PENGUKURAN M ANAJEMEN RISIKO TI DI PT.X MENGGUNAKAN COBIT 5

Myrna Dwi Rahmatya, Ana Hadiana, Irfan Maliki
Universitas Komputer Indonesia

Program Pasca Sarjana, Program Studi Magister Sistem Informasi
Jl. Dipati Ukur No. 112-116, Bandung 40132
e-mail: myrna1412@ymail.com, ana.hadiana@lipi.go.id, irfanmaliki007@gmail.com

ABSTRAK

PT. X menerapkan *Good Corporate Governance* (GCG) sesuai dengan Peraturan Menteri Negara BUMN Nomor: Per-01/MBU/2011 tentang Penerapan Tata Kelola Perusahaan yang Baik (*Good Corporate Governance*) pada BUMN. Sebagai salah satu bagian dari penerapan GCG, PT. X membentuk unit kerja manajemen risiko. Namun, manajemen risiko pada PT. X, khususnya risiko TI belum berjalan dengan baik sebab masih ditemukannya permasalahan terkait TI yang dapat menganggu operasional.

Penelitian ini bertujuan mengukur manajemen risiko TI PT. X dengan menggunakan *capability level* COBIT 5, melakukan analisis *gap* dan memberikan rekomendasi berupa langkah yang dapat dilakukan untuk dapat mencapai manajemen risiko TI yang diharapkan sehingga dapat meminimailisir tingkat kegagalan/kerugian.

Metodologi penelitian yang digunakan ialah merumuskan permasalahan yang ada, melakukan studi literatur, mencari proses pada COBIT 5 yang dapat memberikan solusi terhadap permasalahan yang ada, mengumpulkan data, menentukan target *capability level* manajemen risiko TI yang diharapkan, analisis *gap* dan memberikan rekomendasi untuk dapat mencapai *capabiliy level* yang diharapkan.

Berdasarkan hasil analisis manajemen risiko TI pada PT. X berada di level 1 (*performed process*), yaitu EDM03, APO12, DSS01, DSS05, MEA02. Manajemen risiko TI di PT. X masih belum terorganisir. Sementara itu, *capability level* yang ingin dicapai ialah level 2 (*managed process*).

Untuk dapat mencapai level tersebut PT. X perlu meningkatkan *capability level* manajemen risiko TI level 1, yaitu dengan memelihara keamanan informasi, memantau dan meningkatkan kontrol internal, menganalisis kekurangan pada kontrol, meningkatkan kinerja operasional dan sistem kontrol internal. Sedangkan langkah untuk dapat mencapai level 2, yaitu dengan mengelola kinerja proses dan mengelola kriteria serta kualitas *work product* dari setiap proses.

Kata kunci: Manajemen Risiko TI, COBIT 5

1. Pendahuluan

PT. X merupakan BUMN yang menerapkan *Good Corporate Governance* (GCG) sesuai dengan Peraturan Menteri Negara BUMN Nomor: Per-01/MBU/2011 tentang Penerapan Tata Kelola Perusahaan yang Baik (*Good Corporate Governance*) pada BUMN. Sebagai salah satu bagian dari penerapan GCG, PT. X membentuk unit kerja manajemen risiko.

Manajemen risiko dilakukan untuk mengenali dan mengelola risiko serta kejadian-kejadian yang mungkin akan muncul, meminimalkan dampaknya dan menentukan penanganan risiko yang tepat untuk meningkatkan peluang sukses.

Namun, manajemen risiko pada PT. X, khususnya risiko TI belum berjalan dengan baik sebab masih ditemukannya permasalahan, seperti kehilangan/kerusakan database tanpa kejelasan siapa dan unit mana yang bertanggung jawab karena penggunaan *password* DBA yang dibagi pakai, *user* dan *password* diketahui oleh yang tidak berhak dan kecurangan ditemukan dalam waktu yang lama dikarenakan tidak adanya penghapusan *user* lama, waktu respon CPU melambat dan transaksi terganggu karena penggunaan aplikasi layanan transaksi di loket bercampur dengan aplikasi lain yang tidak berhubungan, tidak terpantaunya masa pakai komponen mesin yang dapat mengganggu terhentinya transaksi layanan dan sering terjadi kerusakan peralatan elektronik (alat komunikasi, *switch*, hub dan sebagainya) yang mengakibatkan terhentinya kegiatan.

