawai dalam jumlah banyak dari putra-putri terbaik Indonesia maka dibutuhkan penerapan sebuah sistem informasi terpadu perekrutan pegawai PT. Pertamina (Persero) yang pada penerapannya membutuhkan tingkat kematangan tinggi agar efisien dalam prosesnya, membuat kinerja karyawan semakin baik dan terstruktur serta semua data yang terproses dapat terkendali secara sistem sehingga menjadi fakta konkrit di kemudian hari. Namun untuk mengetahui efisiensi waktu dan sumber daya dalam penerapan sistem, akan sangat penting dilakukannya analisa manajemen risiko terhadap

*) Penulis korespondensi: hanafindra@gmail.com

sistem tersebut agar terhindar dari kelemahan dan ancaman yang tidak diinginkan setelah penerapan sistem, proses pengelolaan data yang kurang baik melalui sebuah sistem akan menimbulkan permasalahan berupa kelemahan (*vulnerabilities*) baik secara pertanggungjawaban data maupun perusahaan sehingga akan menimbulkan berbagai ancaman (*threats*). Risiko yang timbul akibat kesalahan dalam penerapan sistem informasi tersebut akan berkurang seperti proses dalam aplikasi yang belum stabil, pemrosesan data yang tidak dapat dilakukan dalam jumlah banyak sehingga harus melakukan pemrosesan data satu per satu, hal ini menyebabkan kemungkinan proses yang akan memakan waktu lebih lama dan akan terdapatnya redudansi data.

Risiko dan ancaman dapat dihadapi dengan menyusun suatu pengelolaan (manajemen) risiko yang baik sebagai pertimbangan kepada perusahaan agar dapat mengambil keputusan dengan tepat. Guna memanajemen risiko pada penelitian ini berdasarkan pada ISO 31000:2018 dan penilaian risiko dengan model FMEA (*Failure Modes and Effects* Analysis) dari ISO 31010:2009 untuk mendapatkan *Risk Priority Number* (RPN) sebagai langkah pertimbangan dalam mengambil tindakan dari risiko yang didapat.

FMEA merupakan sebuah metodologi yang digunakan untuk mengevaluasi kegagalan terjadi dalam sebuah sistem, desain, proses, atau pelayanan (*service*). Identifikasi kegagalan potensial dilakukan dengan cara pemberian nilai atau skor masing – masing moda kegagalan berdasarkan atas tingkat kejadian (*occurrence*), tingkat keparahan (*severity*), dan tingkat deteksi (detection) (Stamatis D.H, 1995).

Secara umum, terdapat dua tipe FMEA desain dan FMEA proses. Pada FMEA desain, pengamatan difokuskan pada desain produk. Sedangkan FMEA proses, pengamatan difokuskan pada kegiatan proses produksi. Metode yang diterapkan pada penelitian ini adalah FMEA proses, karena pengamatan hanya dilakukan pada kegiatan proses penerapan sistem yang sedang berlangsun. Tujuan penerapan metode ini adalah untuk meminimasi kemungkinan terjadi cacat.

Tujuan manajemen risiko teknologi informasi pada penelitian ini adalah untuk mengetahui seberapa besarnya ancaman dan risiko sebuah sistem terpadu dalam proses rekrutmen calon pegawai, sebagai pertimbangan kepada pengambilan keputusan pada level manajemen perusahaan dalam penerapan sistem informasi tersebut dan untuk menentukan sumber daya yang dikeluarkan dalam proses rekrutmen calon pegawai berdasarkan penerapan sistem.

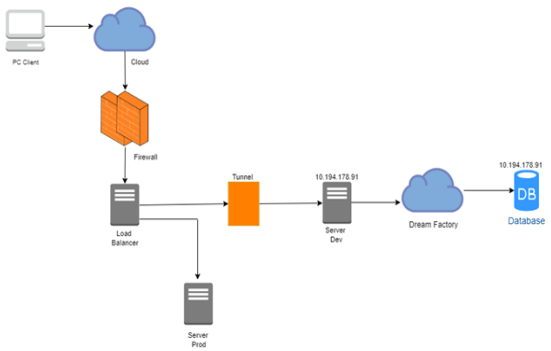
2. Kerangka Teori

2.1. Sistem Informasi Rekrutmen

Sistem informasi merupakan aktivitas kolaborasi beberapa komponen yang melibatkan teknologi informasi berupa perangkat keras dan perangkat lunak serta orang (pengguna), data, dan jaringan dalam pengumpulan dan penyebaran data tentang suatu tujuan tertentu dalam mendukung proses bisnis.

