Applied Information Systems and Management (AISM)
Volume 3, (2) 2020, hal 101-106
P-ISSN: 2621-2536; E-ISSN: 2621-2544

Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Framework Cobit 5 (Studi Kasus)

Muhammad Kamal Sani Firdaus

Abstract*— Kemungkinan adanya ancaman dan risiko TI (Teknologi Informasi) yang muncul seiring dengan penerapan IT Governance dapat menganggu proses bisnis yang berjalan. Hal ini penting bagi suatu perusahaan untuk menerapkan manajemen risiko TI. Dalam penerapannya, PLN P2B didukung oleh Divisi Teknologi Informasi dan Telekomunikasi sebagai penyedia layanan TI. Diketahui permasalahan yang sedangdialami PLN P2B adalah insidenkehilangan datayang diakibatkan adanya kegagalan dalam migrasi data ketika PLN P2B mengupgrade server dari 3-node clusters menjadi 6-node clusters. Oleh karena itu, diperlukan adanya evaluasi terhadap manajemen risiko TI sesuai dengan standar yang ada. Penelitian ini bertujuan untuk mengetahui tingkat kapabilitas manajemen risiko TI menggunakan metodologi Process Assessment Model (PAM)COBIT 5 yang terdiri dari tahapan Initiation, Planning the Assesment, Briefing, Data Collection, Data Validation, Process Attribute Level dan Reporting the Result. Hasil dari penelitian ini menunjukan tingkat pengelolaan risiko dan pengoptimalan risiko saat ini berada pada level 3 (Established Process) dan berdasarkan hasil penilaian risiko terdapat 6 risk issue yang tingkat risikonya di atas batas risk appetite. Sehingga PLN P2B direkomendasikan untuk menerapkan dan mengemb angkan DRP (Disaster Recovery Plan) berdasarkan kerangka kerja yang didesain untuk mengurangi dampak terhadap fungsi dan proses bisnis utamanya. Selain itu PLN P2B direkomendasikan menentukan dan mengimplementasikan langkah pengamanan fisik sesuai dengan persyaratan. Salah satunya dengan menempatkan database server di tempat yang aman. Dengan demikian diharapkan hasil penelitian ini dapat dijadikan bahan pertimbangan PLN P2B dalam melakukan perbaikan tata kelola TI agar dapat berjalan lebih optimal..

***Index Terms*— IT Governance, Manajemen Risiko,Disaster Recovery Plan, Business Continuity Plans, Risk Assessment**

I. PENDAHULUAN

IT Governance saat ini menjadi salah satu *critical success factor* (CSF) bagi organisasi untuk mengoptimalkan peran TI dalam efektifitas peningkatan aset, capaian kinerja, sasaran, tujuan, visi dan misi organisasi[1]. Namun tidak dapat dipungkiri bahwa kemungkinan berbagai ancaman dan risiko yang muncul dalam penerapan *IT governance* akan mengganggu bahkan melumpuhkan aktivitas di dalam penerapannya tidak dapat berjalan secara optimal (Rilyani et al., 2015). Risiko-risiko yang muncul diakibatkan penerapan *IT governance,* berpotensi memiliki dampak pada organisasi jika tidak ditangani secara serius. Selain menimbulkan risiko operasional, juga akan mempengaruhi risiko reputasi dan berdampak pada menurunnya tingkat kepercayaan publik. Oleh karena itu pentingnya manajemen risiko TI diterapkan adalah untuk menjaga keseimbangan proses bisnis juga menghindari perusahaan dari risiko-risiko yang tidak diinginkan. Berdasarkan peraturan Menteri BUMN No. PER-01/MBU/2011 Tanggal 1 Agustus 2011 tentang penerapan Tata Kelola Perusahaan yang baik (*Good Corporate Governance* – GCG) pada Badan Usaha Milik Negara pada bagian keenam Pasal 25 menyebutkan bahwa dalam setiap pengambilan keputusan/tindakan, harus mempertimbangkan risiko usaha serta wajib membangun dan melaksanakan program manajemen risiko korporasi secara terpadu yang merupakan bagian dari pelaksanaan program GCG.