Permasalahan tersebut menandakan bila manajemen risiko TI PT. X belum berjalan dengan baik. Akibatnya, kerusakan/kehilangan dan perubahan data oleh pihak yang tak berwenang dan kerusakan perangkat TI yang dapat mengganggu operasional.

Karena itulah perlu dilakukan pengukuran terhadap manajemen risiko TI yang berjalan saat ini untuk mengetahui kinerja manajemen risiko TI. Kekurangan yang ada pada manajemen risiko TI saat ini dapat menjadi dasar untuk menentukan langkah apa saja yang perlu dilakukan untuk dapat meningkatkan manajemen risiko dan menurunkan tingkat kegagalan/kerugian.

Pengukuran manajemen risiko TI menggunakan COBIT 5 karena memberikan kerangka kerja yang lengkap yang membantu perusahaan dalam mencapai tujuan untuk *IT Governance* dan *IT Management*. COBIT 5 juga membantu perusahaan dalam menciptakan nilai yang optimal dari TI dengan menjaga keseimbangan antara realisasi manfaat, optimasi risiko, dan optimasi sumber daya.

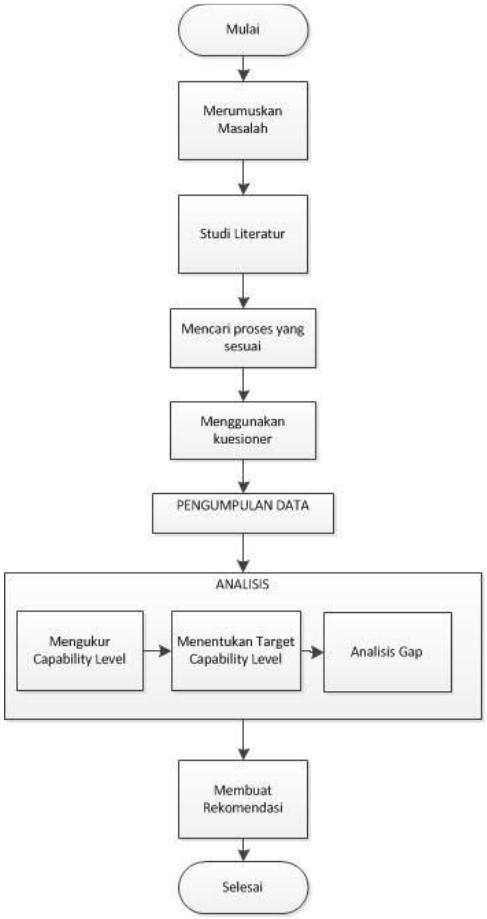
Menurut *IT Governance Institute*, perusahaan yang telah menerapkan COBIT 5 mengalami peningkatan manajemen risiko yang berkaitan dengan TI, meningkatkan komunikasi dan hubungan antara bisnis dengan TI, menurunkan biaya TI, meningkatkan penyampaian tujuan bisnis dan meningkatkan daya saing TI[8].

Selain itu, manfaat dalam penerapan COBIT 5 adalah untuk mengelola risiko terkait TI pada tingkatan yang dapat diterima, mengelola informasi dengan kualitas yang tinggi untuk mendukung keputusan bisnis, mencapai tujuan strategi dan manfaat bisnis melalui pemakaian TI secara efektif dan inovatif, mencapai tingkat operasional yang lebih baik dengan aplikasi teknologi yang handal dan efisien, mengoptimalkan biaya dari layanan dan teknologi TI, mendukung

kepatuhan terhadap hukum, peraturan, kontrak dan kebijakan.