Proses rekrutmen bertujuan untuk mendapatkan calon pegawai yang memiliki kredubilitas tinggi dengan menggunakan prosedur terapan dengan proses penyeleksian yang valid dan sesuai persyaratan yang diterapkan kedalam aplikasi sistem informasi. Prosedur rekrutmen akan berpengaruh besar pada kualitas dan jenis keterampilan yang dimiliki pegawai baru dengan menerapkan kode etik rekrutmen yang direkomendasikan untuk memastikan agar setiap pelamar mendapatkan perlakuan yang adil dan memenuhi persyaratan hukum terkait dengan peluang pekerjaan yang setara.

Adapun topologi infrastruktur sistem *E-Recruitment* PT. Pertamina (Persero) adalah sebagai berikut:



Gambar 1. Rancangan Infrastruktur *E-Recruitment* PT. Pertamina

Berdasarkan gambar rancangan infrastruktur sistem diatas diketahui bahwa terdapat 3 *server* utama yang berfungsi sebagai *server production* yang terhubung ke *tunnel* sebagai mediasi ke *server development* yang terhubung dengan *middleware* API basis data dengan *dream factory*, *server development*, dan *server load balancer* sebagai penyeimbang struktur aplikasi jika sewaktu-waktu perangkat mengalami gangguan, dengan demikian maka diperlukan proses analisis dan manajemen risiko.

2.2. Risiko

Risiko adalah potensi bahaya yang mungkin timbul dari beberapa penerapan proses pada saat ini atau dari beberapa peristiwa di masa depan. Risiko hadir dalam setiap aspek kehidupan kita dan banyak disiplin ilmu yang berbeda tergantung pada risiko yang berlaku dalam sebuah pemrosesan. Dari perspektif keamanan Teknologi Informasi (TI), manajemen risiko adalah proses memahami dan

menanggapi faktor-faktor yang dapat menyebabkan kegagalan dalam kerahasiaan, integritas atau ketersediaan sistem informasi. Adapun risiko keamanan TI adalah kesalahan yang terjadi pada suatu proses yang terkait dengan informasi yang dihasilkan dari beberapa peristiwa yang disengaja atau tidak disengaja yang berdampak negatif pada tahap pemrosesan atau informasi terkait.

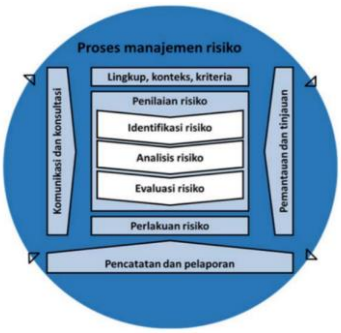
Bahaya (hazard) dapat didefenisikan sebagai keadaan yang menimbulkan atau meningkatkan terjadinya chance of loss dari suatu bencana tertentu. Hazard (bahaya) adalah suatu keadaan yang dapat memperbesar kemungkinan terjadinya suatu peril (bencana). Pengertian tersebut dapat diperluas meliputi berbagai keadaan yang dapat menimbulkan suatu kerugian. Bahaya dapat diklasifikasikan dalam 4 bentuk yaitu (Herman Darmawi 2014:22) :

1. *Physical Hazard*, adalah suatu kondisi yang bersumber pada karakteristik secara fisik dari suatu objek lingkungan yang dapat memperbesar terjadinya suatu kerugian.
2. *Moral Hazard*, adalah suatu kondisi yang bersumber dari orang yang bersangkutan yang berkaitan dengan sikap mental atau pandangan hidup serta kebiasaannya yang dapat memperbesar kemungkinan terjadinya suatu bencana ataupun suatu kerugian.
3. *Morale Hazard*, adalah bahaya yang ditimbulkan oleh sikap ketidak hati-hatian dan kurangnya perhatian sehingga dapat meningkatkan terjadinya kerugian.
4. *Legal Hazard*, yaitu seringkali berdasarkan peraturan-peraturan ataupun perundang-undangan yang bertujuan melindungi masyarakat justru diabaikan ataupun kurang diperhatikan sehingga dapat memperbesar terjadinya suatu peril.