PLN P2B (Pusat Pengatur Beban) adalah unit induk PLN yang dibentuk atas Keputusan Direksi PLN nomor 093.K/023/DIR/1995 mempunyai tugas dalam mengelola transaksi energi dalam menjalankan proses bisnisnya, PLN didukung oleh Divisi TI-Telkom dalam sebagai penyedia sarana infrastruktur, pengamanan jaringan, pengelolaan data, *user support* yang mendukung proses kerja. Dalam proses kegiatan tersebut selain dapat mempercepat kinerjanya, juga memiliki risiko yang berpotensi menimbulkan kerugian. Untuk mengukur sejauh mana pencapaian PLN P2B Jawa Bali dalam

M.K.S. Firdaus, a student of Department of Information System UIN Syarif Hidayatullah Jakarta Indonesia. (kamalsanifirdaus@gmail.com)

Received: 2 Juli 2018; Revised: 6 Juli 2020; Accepted: 8 November 2020

mengelola penerapan manajemen risiko TI dibutuhkan sebuah evaluasi. PT PLN P2B pernah mengalami kerugian finansial akibat kegagalan migrasi data serta terjadinya kerusakan pada back-up data sehingga PT PLN P2B kehilangan data.

Berdasarkan permasalahan tersebut maka dapat diidentifikasi rumusan masalah yaitu "bagaimana melakukan evaluasi manajemen risiko TI menggunakan *framework* COBIT 5 di PLN P2B". Evaluasi tersebut bertujuan untuk mengetahui *capability level*, *gap* dan mengidentifikasi risiko. Dari hasil evaluasi tersebut menghasilkan rekomendasi dan langkah mitigasi yang dapat digunakan PLN P2B dalam meningkatkan pencapaian kapabilitas serta meminimalisir dampak dan kemungkinan terjadinya risiko itu kembali.

Penelitian ini menggunakan metode analisis data dengan tahapan *Assessment Process Activities* dari COBIT 5 yang dimana fokus pada domain proses EDM03 dan APO12. Sedangkan untuk metode pengumpulan data terdiri dari observasi, wawancara, kuesioner dan studi literature.

Manfaat dari penelitian ini adalah untuk memberikan gambaran pada perusahaan mengenai tata kelola teknologi informasi yang baik. Membantu perusahaan dalam mengetahui gap yang tterdapat dalam pengelolaan TI terutama pada proses manajemen risiko TI.

II. LITERATUR REVIEW

Penelitian evaluasi tata kelola TI bertujuan untuk mengetahui sejauh mana pengelolaan dan pemanfaatan TI dalam meningkatkan pelayanan TI. (Hakim et al., 2014). Tata kelola yang efektif dengan TI telah menjadi sebuah keharusan bagi banyak perusahaan. Karena alasan ini semakin banyak kerangka kerja yang dikembangkan untuk menanggapi kebutuhan bisnis yang terus berubah. Salah satunya adalah COBIT (Pasquini & Galiè, 2013)

Terdapat beberapa penelitian sebelumnya tentang evaluasi tata kelola informasi khususnya evaluasi manajemen risiko teknologi informasi yang peneliti jadikan acuan.

Telah dilakukan penelitian tentang evaluasi pengelolaan risiko teknologi informasi (TI) pada instansi pemerintahan di Direktorat Jenderal Kependudukan dan Pencatatan Sipil kementerian Dalam Negeri (Samaptoaji,2014). Penelitian dilakukan dengan menyusun profil risiko TI sebagai salah satu langkah untuk melakukan pengelolaan risiko TI dengan menggunakan standar *framework* RiskIT dan teridentifikasi terdapat 64 *risk issue* dalam penggunaan TI, yang dikelompokan ke dalam 23 *high level* skenario risiko.

Telah dilakukan penelitian tentang analisis risiko teknologi informasi menggunakan framework ISO31000 pada i-Gracias Telkom(Novia et al., 2015). Hasil dari penelitian ini diketahui terdapat 43 Risk Issue yang teridentifikasi. Risiko paling tinggi yaitu database server down. Kemudian diberikan rekomendasi untuk mengatasi risiko tersebut.

