Jurnal IPTEK-KOM (Jurnal Ilmu Pengetahuan dan Teknologi Komunikasi) eISSN 2527 - 4902
Vol. 23 No. 2, Desember 2021: 107 - 123

Analisis Manajemen Risiko SPBE Menggunakan COBIT 5 For Risk dan ISO 31000:2018 di Kabupaten Magetan

E-Government Risk Management Analysis Using COBIT 5 For Risk and ISO 31000:2018 in Magetan Regency

Khrisna Aprianto[1], Endroyono[2], Supeno Mardi Susiki Nugroho[3]
[123]Teknik Elektro, Fakultas Teknologi Elektro dan Informatika Cerdas, ITS Surabaya

[1]khrapr@gmail.com, [2]endroeleven@gmail.com, [3]mardi@its.ac.id

Naskah diterima: 1 Juli 2021 , direvisi: 11 November 2021, disetujui: 16 Desember 2021

Abstract

The implementation of e-government in Indonesia is currently experiencing several obstacles. More than 50% of government agencies' budgets are spent on procurement of similar software between organizations. The use of servers and data centers is small below 40% of its utility. Sectoral ego between government organizations is one of the reasons why the implementation of e-government is not optimal. Government, through the Indonesian Ministry of Administrative Reform issued Ministerial Regulation Number 5 of 2020 as a guide for government organizations in SPBE risk management. The XY organization in Magetan Regency as the implementing agency for the e-government is obliged to carry out risk management to ensure the achievement of goals and objectives. In this study, researchers used COBIT 5 for risk and ISO 31000:2018 to analyze e-government risk management. The purpose of the research is to analyze the effectiveness of e-government risk management published by the Indonesian Ministry of Administrative Reform with COBIT 5 for risk and ISO 31000:2018 and produce recommendations for SPBE risk management which are used as a guide in developing SPBE risk management. From the results, it could be concluded that there are 21 risks and 15 control recommendations based on SPBE risk management.

Keywords: *COBIT 5 for risk, ISO 31000:2018, e-government risk management.*

Abstrak

Kondisi penerapan SPBE di Indonesia saat ini mengalami beberapa hambatan. Diantaranya yaitu, lebih dari 50% anggaran instansi pemerintah dibelanjakan untuk pengadaan perangkat lunak sejenis. Penggunaan server dan pusat data masih di bawah 40% utilitasnya. Ego sektoral antar instansi pemerintah menjadi salah satu sebab penerapan SPBE tidak optimal. Untuk itu, pemerintah melalui KemenPAN RI menerbitkan Peraturan Menteri Nomor 5 Tahun 2020 sebagai pedoman bagi instansi pemerintah dalam manajemen risiko SPBE. Organisasi XY di Kabupaten Magetan sebagai instansi pelaksana SPBE berkewajiban melakukan manajemen risiko untuk menjamin tercapainya sasaran dan tujuannya. Dalam penelitian ini, peneliti menggunakan COBIT 5 for risk dan ISO 31000:2018 untuk melakukan analisa terhadap manajemen risiko SPBE. Tujuan dari penelitian adalah analisa efektifitas manajemen risiko SPBE yang diterbitkan KemenPAN RI dengan COBIT 5

for risk dan ISO 31000:2018 dan menghasilkan rekomendasi manajemen risiko SPBE sebagai panduan penyusunan manajemen risiko SPBE. Dari hasil identifikasi diperoleh 21 risiko dan 15 rekomendasi pengendalian.

Kata kunci: *COBIT 5 for risk,*ISO 31000:2018*,*manajemen risiko *e-goverment.*

PENDAHULUAN

Sistem Pemerintahan Berbasis Elektronik (SPBE) telah dimulai sejak tahun 2013, ditandai dengan terbitnya Instruksi Presiden Nomor 3 Tahun 2003 yang mengintruksikan kepala daerah membuat kebijakan yang sesuai dengan kewenangan, tugas dan fungsinya untuk melaksanakan *e-government* secara nasional. Di Indonesia, penerapan SPBE dinilai belum maksimal, didasarkan atas kajian Dewan TIK Nasional tahun 2016 bahwa 65% instansi pusat atau daerah membelanjakan anggaran untuk pengadaan perangkat lunak yang serupa. Data dari Kementrian Komunikasi dan Informatika tahun 2018 juga menunjukkan hanya 30% pemerintah daerah yang memanfaatkan kapasitas dari sejumlah pusat data dan *server*, beberapa layanan yang seharusnya terintegrasi masih merupakan layanan yang berdiri sendiri (KemenpanRB RI 2020).

Pengadaan barang dan jasa baik dilakukan secara manual atau elektronik mengandung risiko dalam proses pelaksanaannya tetapi juga memberikan pengaruhsignifikan terhadap kinerja pengadaan (Rotich, Ochiri, and Kamoni 2018). Pengadaan barang jasa secara elektronik atau *e-procurement* dimulai sejak terbitnya Keputusan Presiden Nomor 80 Tahun 2003, yang dilakukan secara transparan, terbuka, akuntabel sehingga mengurangi potensi korupsi, kolusi dan nepotisme. Risiko baru muncul sebagai akibat dari penggunaan media internet yaitu risiko yang berhubungan dengan infrastrukur jaringan internet. Gangguan pada sisi *server email* merupakan risiko yang terjadi ketika menggunakan media internet (Ariani and Jati 2016).

Dalam Peraturan Presiden Nomor 5 Tahun 2018, manajemen risiko termasuk dalam lingkup manajemen SPBE yang bertujuan untuk menjamin keberlangsungan SPBE dengan meminimalkan dampak risiko dalam penerapan SPBE. Organisasi XY sebagai organisasi pemerintah yang menyelenggarakan *e-government*, belum memiliki panduan manajemen risiko SPBE. Akibatnya, organisasi XY tidak dapat melakukan identifikasi, analisis dan penanganan risiko SPBE yang berdampak pada tidak tercapainya sasaran dan tujuan secara efektif jika risiko terjadi. Perpaduan COBIT 5 *for risk* dan ISO 31000:2018 dapat membantu instansi pemerintah dalam melakukan identifikasi, analisis dan penanganan risiko.

COBIT digunakan dalam mengidentifikasi manajemen risiko pada unit pelayanan organisasi (Astuti et al. 2017). COBIT juga dapat dikombinkasikan dengan PMBOK dan ISO 31000 untuk mengelola risiko-risiko TI dan membantu kelancaran jalannya proyek perusahaan (Iin 2017b). COBIT dengan metode *FMEA* juga digunakan untuk identifikasi risiko pada proses pengadaan barang jasa (Ariani and Jati 2016), perguruan tinggi (Nurhidayat and Handayaningsih 2019), serta untuk mendukung proses pengambilan keputusan (Firdaus and Suprapto 2018), dan *Enterprise Resource Planning* (Indah and Firdaus 2014). ISO 31000:2008 tentang manajemen risiko telah digunakan dalam penelitian untuk menentukan prioritas risiko atau *Risk Priority Number* (Wicaksono 2020), perancangan *Standard Operational Procedure* (Angraini and Pertiwi 2017), dan mengevaluasi sistem penjualan (Driantami, Suprapto, and Perdanakusuma 2018).

