

## **EVALUASI MANAJEMEN RISIKO TEKNOLOGI INFORMASI BERBASIS ISO 31000:2018**

**Jakaria, Rini Fitriani, Joy Nashar Utamajaya**

Sistem Informasi, STMIK Borneo Internasional Balikpapan, Indonesia

Email: jakaria.18@stmik-borneo.ac.id, rini\_fitriani.18@stmik-orneo.ac.id,

joy.nashar@stmik-borneo.ac.id

### **Abstrak**

*PT Pertamina Balikpapan Refinery merupakan anak perusahaan PT Pertamina (Persero) yang bergerak di bidang usaha penyulingan minyak dan petrokimia. PT Pertamina Balikpapan Refinery berperan sebagai pengelola kilang proyek Balikpapan Refinery Development Master Plan (RDMP) dan juga menjadi salah satu cara Pertamina bekerjasama dengan mitra untuk berinvestasi di proyek RDMP Balikpapan. PT Pertamina (Persero) sangat perlu mengembangkan proses bisnisnya di seluruh Indonesia yaitu penerapan sistem rekrutmen online berbasis website. Sebuah sistem tanpa masalah dapat mencapai efisiensi yang lebih tinggi. Untuk kelemahan (kerentanan) pada sistem akan menjadi ancaman besar bagi perusahaan, maka perlu dilakukan manajemen risiko teknologi informasi dalam penerapan sistem E-Recruitment. Merujuk pada ISO 31000 :2018 dan penilaian risiko untuk mendapatkan angka prioritas (RPN). Risiko yang diperoleh dalam penelitian ini adalah 3 jenis risiko potensial dan 28 atribut risiko. Setelah dilakukan penilaian risiko, didapatkan hasil bahwa 7 atribut risiko memerlukan perhatian khusus selama implementasi sistem agar dapat beroperasi dengan baik di masa yang akan datang.*

**Kata Kunci :** ISO 31000; Manajemen Risiko; PT Kilang Pertamina.

Diterima: 22-09-2021 Direvisi: 15-10-2021 Disetujui: 18-10-2021

### **Pendahuluan**

PT Pertamina Balikpapan Refinery merupakan anak perusahaan PT Pertamina (Persero) yang bergerak di bidang usaha penyulingan minyak dan petrokimia. PT Pertamina Balikpapan Refinery berperan sebagai pengelola kilang proyek Balikpapan Refinery Development Master Plan (RDMP) dan juga menjadi salah satu cara Pertamina bekerjasama dengan mitra untuk berinvestasi di proyek RDMP Balikpapan. Proyek RDMP Balikpapan didanai bersama oleh Pertamina dan mitra terpilih yang nantinya akan bergabung melalui PT Refinery Pertamina Balikpapan.

Kilang PT Pertamina Balikpapan saat ini sedang memilih mitra, dan Pertamina juga menjajaki kerja sama keuangan dengan sejumlah lembaga keuangan di Korea Selatan. Pekerjaan ini dilakukan oleh kontraktor yang dibentuk oleh konsorsium SK

Engineering & Construction Co. Co., Ltd., Hyundai Engineering Co., Ltd. Ltd., PT Rekayasa Industri dan PT PP (Persero) Tbk. Nilai kontraknya sekitar US\$4 miliar. Pembangunan proyek tahap pertama ini bertujuan untuk meningkatkan kapasitas produksi kilang sebesar 38% menjadi 360.000 barel per hari dan menghasilkan produk bahan bakar yang memenuhi spesifikasi Euro V (1).

PT. Pertamina (Persero) adalah Badan Usaha Milik Negara yang menjalankan kegiatan usaha minyak dan gas bumi di sektor hulu hingga hilir. Untuk memenuhi kebutuhan bahan bakar dan gas Indonesia. Pelaksanaan proses bisnis membutuhkan jumlah karyawan yang banyak dari anak-anak terbaik Indonesia, maka perlu diterapkan sistem informasi yang komprehensif di PT untuk merekrut karyawan. Pertamina (Persero) membutuhkan tingkat kematangan yang tinggi dalam penerapannya untuk berperan dalam proses, membuat kinerja pegawai menjadi lebih baik dan terstruktur, serta semua data yang diolah dapat dikendalikan dalam sistem menjadi fakta konkrit di masa depan.