2.3. ISO 31000:2018

ISO (*International Organization for Standardization*) merupakan federasi badan standarisasi nasional bagi seluruh dunia. Pekerjaan yang membutuhkan persiapan terkait dengan standarisasi internasional biasanya dilakukan melalui komite teknis ISO sesuai dengan kebutuhan teknis yang distandarisasi, ISO 31000:2018 merupakan sebuah standar internasional yang disusun dengan tujuan memberikan prinsip dan panduan generik untuk penerapan manajemen risiko.

Proses manajemen risiko melibatkan penerapan sistematis dari kebijakan, prosedur dan praktik pada aktivitas komunikasi dan konsultasi, penetapan konteks, serta penilaian, peninjauan hingga pelaporan risiko (Gambar 2).



Gambar 2. Proses manajemen risiko

2.4. FMEA (Failure Modes and Effects Analysis)

Analisis FMEA merupakan suatu teknik analisa bahaya secara kualitatif yang dapat digunakan untuk mengidentifikasi bagaimana suatu peralatan, fasilitas, atau sistem dapat gagal serta akibat yang dapat ditimbulkan (CCPS, 1992). Hasil dari identifikasi bahaya menggunakan metode FMEA yaitu berupa nilai RPN (Risk Priority Number), kemudian akan diketahui komponen mana yang memiliki nilai RPN paling tinggi.

Metode FMEA dilakukan untuk menganalisa potensi bahaya/kegagalan pada setiap komponen sistem. Potensi bahaya yang teridentifikasi akan dikelompokkan menurut besarnya potensi bahaya dan kemungkinan efek yang terjadi terhadap komponen sistem. Adapun manfaat dan tujuan yang dapat dicapai dari penerapan FMEA dalam manajemen risiko adalah:

a. Untuk mengidentifikasi mode kegagalan dan tingkat keparahan dampaknya.
b. Untuk mengidentifikasi karakteristik kritis dan signifikan.
c. Untuk mengurutkan pesanan desain potensial dan definisi proses.
d. Mengidentifikasi defisiensi proses, sehingga para engineer dapat berfokus pada pengendalian untuk mengurangi output sistem yang tidak sesuai dengan yang diinginkan atau pada metode untuk meningkatkan deteksi pada produk yang tidak sesuai tersebut.

3. Metode

Pendekatan penelitian dalam penulisan ini menggunakan metode verifikatif dalam menentukan atribut risiko berdasarkan ISO 31000:2018 dan pembobotan risiko menggunakan metode FMEA. Metode Verifikatif (Kuantitatif) menurut Rosgandika Mulyana (2005:8) adalah : “Metode ilmiah untuk pencapaian validitas yang tinggi reabilitasnya dan mempunyai peluang kebenaran ilmiah yang tinggi, sifat kuantitatif memberi bobot (*rating*), peringkat (*rangking*), atau skor (*scoring*)”. Dalam penggunaan metode verifikatif, maka diperlukan beberapa tahap diantaranya:

3.1. Pengumpulan Data

Pada tahap pengumpulan data, penulis melakukannya dengan menyebar kuesioner *online* berbasis *google form* terkait risiko penerapan teknologi informasi yang telah dianalisis sebelumnya untuk kemudian dilakukan pengujian validitas dan reliabilitas dengan jumlah responden minimal sebanyak 30 responden dan maksimal 500 responden (Uma, 2006). Instrumen yang valid maka dilakukan pembobotan risiko dengan metode FMEA oleh pihak manajemen divisi IT Development di perusahaan pengembang sistem E-Recruitment tersebut.

3.2. Pengolahan dan Analisis Data

Pada tahap analisis dengan FMEA dilakukan identifikasi penilaian risiko atau *Risk Priority Number* (RPN) terhadap sistem E-Recruitment yang bertujuan untuk mengetahui tingkat risiko bahaya yang paling kritis dengan memperhatikan risiko yang memiliki tingkat keparahan yang tinggi dan memiliki dampak atau keparahan yang besar serta kemampuan deteksi untuk mencegah terjadinya dampak yang ditimbulkan. Nilai RPN didapatkan melalui hasil perkalian antara severity (S), occurance (O), dan detection (D). Berikut acuan nilai dalam menentukan keparahan risiko (Sumber: McDermott, 2009).