Risiko adalah dampak ketidakpastian yang mempengaruhi tujuan atau sasaran (Susilo and Kaho 2018, 32). Manajemen risiko adalah aktivitas terkoordinasi yang dilakukan untuk

mengarahkan dan mengelola organisasi dalam rangka menangani risiko (ISO 2018). Manfaat penerapan manajemen risiko salah satunya adalah dapat mengukur kinerja dan mendukung efektivitas kinerja dari sebuah organisasi (Tupa, Simota, and Steiner 2017). Manajemen risiko juga digunakan sebagai dasar atau landasan dalam penanganan risiko, perencanaan risiko, dan pengambilan keputusan oleh pimpinan suatu organisasi (de Oliveira et al. 2017). Manajemen risiko TI memberikan pengaruh atas nilai-nilai bisnis dengan pengendalian internal, tujuan tata kelola TI, dan kualitas informasi yang dihasilkan (Tsai et al. 2016).

COBIT 5 merupakan sebuah kerangka kerja yang didesain membantu organisasi dalam mencapai tujuan dan sasaran dengan tata kelola dan manajemen teknologi informasi (ISACA,2012). COBIT 5 *for risk* merupakan bagian dari COBIT 5 yang membahas manajemen risiko. *Risk appetite* yaitu level dan jenis risiko yang bersedia diterima oleh organisasi sehingga risiko tidak harus dihindari dengan menetapkan nilai maksimum terhadap risiko pada beberapa kategori proses bisnis yang di dalamnya mengandung risiko TI yang digunakan dalam rangka mencapai tujuan perusahaan (Iin 2017a). Langkah-langkah dalam manajemen risiko dalam COBIT 5 *for risk*:

1. APO12.01-Pengumpulan data
2. APO12.02-Analisis data
3. APO12.03-Penyusunan profil risiko
4. APO12.04-Penjabaran risiko
5. APO12.05-Membuat portofolio manajemen risiko
6. APO12.06-Respons risiko

ISO 31000 merupakan sebuah standar internasional yang dikeluarkan oleh International Organization for Standardization (ISO) untuk mengelola risiko. ISO 31000 terbagi menjadi tiga bagian yaitu prinsip-prinsip manajemen risiko, kerangka kerja manajemen risiko dan proses manajemen risiko (ISO 2018).

Manajemen Risiko SPBE adalah pendekatan sistematis meliputi beberapa proses, pengukuran, struktur, dan budaya yang tujuan akhir untu menentukan tindakan terbaik terkait risiko SPBE (KemenpanRB RI 2020). Penerapan manajemen risiko pada *e-government* dapat mengurangi munculnya risiko yang dapat memberikan akibat atau dampak yang merugikan bagi organisasi pemerintah (Kurniati, Nugroho, and Rizal 2020). Proses manajemen risiko SPBE merupakan sebuah proses yang dimulai dari tahap penerapan secara sistematis dari kebijakan, prosedur, dan praktek terhadap aktivitas komunikasi dan konsultasi, penetapan konteks, penilaian risiko (identifikasi risiko, analisis risiko, evaluasi risiko), penanganan risiko, pemantauan dan reviu, serta pencatatan dan pelaporan.

Berdasarkan dengan uraian di atas, maka penelitian ini bertujuan untuk melakukan analisa ekektifitas manajemen risiko SPBE yang diterbitkan oleh Permenpan dengan COBIT 5 *for risk* dan ISO 31000:2018 serta memberikan gambaran mengenai proses manajemen risiko berdasarkan *framework* COBIT 5 *for risk* dan ISO 31000:2018, dan menghasilkan rekomendasi kepada organisasi XY tentang tindakan pengendalian yang efektif dan perlakuan yang tepat bagi risiko-risiko dalam penerapan SPBE.

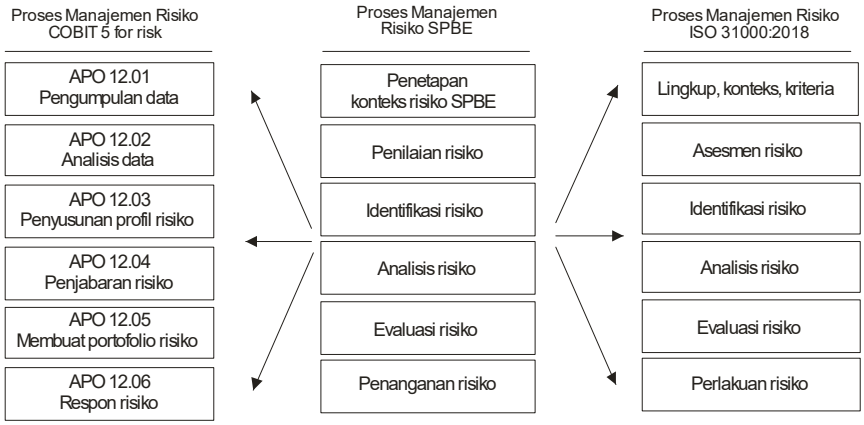
METODE

Secara garis besar metode yang digunakan dalam penelitian terdiri dari 6 tahapan sebagai berikut:

1. Studi literatur. Pada tahapan ini mempelajari sumber dari buku dan jurnal yang

membahas tentang manajemen risiko SPBE, COBIT 5 *for risk,* dan ISO 31000:2018.

2. Pengumpulan data. Tujuan dari tahapan ini yaitu untuk mengidentifikasi mengenai risiko yang pernah terjadi dengan menggunakan metode *document review* terhadap dokumen rencana strategis organisasi tahun 2018-2023, dokumen proses bisnis, dan dokumen lain, informasi penting dicatat yang digunakan sebagai input atau masukan dalam indentifikasi risiko. Selain itu juga menggunakan kuesioner dan wawancara secara acak terhadap SDM organisasi XY, diperoleh sampel sejumlah 10 orang atau 50% dari populasi. Dari 10 sampel mayoritas bekerja di lingkungan yang sama sebagai personil yang menangani proses pengadaan barang dan jasa yaitu 9 dari 10 data sehingga data yang didapat memiliki kemiripan dalam segi latar belakang data sampel. Kuesioner memuat 33 jenis risiko.
3. Analisis manajemen risiko. Tujuan dari tahapan ini menghasilkan level risiko baik menggunakan manajemen risiko SPBE, COBIT 5 *for risk* dan ISO 31000:2018 dengan dengan melakukan analisa terhadap formulir manajemen risiko SPBE berdasarkan PermenPANRB Nomor 5 tahun 2020. Formulir dalam manajemen risiko SPBE dianalisis keterkaitannya dengan COBIT 5 for risk dan ISO 31000:2018 kemudian hasilnya dievaluasi. Metode yang digunakan antara lain metode RACI untuk menentukan struktur pelaksana atau penanggung jawab risiko. Metode RACI adalah suatu metode untuk menentukan peran tanggung jawab dari pihak yang berkaitan sekaligus memperjelas tindakan yang dilakukan. Tahap ini juga menggunakan matriks risiko yang merupakan kombinasi (dalam SPBE) atau perkalian antara level kemungkinan dan level dampak (COBIT 5 dan ISO 31000). Tahapan dalam proses manajemen risiko SPBE dianalisis menurut proses manajemen risiko COBIT 5 *for risk* dan ISO 31000:2018 seperti tersaji dalam Gambar 1.



Gambar 1. Analisis Proses Manajemen Risiko SPBE dengan COBIT 5 *for risk* dan ISO 31000:2018
(Sumber: Hasil olah data penelitian)

4. Rekomendasi pengendalian risiko. Tujuan dari tahapan ini yaitu menghasilkan rekomendasi atau pengendalian risiko yang digunakan sebagai acuan dalam merespon risiko yang terjadi.
5. Analisa kondisi saat ini, melakukan analisa terhadap kondisi organisasi XY pada saat ini dan identifikasi pengendalian risiko yang sudah dilakukan.
6. Kesimpulan, menyimpulkan hasil dari penelitian yang dilakukan.