Namun, untuk menentukan efisiensi waktu dan sumber daya untuk implementasi sistem, analisis manajemen risiko sistem untuk menghindari kelemahan dan ancaman yang tidak perlu setelah implementasi sistem, akan sangat penting untuk melakukan manajemen data yang buruk. Proses melalui sistem, yang akan menimbulkan data dan kelemahan (*vulnerabilities*) dalam tanggung jawab perusahaan berupa permasalahan yang menimbulkan berbagai ancaman (*threats*).

Mengurangi risiko kesalahan aplikasi sistem informasi, seperti proses yang tidak stabil pada aplikasi, data yang tidak dapat diproses dalam jumlah banyak, dan data harus diproses satu per satu, yang akan menyebabkan proses menjadi lebih lama dan akan ada redundansi data. Dengan merumuskan manajemen risiko yang baik sebagai pertimbangan perusahaan dapat menghadapi risiko dan ancaman sehingga perusahaan dapat mengambil keputusan yang tepat. Untuk manajemen risiko berdasarkan ISO 31000:2018 dalam penelitian ini dan model FMEA (failure mode and impact analysis) pada ISO 31010:2009 untuk penilaian risiko, diperoleh angka prioritas risiko (RPN) sebagai pertimbangan untuk mengambil tindakan dari risiko tersebut. Langkah-langkah untuk mendapatkan (Tohidi, 2011).

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 (Hartanto & Tjahyanto, 2008).

Risiko adalah potensi bahaya yang mungkin disebabkan oleh implementasi proses tertentu saat ini atau peristiwa tertentu di masa depan. Menurut risiko yang terlibat dalam pemrosesan, risiko ada di semua aspek kehidupan kita dan di berbagai disiplin ilmu. Dari perspektif keamanan teknologi informasi (TI), manajemen risiko adalah proses memahami dan menanggapi faktor-faktor yang dapat menyebabkan kegagalan dalam kerahasiaan, integritas, dan ketersediaan sistem informasi.

Risiko keamanan TI adalah kesalahan yang terjadi dalam proses terkait informasi. Kesalahan ini disebabkan oleh beberapa kejadian yang disengaja atau tidak disengaja yang berdampak negatif pada tahap pemrosesan atau informasi terkait. ISO (Organisasi Internasional untuk Standardisasi) adalah federasi global badan standardisasi nasional (Stamatis, 2003).

Pekerjaan persiapan terkait standardisasi internasional biasanya dilakukan melalui komite teknis ISO sesuai dengan persyaratan teknis standardisasi. ISO 31000:2018 merupakan standar internasional yang dirancang untuk memberikan prinsip dan pedoman umum penerapan manajemen risiko. Proses manajemen risiko melibatkan komunikasi dan konsultasi Penerapan kebijakan, prosedur, dan praktik yang sistematis dalam aktivitas, latar belakang, dan penilaian risiko, tinjauan, dan pelaporan..

### Metode Penelitian

Metode penelitian dalam artikel ini menggunakan metode verifikasi untuk menentukan atribut risiko berdasarkan ISO 31000:2018, dan menggunakan metode FMEA ini untuk melakukan pembobotan risiko. Metode verifikasi kuantitatif adalah “metode ilmiah yang mencapai validitas dan reliabilitas tinggi, dengan kebenaran ilmiah yang tinggi, dan atribut kuantitatif diberi bobot, rangking atau skor (Zainal, 2007).

Pada tahap pengumpulan data, penulis mencapainya dengan menyebarkan kuesioner online berbasis *Google Sheets*, yang terkait dengan risiko penerapan teknologi informasi. Validitas dan validitas minimal 20 responden dan maksimal 100 responden telah diuji Analisis Uji Reliabilitas Kemudian, manajemen departemen pengembangan TI perusahaan yang mengembangkan sistem *e-recruitment* menggunakan metode FMEA untuk menimbang alat yang efektif (Akbar, Subekti, & Dhani, 2018).