Tabel 1. Tingkat Dampak / Keparahan (Severity (S))

Rank	*Severity*	Deskripsi
10	Berbahaya tanpa peringatan	Kegagalan sistem yang menghasilkan efek sangat berbahaya
9	Berbahaya dengan peringatan	Kegagalan sistem yang menghasilkan efek berbahaya
8	Sangat tinggi	Sistem tidak beroperasi
7	Tinggi	Sistem beroperasi tetapi tidak dapat dijalankan secara penuh
6	Sedang	Sistem beroperasi dan aman tetapi mengalami penurunan performa sehingga mempengaruhi *output*
5	Rendah	Mengalami penurunan kinerja secara bertahap
4	Sangat rendah	Efek yang kecil pada performa sistem
3	Kecil	Sedikit berpengaruh pada kinerja sistem
2	Sangat kecil	Efek yang diabaikan pada kinerja sistem
1	Tidak ada efek	Tidak ada efek

Sedangkan acuan nilai yang digunakan dalam menentukan kemungkinan kejadian risiko terhadap sistem yang dianalisa. (Sumber: McDermott, 2009):

Tabel 2. Tingkat kemungkinan kejadian (*Occurrence*)

Rank	*Occurrence*	Deskripsi
10	Sangat tinggi	≥ 1 kejadian / shift
9		≥ 1 kejadian / hari
8	Tinggi	≥ 1 kejadian / 2-3 hari
7		≥ 1 kejadian / minggu
6	Sedang	≥ 1 kejadian / 2 minggu
5		≥ 1 kejadian / bulan
4	Rendah	≥ 1 kejadian / 4 bulan
3		≥ 1 kejadian / ½ tahun
2	Tidak ada efek	≥ 1 kejadian / tahun
1		≥ 1 kejadian / > 1 tahun

.

Adapun acuan nilai yang digunakan dalam menentukan tingkat deteksi penyebab risiko terhadap sistem yang dianalisa (Sumber: McDermott, 2009).

Tabel 3. Tingkat Deteksi Penyebab (*Detection* (D))

Rank	*Detection*	Deskripsi
10	Tidak pasti	Pengecekan akan selalu tidak mampu untuk mendeteksi penyebab kegagalan.
9	Sangat kecil	Pengecekan memiliki kemungkinan *very remote* untuk mampu mendeteksi penyebab kegagalan.
8	Kecil	Pengecekan memiliki kemungkinan "*remote*" untuk mampu mendeteksi penyebab kegagalan.
7	Sangat rendah	Pengecekan memiliki kemungkinan sangat rendah untuk mampu mendeteksi penyebab kegagalan.
6	Rendah	Pengecekan memiliki kemungkinan rendah untuk mampu mendeteksi penyebab kegagalan.
5	Sedang	Pengecekan memiliki kemungkinan "*moderate*" untuk mendeteksi penyebab kegagalan.
4	Menengah keatas	Pengecekan memiliki kemungkinan "*moderate high*" untuk mendeteksi penyebab kegagalan.
3	Tinggi	Pengecekan memiliki kemungkinan tinggi untuk mendeteksi penyebab kegagalan.
2	Sangat tinggi	Pengecekan memiliki kemungkinan sangat tinggi untuk mendeteksi penyebab kegagalan.
1	Hampir pasti	Pengecekan akan selalu mendeteksi penyebab kegagalan.

3.3. Skala Pengukuran

Skala pengukuran merupakan sebuah acuan yang digunakan untuk menentukan interval yang terdapat dalam satuan alat ukur guna menghasilkan data

kuantitatif, adapun dalam penelitian ini menggunakan pengukuran nominal dari kategori responden para pekerja bidang Teknologi Informasi dari segala jenis pekerjaan didalamnya, seperti analis sistem, *programmer*, bisnis analis, data analis, IT infrastruktur dan jaringan, IT Tester serta guru komputer dengan ukuran pernyataan pada Tabel 4.