HASIL DAN PEMBAHASAN

Analisis Manajemen Risiko SPBE menggunakan COBIT 5 *for risk* dan ISO 31000:2018

Setiap tahapan proses manajemen risiko baik COBIT 5 *for risk* ataupun ISO 31000:2018 tidak selalu sesuai dengan tahapan dalam proses manajemen risiko SPBE karena antara satu *framework* memiliki proses yang berbeda. Proses manajemen risiko SPBE terdiri dari 3 (tiga) tahap yaitu tahap penetapan konteks risiko SPBE, tahap penilaian risiko SPBE (terdiri dari identifikasi risiko, analisis risiko, evaluasi risiko) dan tahap penanganan risiko SPBE. Pada tahap penetapan konteks SPBE, COBIT 5 *for risk* tidak memiliki proses atau tahapan untuk menentukan ruang lingkup dan konteks sedangkan ISO 31000:2018 memiliki tahapan atau proses tersebut.

Ada 3 (tiga) tahapan yang dilakukan dalam penilaian risiko SPBE yaitu identifikasi risiko SPBE, analisis risiko SPBE, dan evaluasi risiko SPBE. Untuk melakukan proses penilaian risiko, COBIT 5 *for risk* menggunakan domain APO 12, yaitu pedoman proses untuk manajemen risiko berkelanjutan dalam proses identifikasi, evaluasi, dan mengurangi risiko. Domain APO dimulai dari APO12.01 sampai dengan APO12.05. Sedangkan di ISO 31000:2018, tahap penilaian risiko dinamakan penilaian risiko yang terdiri dari 3 (tiga) tahap yaitu identifikasi risiko, analisis risiko dan evaluasi risiko. ISO 31000:2018 tidak memiliki metode khusus untuk itu ISO menerbitkan sebuah panduan yang berisi alat dan teknik dalam melakukan penilaian risiko.

Identifikasi risiko merupakan proses identifikasi dan menggali informasi mengenai penyebab, kejadian dan dampak risiko SPBE. Analisa yang digunakan yaitu *risk scenario* yang terdapat dalam COBIT 5 *for risk* dan metode RBS (*Risk Breakdown Structure)* dalam ISO 31000:2018. Analisis risiko adalah upaya untuk memahami risiko SPBE secara lebih mendalam. Analisis risiko SPBE merupakan proses untuk melakukan penilaian atas identifikasi risiko yang telah dilakukan sebelumnya. Metode yang digunakan dalam tahap analisis risiko SPBE adalah Matriks Risiko yang menilai level kemungkinan, level dampak, dan level risiko SPBE. Evaluasi risiko, bertujuan memperoleh informasi yang memadai tentang risiko yang akan mempengaruhi pencapaian sasaran organisasi XY baik yang bersifat positif dan negatif. Informasi tersebut dapat menjadi dasar dalam proses pengambilan keputusan mengenai perlu tidaknya dilakukan upaya penanganan risiko SPBE lebih lanjut apakah risiko tersebut diterima atau ditolak serta penentuan prioritas penanganannya.

Berikut adalah hasil analisis tahapan manajemen risiko SPBE:

1. Identifikasi Aset

Identifikasi aset diperlukan untuk mendeteksi sumber risiko. Dalam studi ini, identifikasi aset hanya fokus pada *hardware* yang menunjang proses bisnis organisasi. Berdasarkan rencana strategis organisasi tahun 2018-2021, aset *hardware* meliputi laptop, printer, komputer PC, *external hard disk*, mesin fax, *router*, dan server SPBE

2. Penetapan Konteks SPBE

Bertujuan untuk mengidentifikasi ruang lingkup penerapan risiko SPBE. Menurut COBIT 5 *for risk* dalam APO12.01, proses pertama dalam manajemen risiko adalah perencanaan optimasi risiko dan pengumpulan data. Proses perencanaan optimasi risiko dalam COBIT 5 *for risk* bukanlah sebuah rangkaian proses manajemen risiko tetapi merupakan proses yang terpisah karena termasuk dalam *risk governance and management* dalam domain EDM03. Pelaksanaan inventarisasi penetapan konteks SPBE terdiri dari 10 (sepuluh) tahapan, yaitu:

1) Identifikasi informasi umum, bertujuan untuk mendapatkan gambaran awal dari sebuah organisasi yang memuat nama, tugas pokok dan fungsi dari organisasi tersebut.

2) Identifikasi sasaran SPBE, bertujuan untuk menentukan sasaran, indikator dan target SPBE. ISO 31000:2018 memberikan metode dalam identifikasi sasaran organisasi dengan menggunakan metode SMART (*Specific, Measurable, Achievable, Relevant/ Realistic*, *Time-bound*) yang lebih rinci dalam menjabarkan pencapaian sasaran.

Tabel 1. Sasaran SPBE Organisasi

Sasaran Unit Kerja	Sasaran	Indikator Kinerja	Target Kinerja
Terlaksananya pelayanan pengadaan barang/jasa yang efektif, efisien, terbuka, kompetitif, akuntabel dan transparan	Melaksanakan Pengadaan Barang dan Jasa secara e-*tendering* Menyediakan akses 24 jam terhadap layanan SPBE Pengembangan aplikasi berbasis elektronik sebagai alat bantu dalam menunjang proses PBJ Menyediakan perangkat teknologi informasi baik *hardware* dan *software* Peningkatan kualitas aparatur SDM	Skor Indeks Kepuasan Masyarakat (IKM) bidang pengadaan barang/jasa Persentase proses pengadaan barang/jasa melalui e-*tendering* yang diselesaikan	"> 88" Sangat baik 100 %

Sumber: Renstra 2018-2023

Tabel 2. Identifikasi Sasaran dengan Metode SMART

No	Atribut	Uraian	Elemen
1	Specific	Hal yang ingin dicapai	Terlaksananya pelayanan pengadaan barang/jasa
2	Measurable	Indikator dan nilai target	Skor IKM > 88, Persentase proses pengadaan 100%
3	Achievable	Cara untuk mencapai	- Peningkatan peralatan guna mendukung proses tender barang/jasa - Optimalisasi penggunaan teknologi sistem pengadaan (LPSE) - Meningkatkan kualitas SDM
4	Relevant & realistic	Target realistis	Persentase proses pengadaan 100%
5	Time bound	Jangka waktu	2023
	Sasaran	Terlaksananya pengadaan barang dan jasa yang efektif dan efisien pada tahun 2023 oleh organisasi melalui peningkatan peralatan (*hardware*, *software*), kualitas SDM, dan penggunaan teknologi sistem pengadaan untuk memenuhi persentase proses pengadaan 100 %	

Sumber: hasil olah data penelitian

3) Penentuan Struktur Pelaksana Manajemen Risiko SPBE

Struktur pelaksana manajemen risiko SPBE terdiri dari 3 tingkatan yaitu:

a. Pemilik risiko, yakni pejabat yang bertanggung jawab atas pelaksanaan manajemen risiko SPBE, umumnya adalah pimpinan tertinggi unit (organisasi kecil).
b. Koordinator risiko, yakni pejabat yang ditunjuk oleh pemilik risiko untuk berkoordinasi dengan pemangku kepentingan baik internal dan eksternal organisasi.
c. Pengelola risiko, yakni staf/pejabat yang bertanggung jawab atas pelaksanaan operasional manajemen risiko pada unit-unit di bawah unit pemilik risiko.