Telah dilakukan penelitian ini tentang evaluasi pelaksanaan manajemen risiko teknologi informasi pada Kantor Arsip Daerah Kota Samarinda (Nurcahyono & Djunaedi, 2013). Penelitian ini menggunakan The RiskIT *Framewor*k. Hasil dari penelitian ini adalah Dari hasil penelitian tersebut diketahui bahwa kondisi tingkat kematangan saat ini di Kantor Arsip Daerah Kota Samarinda untuk domain Tata Kelola Risiko rata-rata *repeatable but intuitive*, domain Evaluasi Risiko rata-rata *defined* dan domain Respon Risiko rata-rata *repeatable but intuitive* yang dimana berarti tingkat kematangannya berada dalam kondisi proses pengembangan kedalam tahapan yang prosedur.

.

III. METODE PENELITIAN

Metode analisis data dilakukan dengan menggunakan *Assessment Process Activities*, yang terdiri dari:

1. *Initiation*, pada tahap ini peneliti melakukan identifikasi awal profil PT PLN P2B bertujuan untuk memperoleh pemahaman tentang organisasi saat ini dan mengumpulkan data dan informasi untuk mengetahui kondisi organisasi saat ini yang nantinya akan dievaluasi.
2. *Planning the assessment*, Tahap kedua melakukan rencana penilaian yang bertujuan untuk mendapatkan data yang dibutuhkan, mengkonversikan struktur organisasi yang terdapat di COBIT 5 terhadap fungsional-fungsional yang terdapat dalam struktur organisasi Divisi TI-Telkom PLN P2B kemudian membuat kuesioner yang dikembangkan dari COBIT 5.
3. *Briefing*, tahap ini peneliti memberikan pengarahan kepada responden yang ada pada diagram RACI sehingga memahami input, proses dan output dalam unit organisasi dan menjelaskan jadwal penelitian yang akan dilakukan.
4. *Data Collection*, Pada tahap ini melakukan pengumpulan data dari hasil temuan yang terdapat pada sistem yang dijalankan oleh PLN P2B.
5. *Data Validation*, Pada tahap ini melakukan validasi data dari kuesioner yang telah diisi para responden sesuai dengan identifikasi diagram RACI.
6. *Process Attribute Level*, Pada tahap ini peneliti memberikan tingkat pada atribut yang ada pada setiap indikator proses kapabilitas.
7. *Reporting the Result*, Pada tahap ini peneliti melaporkan hasil dari evaluasi yang telah dilakukan dengan memberikan laporan dari hasil identifikasi risiko dan analisis kesenjangan yang dimananya bisa dijadikan perusahaan untuk dapat mencapai level yang diharapkan (to be).

IV. IMPLEMENTASI DAN UJICOBA

Hasil Analisis

No.	Kategori Aset	Jumlah *Risk Issue*	Persentase
1	Aplikasi	3	17.6%
2	Fasilitas	1	5,9%
3	Infrastruktur TI	5	29.4%
4	Informasi / Data	3	17.6%
5	Proses	2	11.8%
6	SDM	3	17.6%
	TOTAL	17	100%

Capability Level* dan *Gap

Berdasarkan data hasil kuesioner yang telah divalidasi dengan data wawancara dan observasi terhadap bukti atau dokumen pendukung. Dihasilkan nilai *capability level* untuk domain proses EDM03 dan APO12 PT PLN P2B Jawa Bali berada pada level 3 (*Established Process*) dan kondisi yang diharapkan dari perusahaan pada domain EDM03 dan APO12 berada pada level 4 (*Predictable Process*) Sehingga dapat disimpulkan terdapat gap sebesar 1 level.

Tabel 1 Rekapitulasi Hasil Capability Level

Nama Proses	As is	To be
EDM03 (*Ensure Risk Optimisation*)	3	4
APO12 (*Manage Risk*)	3	4

Pada proses EDM03 *Ensure Risk Optimisation* dan APO12 *Manage Risk* berada pada level 3 yang artinya Proses pengoptimalan risiko dan pengelolaan risiko di PT PLN P2B telah diimplentasikan menggunakan proses yang telah ditetapkan. Dari hasil tersebut diketahui terdapat gap yang harus dipenuhi oleh PLN P2B, berikut ini adalah hasil analisis gap:

- Belumteridentifikasinya tanggung jawab pada proses optimasi risiko.
- Belum teridentifikasinya proses penyediaan sumber daya dan informasi untuk mendukung performa optimasi risiko.
- Belum optimalnya divisi TI dalam merespon sebuah perubahan risiko dengan cepat.
- Belum optimalnya penggunaan SOP terkait dengan pengelolaan *database*.

