Jurnal Sistem Informasi Bisnis 02(2024)
Copyright ©2024, JSINBIS, p-ISSN: 2502-2377, e-ISSN: 2088-3587
On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/58584

Audit Tata Kelola Teknologi Informasi dalam Mendukung Penerapan *Good Corporate Governance* (Studi Kasus PT XYZ)

Agustin Simatupang*, Henricus Judi Adrianto

Magister Manajemen, Universitas Kristen Indonesia, Jakarta, Indonesia

Naskah masuk: 5 Desember 2023; Diterima untuk publikasi: 5 Maret 2024
DOI : 10.21456/vol14iss2pp162-170

Abstract

The development of Information Technology (IT) is rapidly growing and has increasing risks. Based on the Decision of the Ministry of State-Owned Enterprises S-122-MBU-DSI-05-2021 regarding the implementation guidelines for the assessment of IT Maturity Levels, companies are required to carry out an independent assessment of the maturity level of information technology. This research aims to assess the governance of IT risk management using the COBIT 2019 framework. The research method was carried out using descriptive qualitative methods using the COBIT 2019 framework and literature review, as well as through interviews, observations, questionnaires and review of company documents. The assessment results showed an average maturity level of 3.00 (Established) for 2 COBIT 2019 processes which were considered relevant to Information Technology Risk Management. On average, the 2019 COBIT processes have been implemented at PT XYZ is already running well with the IT risk management maturity level at level 3 and initiatives are still needed to reach maturity level 4 or better. Maturity level 3 means the process has been managed and achieved its goals in a more organized manner using organizational assets and resources. The process has been well defined with policies and standard operating procedures for the process and is carried out in accordance with good risk management and supports the Good Corporate Governance. In the process of increasing the maturity level of information technology risk management to higher level, there are 7 (seven) main recommendations to be implemented so that the information technology risk management process can improve and the implementation of recommendations from the assessment results will be prioritized in the implementation roadmap IT according to Company needs and targets.

Keywords: Good Corporate Governance (GCG), COBIT 2019, Information Technology Governance, Risk Management, Information Technology.

Abstrak

Perkembangan Teknologi Informasi berkembang pesat dan memiliki risiko yang semakin meningkat. Berdasarkan Keputusan Kementerian Badan Usaha Milik Negara (BUMN) nomor S-122-MBU-DSI-05-2021 tentang Pedoman Pelaksanaan *Assessment* IT *Maturity Level* BUMN, perusahaan BUMN diwajibkan untuk melakukan penilaian terhadap tingkat kematangan teknologi informasi secara independen. Penelitian ini bertujuan untuk melakukan penilaian terhadap tata kelola manajemen risiko teknologi informasi (TI) dengan menggunakan *framework* COBIT 2019. Metode penilitian dilakukan dengan metode kualitatif deskriptif dengan kerangka kerja COBIT 2019 dan tinjauan literatur, juga melalui wawancara, observasi, kuisioner, dan *review* dokumen Perusahaan. Hasil *assessment* didapatkan rata-rata tingkat kematangan sebesar 3,00 (*Established*) untuk 2 proses COBIT 2019 yang dinilai relevan dengan Manajemen Risiko Teknologi Informasi. Secara rerata umumnya proses-proses COBIT 2019 yang telah diterapkan di PT XYZ sudah berjalan dengan baik dengan tingkat maturitas manajemen risiko TI berada pada level 3 dan masih perlu inisiatif agar dapat mencapai tingkat kematangan 4 atau lebih baik lagi. Adapun tingkat kematangan 3 bermakna proses telah dikelola dan mencapai tujuannya dengan lebih teroganisir dengan menggunakan aset dan sumber daya organisasi. Proses telah terdefinisi dengan baik dengan adanya kebijakan dan *standard operating procedures* untuk proses tersebut dan dijalankan sesuai manajemen risiko yang baik dan mendukung program *Good Corporate Governance* Perusahaan. Dalam proses peningkatan tingkat maturitas manajemen risiko teknologi informasi ke level yang lebih tinggi lagi, terdapat 7 (tujuh) rekomendasi utama yang perlu di implementasikan agar proses manajemen risiko teknologi informasi Perusahaan dapat meningkat dan penerapan rekomendasi dari hasil *assessment* akan di prioritaskan dalam *roadmap* penerapan Tata Kelola TI sesuai kebutuhan dan target Perusahaan.