Pada tahap analisis menggunakan FMEA, risk assessment atau risk priority number (RPN) yang teridentifikasi pada sistem e-recruitment dirancang untuk menentukan tingkat risiko bahaya yang paling kritis dengan mempertimbangkan risiko dengan tingkat keparahan yang tinggi. Dampak besar atau tingkat keparahan dan kemampuan deteksi untuk mencegah dampak. Nilai RPN diperoleh dengan mengalikan tingkat keparahan (S), kejadian (O) dan deteksi (D). Berikut ini adalah nilai referensi untuk menentukan tingkat keparahan risiko (McDermott & Ebmeier, 2009).

### Hasil Dan Pembahasan

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

#### a) Identifikasi Risiko

Identifikasi risiko sebagai variabel penelitian adalah dengan menggunakan kerangka standar NIST SP 800-30 terkait dengan identifikasi risiko teknologi

informasi untuk mengumpulkan data kuesioner dari populasi yang diwawancarai. Staf menurut peraturan pemerintah, yaitu 20 tahun dan berbagai bidang pekerjaan profesional dan teknis.

**b) Hasil Uji Validitas dan Reliabilitas**

Pengujian validitas alat dalam penelitian ini dilakukan pada setiap item pernyataan, setiap item pernyataan terdiri dari 20 item pernyataan, 25 responden menggunakan rumus uji validitas sebagai berikut:

Untuk memperoleh nilai yang signifikan, maka dilakukan uji korelasi dengan membandingkan dan dengan  $dk=n-2$  dan taraf signifikansi sebesar 5%.

**c) Analisis Risiko**

Proses analisis risiko dalam penelitian ini menggunakan teknik yang disediakan dalam ISO/IEC 31010:2009 yaitu Failure Mode and Effect Analysis (FMEA), yang menghasilkan prioritas risiko dengan memberikan penilaian berdasarkan tingkat keparahan, kejadian, dan deteksi dari setiap Tingkat risiko. nomor (RPN). Hasil analisis penilaian risiko yang dilakukan bersama manajemen perusahaan.

Variable No	SEV	OCC	DET	RPN	Pareto
11	4	3	6	72	4%
12	7	1	2	14	1%
13	4	3	3	36	2%
14	10	1	2	20	1%
15	4	8	3	96	6%
16	4	6	3	72	4%
17	10	5	2	100	6%
18	4	8	2	64	4%

**Tabel 5**

Berdasarkan penilaian bobot risiko Severity (tingkat keparahan risiko), Occurrence (tingkat kejadian risiko) dan Deteksi (tingkat deteksi risiko), hasil penilaian risiko dilakukan melalui wawancara dengan pemangku kepentingan perusahaan pengembang sistem, kemudian digunakan rumus untuk menghitung RPN:

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

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%.

#### d) Evaluasi Risiko

Proses penilaian risiko diperlukan untuk menentukan prioritas pengelolaan risiko. Risiko dinilai berdasarkan kriteria risiko teknologi informasi, terlepas dari apakah risiko tersebut termasuk dalam kategori rendah, sedang, atau tinggi. Tabel berikut adalah formulir penilaian risiko:

Variable No	RPN	Perlakuan Risiko
1	40	Avoid
2	30	Avoid
3	30	Avoid
4	30	Avoid
5	50	Avoid
6	100	Avoid
7	10	Mitigation
8	25	Mitigation
9	30	Mitigation
10	75	Mitigation
11	50	Mitigation
12	100	Mitigation
13	18	Avoid
14	21	Mitigation
15	25	Accept
16	28	Mitigation
17	100	Avoid
18	40	Avoid
19	20	Avoid

Tabel 6. Evaluasi Risiko

Proses penilaian risiko adalah untuk mendapatkan tingkat keparahan, kejadian, dan tingkat deteksi risiko, sehingga setiap risiko yang muncul dalam proses implementasi dapat ditangani dengan benar. Setelah dilakukan analisis, beberapa strategi pemilihan dalam manajemen risiko teknologi informasi adalah sebagai berikut:

##### 1. Penerimaan Risiko (*Accept*)

Strategi manajemen risiko menerima risiko adalah strategi menerima risiko,

dan terus menggunakan sistem dan teknologi informasi, sambil berusaha mengendalikan risiko yang ada dalam kisaran yang dapat diterima.