5.2. Hasil *Risk Assesment*

Tahapan *Risk Assessment* ini meliputi tahap analisis risiko dan tahap evaluasi risiko.

1. Analisis Risiko

Analisis Risiko bertujuan untuk menentukan seberapa sering risiko tersebut dapat terjadi dan seberapa besar dampak yang dihasilkan oleh risiko tersebut.Analisis Risiko diawali dengan melakukan identifikasi risiko, menentukan parameter *probability*, parameter *impact* risiko dan *rating* risiko. Setelah itu peneliti melakukan penilaian risiko terhadap *inherent risk* dan *residual risk*. Adapun pengelompokan risiko berdasarkan aset dapat dilihat pada tabel berikut:

Tabel 2 Risiko Berdasarkan Aset

Dari tabel tersebut diketahui bahwa kategori risiko berdasarkan aset terbanyak adalah kategori Infrastruktur TI yang mempunyai persentase 29,4% dengan jumlah sebanyak 5 risk issue.

Tabel 3 Risiko Berdasarkan Skenario

No.	Skenario Risiko	Jumlah *Risk Issue*
1.	*Ageing of Application Software*	1
2.	*Software Implementation*	2
3.	*Utilities Performance*	1
4.	*Infrastructure Theft*	1
5.	*Destruction of Infrastructure*	1
6.	*Infrastructure (Hardware)*	1
7.	*Ageing of Infrastructural Software*	1
8.	*Acts of Nature*	1
9.	*Database Integrity*	1
10.	*Logical Trespassing*	1
11.	*Operational IT Errors*	1
12.	*Malware*	1
13.	*Logical Attacks*	1
14.	*IT Staff*	2
15.	*IT Expertise and Skills*	1
	Total	17

Berdasarkan tabel tersebut diketahui bahwa skenario risiko terbanyak dalam jumlah risiko yaitu *Software Implementation* dan *IT staff*, masing masing dengan jumlah 2 *risk issue.*

Dari hasil rekapitulasi risiko berdasarkan aset dan skenario risiko serta mempertimbangkan nilai risiko berdasarkan dampak dan kemungkinannya. Maka dapat diketahui nilai

risikonya. Adapun rekapitulasi hasil penilaian risiko yang disusun berdasarkan aset dapat dilihat pada tabel berikut ini:

Tabel 4. Rekaputilasi Hasil Penilaian Risiko Berdasarkan Aset

No.	Kategori Aset	Nilai Risiko Dasar				
		R	MR	M	MT	T
1	Aplikasi	3				
2	Fasilitas	1				
3	Infrastruktur TI	4		1		
4	Informasi		1	2		
5	Proses	2				
6	SDM	1		2		
	Total	10	2	5		

2. Evaluasi risiko

Evaluasi risiko bertujuan untuk mengevaluasi apakah risiko – risiko tersebut dapat ditoleransi atau tidak oleh perusahaan. Evaluasi Risiko dilakukan dengan menggambarkan hubungan antara *probability* (kecenderungan) dan *impact* (dampak) ke dalam sebuah matriks yang disebut dengan *risk map*. Dengan menggunakan risk map perusahaan dapat lebih mudah memahami rating risiko dari setiap *risk issue*.

Gambar 1. Risk Map

Nilai		Impact					
		Sangat Kecil (1)	Kecil (2)	Sedang (3)	Besar (4)	Sangat Besar (5)	Total
Probability	Sangat Jarang (1)		**(11)**	**(1)**	**(1)**		13
	Jarang (2)		**(1)**	**(3)**			4
	Kadang - kadang (3)						
	Sering (4)						
	Sangat Sering (5)						
	Total		12	4	1		

Berdasarkan *risk map* di atas, untuk mengetahui rating risiko didapat dari perkalian nilai *impact* dan *probability*. Dari hasil tersebut diketahui bahwa distribusi risiko berdasarkan dampaknya yang termasuk dalam kategori kecil ada 12 buah risiko, kategori sedang 4 buah risiko dan besar 1 risiko. Sedangkan dari sisi kecenderungan (*probability*), dalam kategori sangat jarang terdapat 13 buah risiko dan kategori jarang tedapat 4 buah risiko.Dari *risk map* dapat diketahui ada 6 *risk issue* yang masih berada di luar batas risiko yang dapat diterima perusahaan. Oleh karena itu perlu diambil langkah mitigasi pada setiap *risk issue* tersebut.