2. Metode

Metodologi penelitian terdiri dari merumuskan masalah, analisis manajemen risiko dengan COBIT 5, membuat rekomendasi berdasarkan hasil analisis dan diakhiri dengan dokumentasi. Metodologi penelitian yang digunakan terlihat pada gambar.



2.1 Merumuskan Permasalahan

Pada tahap ini dilakukan perumuskan permasalahan yang terjadi terkait dengan manajemen risiko TI. Dengan adanya perumusan masalah, maka akan menjadikan panduan untuk penelitian ini agar mendapatkan tujuan akhir seperti yang diharapkan.

Manajemen risiko TI di PT. X belum berjalan dengan baik. Hal ini terlihat dari munculnya masalah-masalah berikut ini:

1. Penyalahgunaan hak akses, seperti penggunaan *password* DBA yang dibagi pakai sehingga mengakibatkan kehilangan/kerusakan database tanpa kejelasan siapa dan unit mana yang bertanggung jawab, *user* dan *password* diketahui oleh yang tidak berhak dan kecurangan ditemukan dalam waktu yang lama dikarenakan tidak adanya penghapusan *user* lama,
2. Waktu respon CPU melambat dan transaksi terganggu karena penggunaan aplikasi layanan transaksi di loket bercampur dengan aplikasi lain yang tidak berhubungan,
3. Tidak terpantaunya masa pakai komponen mesin yang dapat mengganggu terhentinya transaksi layanan dan sering terjadi kerusakan peralatan elektronik (alat komunikasi, *switch*, hub dan sebagainya) yang mengakibatkan terhentinya kegiatan operasional.

2.2 Studi Literatur

Pada tahap ini dilakukan studi dari berbagai pustaka yang relevan dengan kajian tesis. Studi literatur dilakukan dengan cara membaca jurnal / paper yang terkait dengan topik penelitian, studi literatur dari tesis terdahulu dan membaca buku yang berhubungan dengan manajemen risiko TI.

2.3 Menentukan Proses COBIT 5

Pada tahap ini dilakukan pemilihan proses dengan menggunakan *mapping* COBIT 5, khususnya yang berkaitan dengan optimasi. Proses yang dipilih, yaitu EDM03 *Ensure Risk Optimisation,* APO12 *Manage Risk*, DSS01 *Manage Operations*, DSS05 *Manage Security Services*, MEA02 *Monitor, Evaluate, and Assess the System of Internal Control.*

Sebagai tambahan proses DSS01 dipilih karena dianggap dapat memberikan solusi

terkait risiko di PT. X yang berhubungan dengan operasional, yaitu gangguan pada komponen mesin atau peralatan TI.

2.4 Menggunakan Kuesioner

Menggunakan kuesioner COBIT 5 yang berisi *output* dari setiap proses. Kuesioner tersebut dibagikan kepada empat responden, yaitu Bagian Pengembangan Perangkat Lunak, Bagian Infrastruktur, Bagian Kemanan TI dan Manajemen Risiko.

2.5 Pengumpulan Data

Pengumpulan data dilakukan melalui wawancara dan mengumpulkan kuesioner.

2.6 Analisis

Pada tahap ini dilakukan pengukuran proses terpilih dengan melakukan pemetaan *capability level* dan analisis gap. Dengan mengetahui *capability level* proses dapat diketahui kondisi manajemen risiko TI PT. X saat ini. Kemudian menentukan *capability level* yang ingin dicapai. Melalui analisis *gap*, level tersebut dibandingkan dengan level yang ingin dicapai.

2.7 Membuat rekomendasi

Setelah melakukan pemetaan dan analisis *gap*, dilanjutkan dengan membuat rekomendasi untuk penerapan manajemen risiko TI yang lebih efektif dan dapat mencapai level yang diharapkan.