Tabel 4. Skala Pengukuran Pernyataan

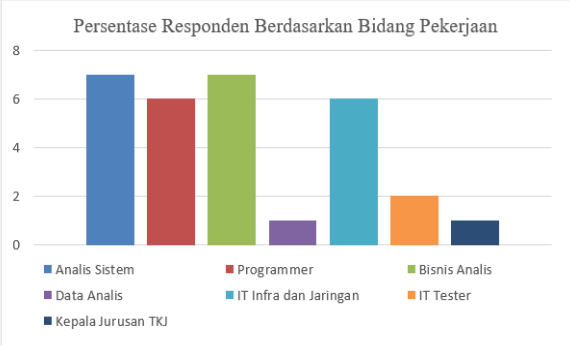
Ukuran Pernyataan	Bobot Nilai
Sangat setuju/ Sangat tinggi/ Sangat banyak/ Selalu	5
Setuju/ Tinggi/ Banyak/ Sering	4
Netral/ Kadang-kadang/ Cukup	3
Tidak setuju/ Rendah/ Sedikit/ Hampir tidak pernah	2
Sangat tidak setuju/ Sangat rendah/ Sangat sedikit/ Tidak pernah	1

4. Hasil dan Pembahasan

Manajemen risiko teknologi informasi berdasarkan ISO 31000:2018 mengacu pada prosesnya yakni melalui beberapa tahap, diantaranya:

4.1. Identifikasi Risiko

Adapun identifikasi risiko sebagai variabel penelitian adalah dengan menggunakan standarisasi dari *framework* NIST SP 800-30 terkait dengan identifikasi risiko teknologi informasi untuk dilakukan pengumpulan data kuesioner dari populasi responden yang dilakukan, dapat dijabarkan bahwa karakteristik responden berasal dari jenis kelamin pria dan wanita dengan usia dari minimal pekerja sesuai regulasi pemerintah yakni 20 tahun serta berbagai profesi pekerjaan dengan bidang teknologi informasi pada terteragrafik Gambar 4.



Gambar 4. Grafik responden penelitian berdasarkan bidang pekerjaan

Berdasarkan grafik diatas, responden terbanyak terdapat pada bisnis analis dan sistem analis yang mana semua responden bekerja pada bidang teknologi informasi.

4.1.1. Hasil Uji Validitas dan Reliabilitas

Pengujian validitas instrumen dalam penelitian ini dilakukan pada setiap item pernyataan yang terdiri dari 29 item pernyataan dengan 30 responden dengan rumus uji validitas sebagai berikut:

$$R_{xy} = \frac{n(\sum xy) - (\sum x)(\sum y)}{\sqrt{\{n\sum x^2 - (\sum x)^2\}\{n\sum x^2 - (\sum y^2)\}}}$$

Keterangan:

R_{xy} = Menunjukan indeks korelasi antara dua variabel yang dikorelasikan
R = Koefisien validitas item yang dicari,dua variabel yang dikorelasikan
x = Skor untuk pernyataan yang dipilih
y = Skor total diperoleh dari seluruh item
$\sum x$ = Jumlah skor dalam distribusi x
$\sum y$ = Jumlah skor dalam distribusi y
$\sum x^2$ = Jumlah kuadrat dalam skor distribusi x
$\sum y^2$ = Jumlah kuadrat dalam skor distribusi y
n = Banyaknya responden

Untuk memperoleh nilai yang signifikan, maka dilakukan uji korelasi dengan membandingkan r_{hitung} dan r_{tabel} dengan dk=n-2 dan taraf signifikansi sebesar 5%. Berikut adalah hasil dari uji validitas variabel penelitian tertera pada Tabel 5.

Tabel 5. Hasil Uji Validitas

No	Variabel	R Hit	R Tabel	Hasil
1	Kebakaran/ banjir/ gempa bumi.	0.823	0.374	Valid
2	Perangkat terserang badai/ petir	0.631	0.374	Valid
3	Adanya embun/ debu	0.597	0.374	Valid
4	Kelembaban ruangan	0.554	0.374	Valid
5	Radiasi panas dari musim	0.681	0.374	Valid
6	Pencurian perangkat	0.754	0.374	Valid
7	Kebocoran data dan informasi internal perusahaan	0.816	0.374	Valid
8	Penyalahgunaan hak akses/ User ID	0.791	0.374	Valid
9	*Cybercrime*, terorisme dan vandalisme.	0.827	0.374	Valid
10	Akses *server* yang tidak terotorisasi	0.855	0.374	Valid
11	Mantan *user*/ pegawai yang masih memiliki akses system	0.821	0.374	Valid