2. Menghindari Risiko (*Avoid*)

Penghindaran risiko adalah strategi untuk mencegah terjadinya risiko dengan tidak melakukan aktivitas yang dianggap memiliki risiko yang tidak dapat diterima. Risiko juga dapat dihindari dengan menghilangkan sumber ancaman yang dapat menimbulkan risiko.

3. Berbagi Risiko (*Sharing/Transfer*)

Pembagian risiko adalah strategi yang digunakan untuk mengalihkan risiko tertentu kepada individu, badan usaha, atau organisasi lain. Mentransfer risiko bukan berarti mengurangi tingkat keparahan risiko, tetapi hanya mengalihkannya ke pihak lain. Harus diakui bahwa dampak risiko pada akhirnya tetap pada pemangku kepentingan risiko utama. (*principal risk owner*).

4. Mitigasi Risiko (*Mitigation*)

Mitigasi risiko adalah perlakuan risiko yang dirancang untuk mengurangi risiko. Pengurangan risiko ini dapat berupa pengurangan kemungkinan terjadinya risiko dan pengurangan risiko.

## **Kesimpulan**

Berdasarkan proses analisis risiko ISO 31000:2018, diperoleh tiga jenis variabel risiko yaitu risiko dari alam/lingkungan, risiko dari kesalahan manusia, dan risiko dari sistem dan infrastruktur, kemudian melakukan penilaian risiko dan menggunakan FMEA (failure Mode dan Efek). Analisis metode ISO 31010:2009 menunjukkan bahwa dengan adanya RPN 100, Pareto 6%, dan kesalahan pada sistem dengan data yang rusak, nilai RPN tertinggi menghasilkan tingkat keparahan, insiden, dan tingkat deteksi kritis. RPN 72., Pareto 4% akan melakukan risk aversion (untuk menghindari terjadinya risiko). Diikuti oleh risiko lain dengan tingkat keparahan dan perlakuan risiko yang berbeda.

## BIBLIOGRAFI

- Akbar, Mochammad Rizal, Subekti, Arief, & Dhani, Mey Rohma. (2018). Identifikasi Bahaya Dengan Menggunakan Metode Fmea Pada Mesin Evaporator Di Pabrik Gula. *Seminar K3*, 2(1), 779–782. [Google Scholar](#).
- Hartanto, Indra Dwi, & Tjahyanto, Aries. (2008). Analisa kesenjangan tata kelola teknologi informasi untuk proses pengelolaan data menggunakan cobit (studi kasus badan pemeriksa keuangan republik indonesia). *Prosiding Seminar Nasional Manajemen Teknologi XI.[Online]*. Hal, 2. [Google Scholar](#).
- McDermott, Lisa M., & Ebmeier, Klaus P. (2009). A meta-analysis of depression severity and cognitive function. *Journal of Affective Disorders*, 119(1–3), 1–8. [Google Scholar](#).
- Stamatis, Diomidis H. (2003). *Failure mode and effect analysis: FMEA from theory to execution*. Quality Press. [Google Scholar](#).
- Tohidi, Hamid. (2011). The Role of Risk Management in IT systems of organizations. *Procedia Computer Science*, 3, 881–887. [Google Scholar](#).
- Zainal, A. (2007). *Metodologi penelitian pada bidang ilmu komputer dan teknologi informasi; konsep, teknik, dan aplikasi*. Fakultas Ilmu Komputer Universitas Indonesia. [Google Scholar](#).