3. Hasil dan Pembahasan

3.1 Hasil Pengukuran Proses

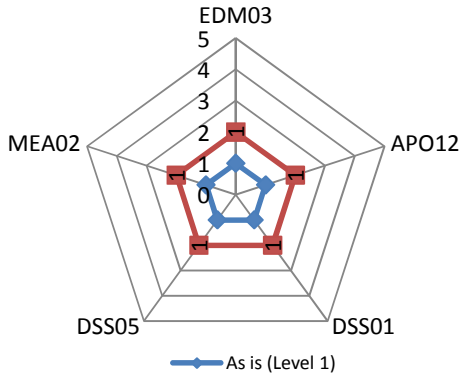
Berdasarkan hasil analisis secara umum manajemen risiko TI pada PT. X berada di level 1, yaitu EDM03, APO12, DSS01, DSS05 dan MEA02. PT. X telah menjalankan proses manajemen risiko TI namun belum berjalan dengan baik karena masih ditemui permasalahan-permasalahan terkait TI yang dapat berdampak pada operasional.

3.2 Capability Level yang Ingin Dicapai

Target *capability level* yang ingin dicapai dari setiap prosesnya ialah level 2. Pada level ini kinerja dan *work product* atau hasil proses dikelola dengan baik.

3.3 Analisis Gap

Berdasarkan hasil analisis terhadap 5 proses yang telah terpilih, umumnya proses-proses tersebut berada pada level 1 dimana proses masih bersifat *ad hoc* dan belum terorganisir. Berikut gambaran umum hasil pengukuran *capability level* seluruh proses:



Gambar 4. 1 Capability Level As is dan To be

Gambaran *gap* antara capability level saat ini dan yang ingin dicapai digambarkan pada tabel 4.6.

Tabel 4. 1 *Capability Level as is*, *to be* dan *gap*

No.	Proses	*As is*	*To be*	*Gap*
1	EDM03	1	2	1
2	APO12	1	2	1
3	DSS01	1	2	1
4	DSS05	1	2	1
5	MEA02	1	2	1

Berdasarkan tabel 4.6 dapat terlihat adanya *gap* sebesar 1 anatara *capability level* saat ini dengan yang diharapkan maka PT. X perlu melakukan tindakan untuk meningkatkan proses-proses yang belum sampai pada level yang diharapkan. Terdapat beberapa rekomendasi yang dapat PT. X lakukan untuk dapat mencapai *capability level*

2, yaitu memenuhi setiap proses yang masih berada di level 1 hingga mencapai *fully achieved* kemudian melakukan tindakan untuk dapat mencapai level 2.

3.4 Rekomendasi

Jika kelima proses tersebut telah mencapai level 1 dengan capaian *fully achieved* maka PT. X dapat melakukan tindakan untuk dapat meningkatkan proses-proses tersebut ke level 2, yaitu:

1. Menetapkan tujuan kinerja proses yang di dalamnya berisi uraian lingkup dan detail tujuan kinerja proses.
2. Merencanakan dan memantau kinerja proses. Catatan kinerja dapat berupa laporan atau daftar permasalahan.
3. Melakukan penyesuaian kinerja proses jika kinerja tidak sesuai dengan yang direncanakan. Perlu dilakukan identifikasi terhadap permasalahan kinerja, penyesuaian rencana dan menyediakan detail tindakan perbaikan.
4. Menetapkan siapa yang bertanggung jawab, pengalaman, pengetahuan dan keahlian seperti apa yang diperlukan dalam menjalankan proses. Dokumentasi kegiatan ini terdiri dari detail pemilik proses, siapa saja yang terlibat, siapa yang bertanggung jawab dan/atau perlu mendapatkan informasi terkait proses.
5. Menetapkan, menyediakan dan mengalokasikan sumber daya untuk melakukan proses.
6. Membuat rencana proses komunikasi dan memastikan komunikasi yang efektif dan tugas yang jelas antar pihak yang terlibat.
7. Menetapkan persyaratan *work product* yang meliputi detail kriteria, kualitas dan isi *work product*.
8. Menetapkan persyaratan dokumentasi kontrol *work product* yang terdiri dari detail kontrol, kriteria *work product*, dokumentasi dan kontrol perubahan.