Untuk membantu identifikasi struktur pelaksana atau penanggung jawab digunakan metode RACI. Struktur pelaksana manajemen risiko SPBE

menggunakan 3 (tiga) struktur (KemenpanRB RI 2020) tergantung struktur organisasi bersangkutan. Sehingga kurang detil menjelaskan mengenai tanggung jawab personil dan wilayah atau area tanggung jawabnya dibandingkan dengan COBIT 5 *for risk* memberikan struktur penanggung jawab yang lebih rinci dan ISO 31000:2018 memberikan struktur yang dapat disesuaikan dengan kebutuhan organisasi.

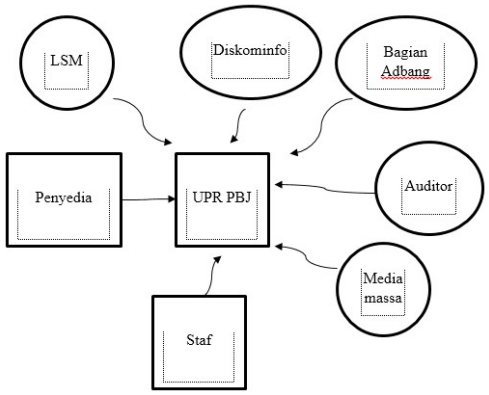
Tabel 3. Struktur Pelaksana Manajemen Risiko SPBE

Tingkat Risiko	Pelaksana Risiko
Pemilik Risiko SPBE	Kepala Bagian organisasi XY
Koordinator Risiko SPBE	Kasubbag A
Pengelola Risiko SPBE	3 Kepala Subbagian

(Sumber: PermenPANRB No.5 tahun 2020 & hasil olah data penelitian)

4) Identifikasi Pemangku Kepentingan

Bertujuan untuk memperoleh informasi dari pihak-pihak yang berinteraksi dengan unit pemilik risiko SPBE dalam rangka mencapai sasaran yang berasal dari internal dan eksternal organisasi misalnya instansi pemerintah dan instansi non pemerintah. Identifikasi pemangku kepentingan membantu unit risiko dalam mengenali asal risiko dan respon terhadap risiko tersebut. Selain itu keberadaan stakeholder seperti ditunjukkan oleh Gambar 2, dapat mempengaruhi organisasi baik secara langsung maupun tidak langsung. Bila tidak dikelola dengan baik dapat menimbulkan gesekan sehingga akan berdampak terhadap sasaran dan tujuan organisasi bahkan dapat merupakan sumber risiko.



Gambar 2. Stakeholder Internal Dan Eksternal Organisasi
(Sumber: hasil olah data penelitian)

5) Identifikasi Peraturan Perundang-Udangan

Bertujuan menginventarisasi peraturan atau regulasi yang berhubungan antara organisasi dan pelaksanaan SPBE. Untuk COBIT 5 *for risk* dan ISO 31000:2018 tidak dibahas lebih lanjut dikarenakan memiliki pengertian yang sama dengan SPBE.

6) Penetapan Kategori Risiko SPBE

Bertujuan untuk menjamin agar proses identifikasi, analisis, dan evaluasi risiko SPBE dapat dilakukan secara komprehensif. Kategori risiko SPBE berjumlah 16 (enam belas) kategori, sedangkan COBIT 5 *for risk* memiliki 20 (dua puluh) kategori dan ISO 31000:2018 memberikan nama kategori sesuai dengan sasaran dari

organisasi sehingga fleksibel menyesuaikan kebutuhan organisasi. Untuk membantu identifikasi risiko digunakan metode kuesioner kepada SDM organisasi. Responden diberikan 33 (tiga puluh tiga) risiko untuk kemudian dipilih berdasarkan risiko-risiko yang pernah terjadi, sehingga diperoleh sebanyak 20 (dua puluh risiko) dengan uraian seperti dalam Tabel 4.

Dari Tabel 4, risiko serangan virus/*worms*/*malware*, serangan manusia, koneksi internet tidak memadai, koneksi jaringan terputus, *server down*, pemahaman *stakeholder* terkait terhadap SPBE menjadi risiko yang banyak dipilih oleh responden. Sedangkan risiko kegagalan backup data, kerusakan *hardware*, pemakaian *Software* non orisinal, dokumentasi atau tata cara penggunaan program/aplikasi tidak lengkap, kebocoran data organisasi, kondisi server, perangkat mengalami *overheat* dan *overload* menjadi risiko yang sedikit dipilih oleh responden.

Risiko yang sudah teridentifikasi menjadi masukan dalam analisis penetapan kategori risiko SPBE (7 kategori), COBIT 5 *for risk* (10 risiko) dan ISO 31000:2018 (4 kategori). Kategori risiko COBIT 5 *for risk* memiliki keunggulan dibandingkan kategori risiko SPBE dan ISO 31000:2018 yaitu jumlah risiko lebih banyak dan terinci sehingga memudahkan dalam identifikasi kategori risiko IT.

Tabel 4. Identifikasi Risiko Melalui Kuesioner

No.	Uraian risiko	Jml	No.	Uraian risiko	Jml
1	Data hilang atau rusak	2	11	Pemeliharaan yang tidak terjadwal	2
2	Kegagalan *backup* data	1	12	Kemampuan SDM	2
3	Serangan virus, *worms*, *malware*	4	13	Antar muka (*user interface*) program atau aplikasi susah dipahami	2
4	Serangan manusia (*hacker*, *cracker*)	4	14	Kebocoran data organisasi	1
5	Kerusakan *hardware*	1	15	Kesalahan yang dilakukan oleh staf (*human eror*)	2
6	Pemakaian *software* non orisinal	1	16	Kurang/tidak memahami aturan pelaksanaan SPBE	2
7	Koneksi internet tidak memadai	4	17	Server down	4
8	Koneksi jaringan terputus	4	18	Kondisi *server*	1
9	Dokumentasi atau tata cara penggunaan program/aplikasi tidak lengkap	1	19	Perangkat mengalami *overheat* dan *overload*	1
10	Listrik padam	2	20	Pemahaman *stakeholder* (pihak yang berkepentingan) terkait terhadap SPBE	4

Sumber: hasil olah data penelitian

7) Penetapan Area Dampak Risiko SPBE

Bertujuan untuk mengetahui area mana saja yang terkena efek dari risiko SPBE setelah risiko dikelompokkan menurut kategori risiko. Tabel 5 menunjukkan area dampak risiko SPBE. Terdapat beberapa risiko yang memiliki area dampak lebih dari satu area sebagai contoh data hilang atau rusak memiliki dampak kepada kinerja dan layanan organisasi. Untuk COBIT 5 *for risk* tidak terdapat tahapan dalam penetapan area dampak sedangkan ISO 31000:2018 area dampak menyesuaikan dengan penetapan kategori risiko.