No	Variabel	R Hit	R Tabel	Hasil
12	Kesalahan pengguna dalam mengoperasi-kan sistem	0.719	0.374	Valid
13	Kerusakan perangkat keras	0.792	0.374	Valid
14	Server *down*	0.772	0.374	Valid
15	*Overheat*	0.785	0.374	Valid
16	Koneksi jaringan server terputus	0.63	0.374	Valid
17	Terdapat *bugs* sistem	0.709	0.374	Valid
18	Kurangnya kapasitas penyimpanan	0.682	0.374	Valid
19	*Overload*	0.704	0.374	Valid
20	Data *corrupt*	0.716	0.374	Valid
21	Gagal *backup* sistem	0.762	0.374	Valid
22	Kualitas jaringan pengguna memburuk	0.64	0.374	Valid
23	Teknologi yang digunakan kurang memadai	0.642	0.374	Valid
24	Catu daya rusak	0.626	0.374	Valid
25	Sistem tidak dapat melakukan proses dengan ratusan ribu data	0.575	0.374	Valid
26	Sistem tidak *up to date* di sisi pengguna	0.422	0.374	Valid
27	Data yang di-*input* hilang.	0.717	0.374	Valid
28	Kesalahan logika program	0.762	0.374	Valid
29	Data yang diinput tidak sesuai dengan *output*-nya	-0.032	0.374	Invalid

Berdasarkan hasil uji validitas kuesioner terkait risiko TI yang terjadi pada penerapan sistem *E-Recruitment* PT. Pertamina (Persero) adalah 28 valid dengan hasil R hitung berada diatas R tabel untuk 30 responden yakni 0.374. Dengan demikian instrumen risiko yang digunakan dalam penelitian ini adalah sejumlah 28 risiko teknologi informasi.

Adapun uji reliabilitas dengan 28 instrumen penelitian yang valid, menggunakan rumus *Cronbach Alpha* berikut:

$$r_{11} = \frac{n}{n-1}\left(1 - \frac{\sum \sigma_i^2}{\sigma_t^2}\right)$$

Keterangan:

r_{11} = Koefisien reliabilitas
n = Banyaknya butir pernyataan
σ_i^2 = Jumlah varians skor pernyataan ke-i
σ_t^2 = Varians skor total

Rumus diatas dapat dilakukan perhitungan setelah mendapatkan jumlah varians butir pernyataan dengan menggunakan rumus sebagai berikut (Arikunto, 2010):

$$\sigma^2 = \frac{\sum x^2 - \frac{(\sum x)^2}{n}}{n}$$

Keterangan:
σ^2 = Varians
$\sum x$ = Jumlah nilai pernyataan
N = Jumlah responden

Berdasarkan rumus uji reliabilitas variabel penelitian diperoleh hasil pengujian jumlah varians sebesar 553.893 dan *Cronbach Alpha* sebesar 0.96 yang berarti mempunyai reliabilitas tinggi karena $r_{hitung} > r_{tabel}$ yang mana 0.96 > 0.374.

4.2 Analisis Risiko

Adapun proses analisis risiko dalam penelitian ini menggunakan salah satu teknik yang ditawarkan dalam ISO/IEC 31010:2009 yakni *Failure Mode and Effects Analysis* (FMEA), dengan memberikan penilaian berdasarkan *severity*, *occurency*, *dan detection* pada tiap risiko untuk menghasilkan *Risk Priority Number* (RPN).

Adapun hasil analisis dengan penilaian risiko dengan pihak manajemen perusahaan adalah sebagaimana Tabel 7.

Tabel 6. Hasil Penilaian Risiko dengan FMEA

Variabel No	SEV	OCC	DET	RPN	Pareto
1	10	1	4	40	2%
2	10	1	3	30	2%
3	10	1	3	30	2%
4	10	1	3	30	2%
5	10	1	10	100	6%
6	10	1	10	100	6%
7	2	1	10	20	1%
8	3	1	5	15	1%
9	4	1	5	20	1%
10	3	5	5	75	5%
11	10	2	5	100	6%
12	4	5	5	100	6%
13	7	2	2	28	2%
14	7	3	1	21	1%
15	7	1	5	35	2%
16	7	4	1	28	2%
17	8	5	5	200	12%
18	8	5	1	40	2%
19	4	5	1	20	1%
20	8	3	5	120	7%