4. Kesimpulan dan Saran

4.1 Kesimpulan

Berdasarkan hasil analisis dapat diambil beberapa kesimpulan mengenai pengukuran manajemen risiko TI, yaitu sebagai berikut:

1. Memetakan *capability level* manajemen risiko TI di PT. X menggunakan COBIT 5. Berdasarkan hasil analisis secara umum manajemen risiko TI pada PT. X berada di level 1, yaitu EDM03, APO12, DSS01, DSS05 dan MEA02. PT. X telah menjalankan proses manajemen risiko TI namun belum berjalan dengan baik karena masih ditemui permasalahan-permasalahan terkait TI yang dapat berdampak pada operasional.
2. Berdasarkan hasil analisis *gap* maka secara umum PT. X berada di level 1 dan terdapat *gap* sebesar 1 untuk mencapai level 2. Berikut rekomendasi untuk dapat meningkatkan *capability level* manajemen risiko TI:
   a. Melengkapi semua proses di level 1. Kemudian melakukan *assessment* untuk mengetahui apakah kelima proses tersebut telah mencapai level 1 dengan capaian *fully achieved. Assessment* dapat dilakukan setelah usaha peningkatan level dijalankan selama 1-3 tahun.
   b. Jika level 1 sudah terpenuhi maka untuk dapat mencapai level yang diharapkan, yaitu level 2 dengan mengelola kinerja proses (merencanakan, memantau, menyesuaikan dan menentukan siapa saja yang terlibat) dan mengelola kriteria serta kualitas *work product* dari setiap proses.

4.2 Saran

Penelitian ini memiliki keterbatasan, yaitu hanya menilai area manajemen risiko. Oleh karena itu, untuk penelitian selanjutnya dapat

mengembangkan penelitian ke area *IT governance* lainnya.

Sementara itu, saran bagi PT. X ialah bila melakukan peningkatan terhadap 5 proses terpilih maka perlu melakukan pemantauan terhadap proses-proses tersebut dan terus melakukan penyesuaian untuk mencapai *capability level* yang diharapkan dari manajemen risiko TI.

5. Daftar Pustaka

[1]. Hopkin, Paul. 2010. *Fundamentals of Risks Management : Understanding, Evaluating and Implementing Effective Risk Management*. Kogan Page. London.

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

[3]. ISACA. 2012. COBIT 5: *Enabling Process*. ISACA

[4]. ISACA. 2012. COBIT 5 Toolkit: COBIT and GRC. ISACA

[5]. ISACA. 2012. *Process Assessment Model (PAM): Using COBIT 5*. ISACA

[6]. ISACA. 2013. Mapping to COBIT 5. Melalui http://www.isaca.org/Certification/CGEIT-Certified-in-the-Governance-of-Enterprise-IT/Prepare-for-the-Exam/Mappin-to-COBIT/Pages/default.aspx.

[7].IT Governance Institute. 2007. *COBIT 4.1*. IT Governance Institute.

[8]. Khanyile, Slindile. Abdullah, Hanifa. COBIT 5: *An Evolutionary Framework and Only Framework to Address The Governance and Management of Enterprise IT*. UNISA.

[9].Kouns, Jake. Minoli., Daniel. 2010. *Information Technology Risk Management in Enterprise Environments*. Wiley. USA

[10].Maulana, Muhammad Mahreza. Supangkat, Suhono Harso. 2006. Prosiding Konferensi Nasional Teknologi Informasi dan Komunikasi untuk Indonesia. *Pemodelan Framework Manajemen Resiko TI untuk Perusahaan di Negara Berkembang*. Mei. p.122

[11].Rafeq, A. 2012. *Systems Audit of GRC Using COBIT 5*. The Chartered Accountant.

[12].Stoneburner, Gary. 2002. *Risk Management Guide for Information Technology Systems: Recomendations of the National Institute of Standards and Technology*. U.S. Departement of Commerce.

[13].The Intermational Organization for Standardization. 2009. *Risk Management*. Principles and Guidelines. The International Organization for Standardization. Switzerland.

[14].Vaughan, Emmet J. Vaughan, Therese M. 2008. *Fundamentals of Risk and Insurance*. John Wiley & Sons. USA.