Tabel 5. Area Dampak Dan Risiko SPBE

No.	Area dampak risiko	Risiko
1	Finansial/ Keuangan	Pemakaian *software* non orisinal
2	Reputasi	Serangan manusia (*hacker*, *cracker*), kebocoran data organisasi, kurang/tidak memahami aturan pelaksanaan SPBE, pemahaman *stakeholder* terkait SPBE
3	Kinerja	Data hilang atau rusak, kegagalan *backup data*, serangan *virus/worms/malware*, serangan manusia (*hacker*, *cracker*), kerusakan *hardware*, pemakaian *software* non orisinal, koneksi internet tidak memadai, koneksi jaringan terputus, dokumentasi atau tata cara penggunaan program/aplikasi tidak lengkap, listrik padam, kurang/tidak memahami aturan pelaksanaan SPBE, *server do*wn, perangkat mengalami *overheat* dan *overload*, pemahaman *stakeholder* terkait SPBE
4	Layanan Organisasi	Data hilang atau rusak, kegagalan *backup data*, serangan *virus/worms/malware*, serangan manusia (*hacker*, *cracker*), kerusakan *hardware*, pemakaian *software* non orisinal, koneksi internet tidak memadai, koneksi jaringan terputus, dokumentasi atau tata cara penggunaan program/aplikasi tidak lengkap, listrik padam, pemeliharaan yang tidak terjadwal, antar muka (*user interface*) program atau aplikasi susah dipahami, kurang/tidak memahami aturan pelaksanaan SPBE, *server do*wn, perangkat mengalami *overheat* dan *overload*, pemahaman *stakeholder* terkait SPBE
5	Operasional dan Aset TIK	Kegagalan *backup data*, serangan *virus/worms/malware*, kerusakan *hardware*, antar muka (*user interface*) program atau aplikasi susah dipahami, kebocoran data organisasi, kesalahan yang dilakukan oleh staf (*human error*), serv*er d*own, kondisi *server*, perangkat mengalami *overheat* dan *overload*
6	Hukum dan Regulasi	Pemakaian *software* non orisinal, pemahaman *stakeholder* terkait SPBE
7	Sumber Daya Manusia	*Skill*/kemampuan SDM, kesalahan yang dilakukan oleh staf (*human erro*r), kurang/tidak memahami aturan pelaksanaan SPBE, kondisi *server*, pemahaman *stakeholder* terkait SPBE

Sumber: hasil olah data penelitian

8) Penetapan Kriteria Risiko SPBE

Bertujuan untuk mengukur dan menetapkan seberapa besar kemungkinan kejadian dan dampak risiko SPBE yang akan terjadi. Penentuan kriteria risiko SPBE melalui dua tahap yaitu menetapkan kriteria kemungkinan dan kriteria dampak SPBE (KemenpanRB RI 2020). Baik SPBE, COBIT 5 *for risk* dan ISO 31000:2018 memiliki kriteria kemungkinan, yang berbeda hanya penamaan kriteria kemungkinan. Begitu juga dengan level dampak sesuai dengan area dampak yang diidentifikasi.

Dalam penetapan level dampak SPBE terdiri dari 7 (tujuh) area dampak. COBIT 5 *for risk* tidak ada tahap yang dilakukan. Sedangkan *ISO 31000:2018* area dampak menggunakan penamaan jenis dampak, yaitu keuangan, waktu, layanan, dan reputasi. Pada tahap penetapan ini, yang berbeda hanya penamaan level dampak menyesuiakan area dampak.

Tabel 6. Level Kemungkinan dalam SPBE, COBIT 5 *For Risk,* dan ISO 31000:2018

Level	SPBE	COBIT 5 for risk	ISO 31000:2018
1	Hampir Tidak Terjadi	Sangat jarang	Sangat jarang
2	Jarang Terjadi	Jarang	Jarang
3	Kadang-Kadang Terjadi	Biasa	Biasa
4	Sering Terjadi	Sering	Sering
5	Hampir Pasti Terjadi	Sering terjadi	Sering terjadi

Sumber: hasil olah data penelitian

9) Matriks Analisis Risiko SPBE dan Level Risiko SPBE

Merupakan kombinasi antara kriteria kemungkinan dan kriteria dampak atas risiko sehingga menghasilkan level risiko yang digunakan untuk menentukan sebuah level risiko dari sebuah risiko. Tabel 7 dan 8 menunjukan perbandingan matriks risiko antara matriks risiko SPBE, *COBIT 5 for risk* dan ISO 31000:2018.

Nilai matriks risiko SPBE bersifat fleksibel atau dapat disesuaikan dengan kebutuhan dari organisasi (KemenpanRB RI 2020). Sedangkan nilai matriks COBIT 5 *for risk* dan ISO 31000:2018 merupakan hasil perkalian antara level kemungkinan dan level dampak yang mengakibatkan hasil analisis level risiko berbeda, sehingga terjadi perbedaan cukup signifikan jumlah risiko dalam tiap level risiko.

Tabel 7. Matriks Risiko SPBE Berdasarkan PermenPANRB Nomor 5 Tahun 2020

Level Kemungkinan		Level Dampak 1 Tidak Signifikan	2 Kurang Signifikan	3 Cukup Signifikan	4 Signifikan	5 Sangat Signifikan
5	Hampir Pasti Terjadi	9	15	18	23	25
4	Sering Terjadi	6	12	16	19	24
3	Kadang Kadang Terjadi	4	10	14	17	22
2	Jarang Terjadi	2	7	11	13	21
1	Hampir Tidak Terjadi	1	3	5	8	20

Sumber: hasil olah data penelitian

Tabel 8. Matriks Risiko COBIT 5 *for risk* dan ISO 31000:2018

Level Kemungkinan		Level Dampak 1 Tidak Signifikan	2 Kecil	3 Sedang	4 Besar	5 Luar Biasa
5	Sering terjadi	5	10	15	20	25
4	Sering	4	8	12	16	20
3	Biasa	3	6	9	12	15
2	Jarang	2	4	6	8	10
1	Sangat jarang	1	2	3	4	5

Sumber: hasil olah data penelitian

10) Selera Risiko SPBE

Level dimana suatu risiko akan direspon. Nilai dalam selera risiko disesuaikan dengan kebutuhan organisasi dalam merespon risiko.

3. Penilaian risiko SPBE

Merupakan proses untuk menjaring setiap risiko yang berpotensi menghambat pencapaian tujuan dan sasaran TI. Pada tahap ini akan dilakukan identifikasi risiko untuk mengenali dan menemukan jawaban terhadap apa, bagaimana, kapan, dan mengapa tentang risiko TI, penyebab risiko, dan dampak risiko. Ada dua tahapan dalam penilaian risiko yaitu identifikasi risiko dan analisis risiko. Identifikasi risiko COBIT 5 *for risk* dengan menyusun *risk scenario* yang berasal dari kategori risiko sebelumnya. Identifikasi risiko SPBE berjumlah 21 risiko pada 5 sasaran organisasi dan COBIT 5 *for risk* identifikasi risiko menggunakan *risk scenario* untuk mengetahui pengaruh baik positif dan negatif dari sebuah risiko seperti tersaji di Tabel 9 dan Tabel 10.