Variabel No	SEV	OCC	DET	RPN	Pareto
21	4	3	6	72	4%
22	7	1	2	14	1%
23	4	3	3	36	2%
24	10	1	2	20	1%
25	4	8	3	96	6%
26	4	6	3	72	4%
27	10	5	2	100	6%
28	4	8	2	64	4%

Hasil penilaian risiko yang merupakan dilakukan dengan wawancara kepada *stakeholder* perusahaan pihak pengembang sistem berdasarkan pertimbangan penilaian bobot risiko mengacu pada *Severity* (tingkat keparahan risiko), *Occurrence* (tingkat kejadian risiko) dan *Detection* (tingkat deteksi risiko) untuk kemudian dilakukan perhitungan RPN (*Risk Priority Number*) dengan rumus:

$$RPN = S \times O \times D$$

Keterangan:

S = *Severity* (tingkat keparahan risiko)

O = *Occurrence* (tingkat kejadian risiko)

D = *Detection* (tingkat deteksi risiko)

Sedangkan persentase (pareto) didapatkan dari RPN variabel dibagi total nilai RPN semua variabel dikali dengan 100%.

4.3 Evaluasi Risiko

Proses evaluasi risiko perlu dilakukan untuk menentukan prioritas penanganan risiko. Risiko dievaluasi berdasarkan kriteria risiko teknologi informasi apakah risiko tersebut masuk kedalam kategori rendah, menengah atau tinggi. Berikut adalah tabel untuk pengevaluasian risiko:

Tabel 7. Evaluasi Risiko

Variabel No	RPN	Perlakuan Risiko
1	40	Avoid
2	30	Avoid
3	30	Avoid
4	30	Avoid
5	100	Avoid
6	100	Avoid
7	20	Mitigation
8	15	Mitigation
9	20	Mitigation
10	75	Mitigation
11	100	Mitigation
12	100	Mitigation
13	28	Avoid
14	21	Mitigation
15	35	Accept
16	28	Mitigation
17	200	Avoid
18	40	Avoid
19	20	Avoid
20	120	Avoid
21	72	Avoid
22	14	Mitigation
23	36	Accept
24	20	Accept
25	96	Avoid
26	72	Avoid
27	100	Avoid
28	64	Avoid

Proses evaluasi risiko dilakukan untuk mendapatkan tingkat keparahan, kejadian dan deteksi suatu risiko untuk mendapatkan perlakuan yang tepat pada setiap risiko yang terjadi pada proses penerapannya.

Beberapa strategi pemilihan dalam perlakuan risiko teknologi informasi setelah dilakukan analisis diantaranya adalah sebagai berikut:

1. Penerimaan Risiko (*Accept*)
   Strategi perlakuan risiko dengan menerima risiko merupakan suatu strategi untuk menerima risiko, dan tetap menggunakan sistem serta teknologi informasi dengan diiringi upaya untuk tetap mengontrol risiko yang ada agar berada dalam batas yang dapat ditoleransi.
2. Menghindari Risiko (*Avoid*)
   Menghindari risiko adalah suatu strategi untuk mencegah terjadinya risiko dengan tidak melakukan kegiatan yang diperkirakan mempunyai risiko yang tidak dapat ditoleransi. Menghindari risiko juga dapat dilakukan dengan menghilangkan sumber ancaman yang dapat menyebabkan risiko.
3. Berbagi Risiko (*Sharing*/*Transfer*)
   Berbagi risiko adalah strategi yang digunakan untuk memindahkan sebagian dari risiko ke individu, entitas bisnis, atau organisasi lain. Memindahkan risiko tidak berarti mengurangi tingkat kegawatan risiko, tetapi hanya memindahkan ke pihak lain dan harus disadari bahwa pada akhirnya dampak risiko tetap pada pemangku risiko utama (*principal risk owner*).
4. Mitigasi Risiko (*Mitigation*)
   Mitigasi risiko adalah perlakuan risiko yang bertujuan untuk mengurangi risiko. Bentuk pengurangan risiko ini dapat berupa pengurangan kemungkinan terjadinya risiko, pengurang.