5.3. Pembahasan

Pada hasil *assessment risk*, risiko yang teridentifikasi digambarkan melalui *risk map*, hal ini sesuai dengan teori dari ISACA (2009), yaitu tehnik yang umum dan mudah untuk mempresentasikan risiko adalah dengan menggunakan *Risk Map*, dimana risiko diplot pada diagram dua dimensi, dengan frekuensi dan dampak pada dimensinyarepresentasi *risk map* sangat kuat dan memberikan pandangan yang lengkap tentang risiko TI dan area tindakan yang jelas. Hal ini juga sejalan dengan penelitian Samaptoaji (2014) yang menggunakan risk map dan membaginya dalam 5 kategori risiko.

Berdasarkan hasil analisis gap pada proses EDM03 dan APO12 peneliti memberikan rekomendasi berupa penyesuaian keahlian SDM dengan peran dan tanggung jawabnya. Terutama untuk pengoptimalan risiko, dibuat tim khusus pada divisi TI atau individu yang bertanggung jawab penuh atas proses pengoptimalan risiko. Serta mendokumentasikan mekanisme yang tepat dalam mengelola sebuah perubahan risiko secara rinci dengan melakukan proses identifikasi terhadap risiko risiko apa saja yang tidak terduga, seperti teknologi baru.

Berdasarkan hasil *assessment risk*, peneliti memberikan rekomendasi dari langkah mitigasi berupa menentukan dan mengimplementasikan langkah pengamanan fisik sesuai dengan persyaratan. Salah satunya dengan menempatkan *database server* di tempat yang aman. Serta mengembangkan *IT Continuity Plan* berdasarkan kerangka kerja yang didesain untuk mengurangi dampak terhadap fungsi dan proses bisnis utama. Dengan membuat DRP (*Disaster Recovery Plan*)

Penelitian ini memiliki beberapa keterbatasan yaitu, ruang lingkup penelitian hanya pada divisi TI saja. Sehingga penentuan narasumber pun berdasarkan struktur organisasi divisi TI. Serta penelitian ini hanya sampai tahap penilaian dan pemberian rekomendasi saja tidak sampai tahap implementasi.

V. KESIMPULAN

Setelah melakukan evaluasi manajemen risiko TI di PT PLN P2B dengan mengetahui tingkat kemampuan PLN P2B dalam mengelola risiko, serta menganalisis dan melakukan penilaian terhadap risiko-risiko yang ada dengan menggunakan *framework*COBIT 5 diketahui bahwa tingkat kapabilitas saat ini (*as is*) Divisi TI-Telkom PLN P2B dalam mengelola risiko TI rata rata berada berada pada level 3 (*Established Process*). Sementara tingkat kapabilitas yang diharapkan dalam mengelola risiko TI berada pada level 4 (*Predictable Process*). Besarnya gap yang terbentuk antara nilai *capability* saat ini dan nilai *capability* yang diharapkan adalah sebesar 1 tingkat. Selain itu diketahui bahwa terdapat 17 *risk issue* dalam penggunaan TI. Secara umum tingkat risiko TI adalah rendah yaitu 64,7% (11 *risk issue*) dan 35,29% (6 *risk issue*) yang tingkat risikonya di atas batas *risk appetite*.

Sehingga PLN P2B direkomendasi menentukan dan menerapkan prosedur untuk *backup* dan restorasi sistem, aplikasi, data dan dokumentasi sesuai dengan kebutuhan bisnis dan rencana kontinuitas. Selain itu, PLN P2B direkomendasikan menetapkan dan menerapkan prosedur penyimpanan data yang efektif dan efisien, pengarsipan yang efektif dan efisien untuk memenuhi tujuan bisnis. Kebijakan keamanan dan persyaratan peraturan organisasi. Serta sesuai dengan permasalahan utama PLN P2B direkomendasikan mengembangkan *IT Continuity Plans* berdasarkan kerangka kerja yang didesain untuk mengurangi dampak terhadap fungsi dan proses bisnis utama. Dengan membuat DRP (*Disaster Recovery Plan*).