Tabel 9. Identifikasi Risiko SPBE

No.	Risiko	No.	Risiko
1	Koneksi internet lancar dan kecepatan memadai;	12	Data pekerjaan lebih aman, tersimpan dengan baik dan terjaga;
2	Waktu tunggu yang lama dalam proses *upload* dan *download*;	13	*Update* sistem operasi lancar;
3	Data pengguna aman dan terjamin;	14	Data gagal tersimpan karena data hilang komputer/laptop tidak bisa booting;
4	Aplikasi (web) SPBE ter-*hack/ deface*;	15	Aplikasi tidak bisa diperbarui;
5	File data terinfeksi *virus, worm*;	16	Sulit menggunakan aplikasi;
6	Terlaksananya akses aplikasi 24/7;	17	Terkena tuntutan hukum terkait HAKI;
7	Publikasi informasi lebih transparan;	18	Pekerjaan selesai sesuai jadwal;
8	Pemeliharaan sistem secara tiba – tiba;	19	Pekerjaan tidak selesai sesuai jadwal;
9	*Server crash*;	20	Penyimpangan proses PBJ;
10	Proses administrasi pengadaan lebih termonitor;	21	Data sensitif organisasi bocor.
11	*Stakeholder* tidak dapat memantau proses administrasi berkas pra e-tender;		

Sumber: hasil olah data penelitian

Tabel 10. Identifikasi Risiko COBIT 5 *for risk*

No.	Jenis Risiko	Tipe Risiko*			Skenario Risiko	
		A	B	C	Positif	Negatif
1	*Portfolio establishment and maintenance*	P	S	P	Pemeliharaan *hardware* sudah terjadwal	Pemeliharaan *hardware* belum terjadwal
2	*IT expertise and skills*	P	S	P	Staf tidak ada yang merangkap tugas	Staf merangkap tugas
		P	S	P	Jumlah SDM sesuai dengan beban kerja	Jumlah SDM terbatas
		S	P	P	Staf memiliki *skill* yang cukup	*Skill* staf masih kurang
		S	P	P	Ada pelatihan yang untuk peningkatan *skill*	Tidak ada pelatihan
		S	P	P	Terdapat proses transfer ilmu kepada staf baru	Tidak terdapat transfer ilmu kepada staf baru
3	*Staff operations (human error and malicious intent)*	S	S	P	Ada pemeriksa	Staf lalai dalam memasukkan data
		S	S	P	Ada pemeriksa/SDM IT	Staf lalai dalam menggunakan perangkat
		S	S	P	Ada pemeriksa	Staf lalai dalam memberikan informasi
4	*Information*	P	P	P	Data tersimpan dengan aman	Data hilang karena tidak ada *backup*
		P	P	P	*Backup* data minimal dua media	Hanya menyimpan pada satu media
		P	P	P	Data disimpan pada area yang aman dari pencurian data	Data mudah diretas oleh pihak yang tidak berkepentingan
		S	S	P	Ada SOP dalam memberikan informasi pada pihak lain	Staf membocorkan data sensitif organisasi
5	*Infrastructure*	P	P	P	Sebelum *hardware* rusak sudah diganti/diperbaiki	Membutuhkan waktu dalam mengganti *hardware* yang rusak
		P	S	P	koneksi jaringan dan internet yang handal	Koneksi jaringan dan Internet yang tidak

					mendukung kelancaran pekerjaan	memadai menghambat pekerjaan
		S	S	P	Ada pemeriksaan	Kondisi server terbengkalai
6	*Software*	S	P	P	Software update	Software tidak update
		S	S	P	Manual pemakaian lengkap	Tidak ada manual pemakaian
		S	S	P	Mudah dalam operasional *Software*	Pengguna kesulitan menggunakan aplikasi
7	*Regulatory compliance*	P	S	P	*Stakeholder* bertanggung jawab sesuai peran tugas dan fungsi	*Stakeholder* tidak bertanggung jawab
8	*Geopolitical*	P	S	P	*Stakeholder* memahami peran tugas dan fungsi	*Stakeholder* memaksakan kehendak
9	*Malware*	P	P	P	Ada perlindungan terhadap virus, *malware*, *worm*	Ada serangan virus, *malware*, *worm*
10	*Logical attacks*	P	P	P	Ada perlindungan terhadap virus, *malware*, *worm*	Ada serangan virus, *malware*, *worm*

Tipe Risiko:
- *A. IT benefit/value enablement risk*
- *B. IT programme and project delivery risk*
- *C. IT operations and servicedelivery risk*

Pada tabel 10, tipe risiko diisi dengan '*P' (Primer)* apabila risiko terkait TI sebagai *enabler* untuk meningkatkan solusi bisnis, sedangkan jika tidak terkait maka diisi dengan *'S' (Sekunder)*. *IT programme and project delivery risk*, diisi dengan *'P' (Primer)* apabila risiko terkait dengan program dan proyek TI, sedangkan jika tidak terkait maka diisi dengan *'S'(Sekunder)*. *IT operations and service delivery risk*, diisi dengan *'P' (Primer)* apabila risiko terkait dengan ketersediaan layanan, stabilitas operasional dan gangguan layanan, sedangkan jika tidak terkait maka diisi dengan '*S' (Sekunder)*.

Rekomendasi Pengendalian Risiko SPBE

Rekomendasi pengendalian risiko SPBE disusun berdasarkan kejadian dan penyebab risiko yang telah diidentifikasi sebelumnya pada tahapan identifikasi risiko SPBE. Penyusunan menghasilkan 15 rekomendasi pengendalian risiko, terdiri dari 2 rekomendasi pengendalian yang berkaitan dengan SDM, 4 rekomendasi mengenai infrastruktur, 3 rekomendasi berkaitan dengan *software*/aplikasi, 5 rekomendasi berkaitan dengan kebijakan, dan 1 rekomendasi yang berkaitan dengan data. Beberapa identifikasi risiko diberikan rekomendasi pengendalian yang sama karena memiliki kemiripan sumber risiko, untuk lebih jelasnya tersaji pada Tabel 11.

Tabel 11. Rekomendasi Pengendalian Risiko SPBE

No	Uraian	Rekomendasi Pengendalian
1	SDM	Memberikan seminar, diklat kepada staf
		Mengadakan sosialisasi, seminar, diklat kepada pelaku PBJ
2	Infrastruktur	Pemantauan rutin koneksi internet dan Koordinasi dengan OPD penanggung jawab layanan internet
		Penjadwalan perawatan rutin server
		Menyediakan peralatan *backup* listrik misal UPS atau genset
		Menggunakan media penyimpanan data /*backup* lebih dari satu
3	Software/ aplikasi	Memastikan aplikasi ter-*update*
		Menggunakan aplikasi orisinal atau open source
		Membuat petunjuk penggunaan aplikasi
4	Kebijakan	SOP pengecekan berkala keamanan sistem
		SOP terima data yang berupa *soft file*

		SOP pemberian informasi kepada pihak lain melalui petugas PPID
		SOP proses pelaksanaan pengadaan
		Pengawasan berjenjang
5	Data	Melakukan cek dan ricek terhadap data pengguna

Sumber: hasil olah data penelitian

Tahap selanjutnya adalah analisis risiko yaitu suatu proses yang dilakukan untuk menilai sebuah risiko SPBE. Analisis risiko berisi tentang sistem pengendalian (berdasarkan identifikasi rekomendasi pengendalian risiko sebelumnya), level kemungkinan, dan level dampak terjadinya risiko SPBE sehingga akan dihasilkan nilai suatu besaran risiko dan level risiko. Hasils analisis risiko akan dipresentasikan dalam matriks risiko. Pada COBIT 5 *for risk* analisia risiko berdasar *risk scenario* yang sudah diidentifikasi pada tahap identifikasi risiko. Sedangkan analisis risiko ISO 31000:2018 sama dengan analisis risiko SPBE. Hasil analisis risiko baik SPBE, COBIT 5 *for risk* dan ISO 31000:2018 tertuang dalam Tabel 12 berikut.