5. Kesimpulan

Proses analisa risiko berbasis ISO 31000:2018 mendapatkan 3 jenis variabel risiko yakni risiko dari Alam/ Lingkungan, risiko dari kesalahan manusia dan risiko dari sistem dan infrastruktur untuk kemudian dilakukan penilaian risiko yang telah dianalisa dengan menggunakan metode FMEA (*Failure Modes and Effects Analysis*) berbasis ISO 31010:2009 menunjukkan hasil bahwa nilai *RPN*

tertinggi sehingga menyebabkan tingkat keparahan (*Severity*), tingkat kejadian (*Occurence*) dan tingkat deteksi (*Detection*) yang kritis adalah pada terdapatnya *bugs* dengan RPN 200, Pareto 12% dan data *corrupt* pada sistem dengan RPN 120, Pareto 7% yang akan dilakukan perlakuan risiko dengan *Risk Avoid* (menghindari terjadinya risiko). Diikuti dengan risiko lainnya dengan tingkat keparahan dan perlakuan risiko yang berbeda.

Adapun saran untuk penelitian selanjutnya adalah analisis risiko berbasis ISO 31000:2018 disarankan dapat menggunakan jenis risiko teknologi informasi yang berbeda dari identifikasinya dengan NIST SP 800-30, seperti menggunakan framework COBIT atau lainnya. Selain penerapannya pada manajemen risiko yang bersifat ancaman, disarankan pula konsep ISO 31000:2018 diterapkan pada risiko yang bersifat positif yang berupa peluang agar proses penerapannya seimbang terhadap segala sisi risiko.

Ucapan Terima Kasih

Terima kasih disampaikan kepada dosen pembimbing penelitian, Dr. Ernastuti, SSi., M.Kom, juga kepada responden kuesioner yakni beberapa pekerja IT Telkom Group dan responden wawancara dari Telkom Group sebagai pihak pengembang sistem serta kepada SSC HC PT. Pertamina (Persero) atas segala waktu dan tenaga yang telah diluangkan untuk membantu penulis dalam menyusun penelitian ini.

Daftar Pustaka

Badan Standarisasi Nasional, 2018. Manajemen Risiko – Pedoman.

Hamid, T., 2011. The role of risk management in IT systems of organizations. Procedia Computer Science 3 881–887.

Hartanto, I.D., Tjahyanto, A. 2010. Analisa kesenjangan tata kelola teknologi informasi untuk proses pengelolaan data menggunakan cobit (studi kasus Badan Pemeriksa Keuangan Republik Indonesia), Program Studi Magister *Prosiding Seminar Nasional Manajemen Teknologi XI*, Surabaya, Pebruari 6, 978-979.

Hasibuan, Z., 2007. Metodologi Penelitian Pada Bidang Ilmu Komputer Dan Teknologi Informasi. Fasilkom Universitas Indonesia, Depok.

Mohammad, I., 2016. The impact of human resource information system (HRIS) applications on organizational performance (efficiency and effectiveness) in jordanian private hospitals. Journal of Management Research. Vol 8, No. 3.

Mulyani, S., 2016. Sistem Informasi Manajemen Rumah Sakit, Bandung.

Nia, B.P., 2014. Penggunaan Fmea dalam mengidentifikasi risiko kegagalan proses produksi sarung Atm (Alat Tenun Mesin) (Studi Kasus Pt. Asaputex Jaya Tegal). J@TI Undip. Vol IX, No 2.

PT. Pertamina, 2019. Sejarah Pertamina, 2019. Website: https://pertamina.com/id/sejarah-pertamina, diakses tanggal 18 Desember 2019.

Ragil, M., 2019. Failure mode and effect analysis (Fuzzy FMEA) implementation for forklift risk management in manufacturing company PT.XYZ. IOP Conference Series, 528 012027.

Rizal, M., Subekti, A., Rohma, M., 2018. Identifikasi bahaya dengan menggunakan metode fmea pada mesin evaporator di pabrik gula. *Proceeding 2nd Conference on Safety Engineering and Its Application*. ISSN No. 2581 – 1770.

Stamatis, D.H., 1995. Failure Mode and Effect Analysis: FMEA from Theory to Execution. Milwaukee : ASQC Quality Press.

Uma, S. 2006. Metode Penelitian Bisnis. Jakarta, Salemba Empat.

Utami, Y., Nugroho, A., Wijaya A.F., Perencanaan strategis sistem informasi dan teknologi informasi pada dinas perindustrian dan tenaga kerja Kota Salatiga. Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK), 253-260.

Waleed, S., 2017. Management information systems and their impact on job performance among employees in the private sector: SAUDI Telecommunications companies. International Journal of Computer Applications (0975 – 8887). Vol 164, No 11.