Selanjutnya hasil rekomendasi yang diberikan dapat dijadikan bahan pertimbangan oleh PLN P2B dalam melakukan perbaikan tata kelola terkait dengan manajemen risiko agar penerapan TI di PLN P2B lebih optimal.

Pada penelitian selanjutnya, dapat menggunakan ruang lingkup yang lebih luas agar informasi yang didapatkan tidak hanya dari divisi TI saja, tapi juga dari *top level management*. Selain itu, penelitian ini diharapkan dapat dilanjutkan sampai tahap perancangan dan implementasi.

REFERENCES

[1]. Hakim, A., Saragih, H., & Suharto, A. (2014).Evaluasi Tata Kelola Teknologi Informasi dengan Framwork COBIT. 5 di Kementerian ESDM. *Journal of Information Systems*, *10*(2).

[2]. [1] Handeri. (2014). Good IT Governance: Framework and Prototype for Higher Education, (1), 1–5

[3]. ISACA. (2009). *The Risk IT Framework Excerpt*. USA.

[4]. ISACA (2012), COBIT 5 *For Risk* . USA

[5]. ISACA. (2012). *COBIT 5 A Business Framework for the Governance and Management of Enterprise IT.* USA: IT Governance Institute.

[6]. ISACA. (2012). *COBIT 5 Enabling Processes.* USA: IT Governance Institute.

[7]. Hakim, A., Saragih, H., & Suharto, A. (2014).Evaluasi Tata Kelola Teknologi Informasi dengan Framwork COBIT. 5 di Kementerian ESDM. *Journal of Information Systems*, *10*(2), 105–117.

[8]. Handeri. (2014). Good IT Governance: Framework and Prototype for Higher Education, (1), 1–5.

[9]. ISACA. (2009). *The Risk IT Framework Excerpt*. USA.

[10]. ISACA (2012), COBIT 5 *For Risk* . USA

[11]. ISACA. (2012). *COBIT 5 A Business Framework for the Governance and Management of Enterprise IT.* USA: IT Governance Institute.

[12]. ISACA. (2012). *COBIT 5 Enabling Processes.* USA: IT Governance Institute.

[13]. Novia, A., Yanuar, R., W, F. A., & Dwi, D. J. (2015). Analisis Risiko Teknologi Informasi Berbasis Risk Management Menggunakan ISO Information Technology Risk Analysis Based On Risk Management Using Iso 31000 (Case Study : i-Gracias Telkom University), *31000*(2), 6201–6208.

[14]. Nurcahyono, D., & Djunaedi, A. (2013). Evaluasi Pelaksanaan Manajemen Risiko Teknologi Informasi pada Kantor Arsip Daerah Kota Samarinda dengan Menggunakan The Risk IT Framework. *Jnteti*, *2*(3), 3–6.

[15]. Pasquini, A., & Galiè, E. (2013). COBIT 5 and the Process Capability Model. Improvements Provided for IT Governance Process. *Proceedings of FIKUSZ '13 Symposium for Young Researchers*, 67–76.

[16]. Samaptoaji, S. (2014). Evaluasi Pengelolaan Risiko Teknologi Informasi (TI) pada Instansi Pemerintahan Studi Kasus Direktorat Jenderal Kependudukan dan Pencatatan Sipil Kementerian Dalam Negeri.

[17]. Snedaker, S., & Rima, C. (2014). *Business Continuity and Disaster Recovery Planning for IT Professionals Business Continuity and Disaster Recovery Planning for IT Professionals Second Edition*.

[18]. Spremic, M, and Popovic, M. (2008). *Emerging issues in IT Governance: Implementing the Corporate IT Risk Management Model, WSEAS Transactions in Systems, issues 3 volume 7*

Westerman, George and Richard Hunter. (2007). *IT Risk: Turning Business Threats Into Competitive Advantage*. Harvard Business School Press.