Terlihat perbedaan yang mencolok pada level risiko sangat rendah dimana dengan menggunakan SPBE risiko yang berada di level sangat rendah hanya 1 tetapi menurut COBIT 5 *for risk* dan ISO 31000:2018 lebih dari 5. Hal ini dikarenakan terdapat perbedaan dalam penentuan representasi angka antara level kemungkinan dengan level dampak antara manajemen risiko SPBE, COBIT 5 *for risk* dan ISO 31000:2018 sehingga mempengaruhi dalam penentuan prioritas penangangan risiko oleh pemilik risiko.

Tabel 12. Perbandingan Level/Kriteria dan Kelompok Risiko SPBE, COBIT 5 *for risk* dan ISO 31000:2018

Level Risiko	SPBE	COBIT 5 for risk	ISO 31000:2018
Sangat Rendah	Listrik padam	1) Data hilang atau rusak 2) Kegagalan backup data 3) Kebocoran data organisasi 4) Kerusakan hardware 5) Koneksi internet tidak memadai, Koneksi jaringan terputus, 6) Kondisi server, Perangkat mengalami Overheat dan overload 7) Serangan virus, Worms, malware	1) Koneksi internet tidak memadai 2) Kegagalan backup data 3) Serangan virus, Worms, malware 4) Perangkat mengalami Overheat dan overload 5) Listrik padam 6) Kerusakan hardware 7) Data hilang atau rusak 8) Kebocoran data organisasi
Rendah	1) Koneksi internet tidak memadai 2) Kegagalan backup data 3) Serangan virus, Worms,malware 4) Kerusakan hardware 5) Data hilang atau rusak 6) Antar muka (user interface) program atau aplikasi susah dipahami 7) Kebocoran data organisasi	1) Serangan manusia (hacker, cracker) 2) Pemakaian Software non orisinal 3) Dokumentasi atau tata cara penggunaan program / aplikasi tidak lengkap 4) Antar muka (user interface) program atau aplikasi susah dipahami	1) Serangan manusia (hacker, cracker) 2) Pemakaian Software non orisinal 3) Dokumentasi atau tata cara penggunaan program / aplikasi tidak lengkap 4) Antar muka (user interface) program atau aplikasi susah dipahami
Sedang	1) Serangan manusia (hacker, cracker) 2) Pemakaian Software non orisinal 3) Dokumentasi atau tata cara penggunaan program /	1) Pemeliharaan yang tidak terjadwal 2) Skill / kemampuan SDM 3) Kesalahan yang dilakukan oleh staf (human eror)	1) Pemeliharaan yang tidak terjadwal 2) Koneksi jaringan terputus 3) Server down 4) Pemahaman stakeholder (pihak yang berkepentingan)

	aplikasi tidak lengkap		terkait terhadap SPBE 5) Skill / kemampuan SDM 6) Kesalahan yang dilakukan oleh staf (human eror)
Tinggi	1) Pemeliharaan yang tidak terjadwal 2) Kondisi server 3) Koneksi jaringan terputus 4) Server down 5) Perangkat mengalami Overheat dan overload 6) Pemahaman stakeholder (pihak yang berkepentingan) terkait terhadap SPBE 7) Kurang / tidak memahami aturan pelaksanaan SPBE 8) Skill / kemampuan SDM 9) Kesalahan yang dilakukan oleh staf (human eror)	1) Kesalahan yang dilakukan oleh staf (human eror) 2) Kurang / tidak memahami aturan pelaksanaan SPBE 3) Pemahaman stakeholder (pihak yang berkepentingan) terkait terhadap SPBE	1) Kondisi server 2) Kurang / tidak memahami aturan pelaksanaan SPBE
Sangat Tinggi	Kurang / tidak memahami aturan pelaksanaan SPBE	-	-

Sumber: hasil olah data penelitian

Analisa Kondisi Saat Ini

Saat ini organisasi XY belum memiliki pengendalian risiko tertulis yang berkaitan dengan penerapan SPBE. Dari pengendalian risiko saat ini, organisasi XY memiliki 7 (tujuh) pengendalian risiko atau hanya 30,43% dari 23 identifikasi risiko menurut manajemen risiko SPBE. Ketujuh pengendalian risiko tersebut dapat terlihat di Tabel 13.

Tabel 13. Pengendalian risiko saat ini pada organisasi XY

No	Jenis pengendalian	Penjelasan
1	SOP pelaksanaan pengadaan	SOP tentang proses pelaksanaan pengadaan dimulai dari tahap persiapan s.d pelaporan
2	Pengawasan melekat	Pemberian informasi kepada pihak luar dilakukan melalui pejabat yang ditunjuk dalam hal ini Kepala Bagian PBJ Magetan
3	Berlangganan ISP lain	Tersedia backup internet sehingga memiliki 2 koneksi internet
4	Melakukan sosialisasi	Rutin mengadakan sosialisasi SPBE *(e-procurement)* kepada pelaku PBJ
5	Mengirim staf mengikuti seminar dan pelatihan	Rutin mengirimkan staf untuk mengikuti pendidikan, pelatihan, seminar yang berhubungan dengan pengadaan
6	Pengawasan berjenjang	Melakukan pemeriksaan dan koreksi terhadap hasil kerja staf
7	Menyediakan backup hard disk	Memberikan media backup cadangan ke masing – masing staf unit

Sumber: hasil olah data penelitian

Sistem pengendalian risiko yang ada saat ini kurang berjalan dengan baik. Terdapat beberapa kendala yang dihadap diantaranya belum ada pejabat atau staf yang diberikan tanggung jawab atau pembagian tugas dalam menangani risiko, terbatasnya anggaran, dan kurangnya staf IT. Pengendalian risiko yang sudah dilakukan perlu diwujudkan dalam bentuk SOP untuk memberikan pedoman dan petunjuk dalam melakukan tugas. Evaluasi Risiko SPBE dilakukan sebagai alat bantu pengambil keputusan tentang perlu atau tidak dilakukan upaya penanganan risiko SPBE serta menentukan skala penanganan prioritas sesuai dengan selera risiko SPBE yang telah ditetapkan sebelumnya. Penyusunan prioritas membantu pemilik risiko dalam merumuskan langkah dalam penanganan risiko yang memuat penyebab, dampak, level, penanggung jawab dan

respon risiko. Penanggung jawab dapat disesuaikan dengan peran (*role*) dalam *COBIT 5 for risk*. Tabel 14 menunjukkan penetapan prioritas penanganan risiko SPBE di organisasi XY.

Tabel 14. Penetapan Prioritas Penanganan Risiko SPBE

Nomor		1
Sistem pengendalian		Mengadakan sosialisasi, seminar, diklat kepada pelaku PBJ
Kemungkinan		
	Level	Hampir pasti terjadi
	Penjelasan	Penyimpangan Proses PBJ
	Penyebab risiko	Pelaku PBJ kurang memahami peraturan dan prosedur proses PBJ
Dampak		
	Level	Signifikan
	Penjelasan	Tuntutan hukum berdampak pada kinerja/performa organisasi
Besaran risiko SPBE		23
Level Risiko SPBE		Sangat tinggi
Evaluasi		
	Keputusan penanganan	Ya
	Prioritas penanganan	1
Penanggung Jawab		CEO/COO/BPO
Respon risiko		Mitigasi

Sumber: hasil olah data penelitian

KESIMPULAN

Manajemen risiko SPBE merupakan hasil kombinasi dari tahapan yang tercantum dalam COBIT 5 *for risk* dan ISO 31000:2018. Masih terdapat kekurangan yaitu dalam penetapan penanggung jawab risiko, untuk organisasi menengah dan besar dimana dalam SPBE hanya terdiri dari 3 (tiga) unsur dan kurang baik dalam mendeskripsikan tanggung jawab sehingga perlu disesuaikan dengan peran (*role*) pada COBIT 5 *for risk* yang lebih detil. Dari hasil identifikasi risiko diperoleh sebanyak 21 (dua puluh satu) risiko yang berkaitan dengan pencapaian sasaran organisasi. Rekomendasi sistem pengendalian diperoleh sebanyak 15 pengendalian risiko dari identifikasi risiko SPBE yang telah dilakukan. Saat ini organisasi XY memiliki 7 (tujuh) sistem pengendalian. Hasil identifikasi risiko SPBE dan rekomendasi sistem pengendalian digunakan dalam analisis risiko SPBE dan COBIT 5 *for risk* untuk menghasilkan level risiko. Terdapat perbedaan jumlah risiko untuk tiap level risiko, pada level sangat rendah, tinggi dan sangat tinggi cukup mencolok. Hal ini dikarenakan dalam matriks risiko, angka yang dihasilkan oleh manajemen risiko SPBE merupakan fleksibilitas atas kebutuhan organisasi berbeda dengan COBIT 5 *for risk* dan ISO 31000:2018 yang merupakan perkalian antara level kemungkinan dan level dampak. Jika menggunakan matriks risiko SPBE maka dimungkinkan tiap organisasi memiliki model matriks risiko yang berbeda jika dibandingkan menggunakan matriks risiko COBIT 5 *for risk* ataupun ISO 31000:2018 sehingga perlu lebih cermat dalam penentuan nilai dalam matriks risiko yang sesuai dengan kondisi organisasi.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada dosen pembimbing, dosen wali, Telematika 2019, rekan kerja atas suport dan Kementerian Komunikasi dan Informatika RI yang telah memberikan kesempatan untuk menempuh pendidikan pada Magister Teknik Prodi Telematika Institut Teknologi Sepuluh Nopember Surabaya.

DAFTAR PUSTAKA

Angraini, and Indri Dian Pertiwi. 2017. "Analisa Pengelolaan Risiko Penerapan Teknologi Informasi Menggunakan Iso 31000." *Jurnal Ilmiah Rekayasa Dan Manajemen Sistem Informasi* Vol. 3, (2): 70–76.

Ariani, Amelia Febri, and Rahmi Kartika Jati. 2016. "Analisis Risiko Pada Proses Pengadaan Melalui E-Procurement Di Pusat Penelitian X." *11th Annual Meeting on Testing and Quality 2016 Lembaga Ilmu Pengetahuan Indonesia*, no. August: 5–8.

Astuti, Hanim Maria, Feby Artwodini Muqtadiroh, Eko Wahyu Tyas Darmaningrat, and Chitra Utami Putri. 2017. "Risks Assessment of Information Technology Processes Based on COBIT 5 Framework: A Case Study of ITS Service Desk." *Procedia Computer Science* 124: 569–76. https://doi.org/10.1016/j.procs.2017.12.191.

Driantami, Hana Talitha Iddo, Suprapto, and Andi Reza Perdanakusuma. 2018. "Analisis Risiko Teknologi Informasi Menggunakan ISO 31000 (Studi Kasus : Sistem Penjualan PT Matahari Department Store Cabang Malang Town Square)." *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer* 2 (11): 4991–98.

Firdaus, Nurfitri Zukhrufatul, and Suprapto. 2018. "Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk (Studi Kasus : PT . Petrokimia Gresik)." *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer* 2 (1): 1–10. http://j-ptiik.ub.ac.id/index.php/j-ptiik/article/view/702.

Iin, Hurin. 2017a. "Manajemen Risiko Teknologi Informasi Pada Proyek Perusahaan XYX Melalui Kombinasi COBIT, PMBOK, Dan ISO 31000." *Tesis*.

———. 2017b. "Manajemen Risiko Teknologi Informasi Pada Proyek Perusahaan Xyz Melalui Kombinasi COBIT, PMBOK, DAN ISO 31000." *Jurnal Ilmiah Teknologi Dan Rekayasa* 9 (2): 43–50.

Indah, Dwi Rosa, and Mgs Afriyan Firdaus. 2014. "Risk Management for Enterprise Resource Planning Post Implementation Using COBIT 5 for Risk." *Proceeding of The 1st International Conference on Computer Science and Engineering*, 113–18. https://media.neliti.com/media/publications/224346-risk-management-for-enterprise-resource.pdf.

ISO. 2018. "ISO 31000:2018 Guidelines."

KemenpanRB RI. 2020. *PermenPAN RI Nomor 5 Tahun 2020 Tentang Pedoman Manajemen Risiko Sistem Pemerintahan Berbasis Elektronik*.

Kurniati, A, L E Nugroho, and M N Rizal. 2020. "… Informasi Pada E-Government: Ulasan Literatur Sistematis Information Technology Risk Management on e-Government: Systematic Literature Review." *Jurnal IPTEK-KOM (Jurnal Ilmu …* 22 (2): 207–22. https://202.89.117.136/index.php/iptekkom/article/viewFile/3452/1473.

Nurhidayat, Riki, and Sri Handayaningsih. 2019. "Analisis Manajemen Risiko Pada Layanan Pengunduran Diri Mahasiswa Menggunakan Framework COBIT 5 Fokus Pada Mengelola Risiko (APO12)." *JSTIE (Jurnal Sarjana Teknik Informatika) (E-Journal)* 7 (1): 69. https://doi.org/10.12928/jstie.v7i1.15806.

Oliveira, Ualison Rébula de, Fernando Augusto Silva Marins, Henrique Martins Rocha, and Valério Antonio Pamplona Salomon. 2017. "The ISO 31000 Standard in Supply Chain Risk Management." *Journal of Cleaner Production* 151: 616–33. https://doi.org/10.1016/j.jclepro.2017.03.054.

Rotich, Gladys, George Ochiri, and Peter Kamoni. 2018. "Influence of Procurement Risk Management on Procurement Performance of Mega Projects in the Energy Sector in Kenya." *European Journal of Logistics, Purchasing and Supply Chain Management* 6 (5): 1–12. https://doi.org/December 2018.

Susilo, Leo J., and Victor Riwu Kaho. 2018. *Manajemen Risiko Berbasis ISO 31000: 2018 Panduan Untuk Risk Leaders Dan Risk Practitioners*. Edited by Diane Novita. Cetakan Ke. PT. Grasindo Jakarta.

Tsai, Wen Hsien, Chu Lun Hsieh, Chung Wei Wang, Chuan Tu Chen, and Wei Hsiang Li. 2016. "The Impact of IT Management Process of COBIT 5 on Internal Control, Information Quality, and Business Value." *IEEE International Conference on Industrial Engineering and Engineering Management* 2016-Janua: 631–34. https://doi.org/10.1109/IEEM.2015.7385724.

Tupa, Jiri, Jan Simota, and Frantisek Steiner. 2017. "Aspects of Risk Management Implementation for Industry 4.0." *Procedia Manufacturing* 11 (June): 1223–30. https://doi.org/10.1016/j.promfg.2017.07.248.

Wicaksono, Ananto Yusuf. 2020. "Applying ISO:31000:2018 as Risk Management Strategy on Heavy Machinery Vehicle Division." *International Journal of Science, Engineering, and Information Technology* 4 (2): 198–202. https://doi.org/10.21107/ijseit.v4i2.6871.