Kata kunci: Tata Kelola Perusahaan yang baik, COBIT 2019, Tata Kelola Teknologi Informasi, Manajemen Risiko, Teknologi Informasi

*) *Corresponding author*: agus.simatupang@gmail.com

On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/58584

1. Pendahuluan

Perkembangan Teknologi Informasi semakin berkembang sangat pesat seiring kebutuhan seluruh perusahaan dalam menunjang operasional perusahaan agar lebih efektif dan efisien dalam mengelola usaha. Pada saat ini teknologi informasi (TI) menjadi bagian yang sangat penting bagi perusahaan atau institusi dengan skala wirausaha (Windasari, 2021).

Perkembangan ini memiliki risiko tersendiri dalam hal penerapan nya dan akan sangat berpengaruh terhadap operasional perusahaan jika risiko tersebut dapat terjadi maka perusahaan perlu melakukan tata kelola yang baik dalam menunjang penerapan teknologi informasi di suatu oraganisasi atau perusahaan. Teknologi informasi dan sistem informasi merupakan *tools* yang penting untuk mendukung tercapainya visi dan misi universitas. (Juliandarini, 2013).

Berdasarkan keputusan Kementerian Badan Usaha Milik Negara (BUMN) nomor S-122-MBU-DSI-05-2021 tentang Pedoman Pelaksanaan Assessment IT Maturity Level BUMN, perusahaan-perusahaan BUMN diwajibkan untuk melakukan penilaian terhadap tingkat kematangan teknologi informasi (TI) secara independen yang dilakukan oleh pihak independen. Perusahaan BUMN di arahkan untuk melakukan penilaian tingkat kematangan Teknologi Informasi dengan menggunakan standar framework COBIT versi 5 atau versi terbaru yaitu COBIT versi 2019.

Salah satu perusahaan BUMN yang turut melaksanakan keputusan tersebut adalah PT XYZ. Perusahaan manufaktur ini telah menerapkan suatu Tata Kelola Teknologi Informasi sesuai dengan arahan kementrian BUMN dan *best practice* di Indonesia dan sejalan dengan peraturan kementrian BUMN nomor PER-02-MBU-2013 tentang panduan penyusunan pengelolaan teknologi informasi badan usaha milik negara yang ada di Indonesia (Negara, 2018).

Perusahaan Badan Usaha Milik Negara (BUMN) dan swasta menyadari bahwa teknologi informasi memiliki peran penting dan strategis dalam mencapai kesuksesan. Oleh karena itu, banyak perusahaan yang mengalokasikan investasi untuk tetap kompetitif dan relevan dalam era bisnis yang baru dan berkembang saat ini. Dalam situasi seperti ini, pentingnya tata kelola teknologi informasi (TI) untuk memastikan bahwa investasi TI yang telah dilakukan perusahaan memberikan nilai tambah yang baik, mengurangi risiko bisnis terkait TI, dan memastikan bahwa kemampuan aset TI sejalan dengan tujuan bisnis yang ada. Dalam konteks ini, kebutuhan BUMN untuk mengevaluasi kapabilitas infrastruktur dan layanan TI yang dimiliki saat ini dipengaruhi oleh pengelolaan risiko TI.

Dalam melaksanakan *Assessmen*t IT *Maturity Level* pada proses Manajemen Risiko Teknologi Informasi, PT XYZ telah menerima rekomendasi untuk meningkatkan kematangan Tata Kelola TI guna mencapai tingkat *maturity level* minimal sebesar 3 (tiga) sesuai arahan dari Kementrian Badan Usaha Milik Negara dengan framework COBIT 2019. Rekomendasi ini penting untuk membantu perusahaan mencapai standar yang ditetapkan dalam peraturan pemerintah dan mendukung penerapan *Good Corporate Governance*.

Dalam rangka mencapai target tingkat *maturity level* manajemen risiko Teknologi Informasi yang diharapkan, PT XYZ perlu mengidentifikasi area-area perbaikan dalam Tata Kelola TI dan mengambil langkah-langkah yang tepat untuk meningkatkan kematangan tata kelola tersebut. Dengan demikian, perusahaan dapat memastikan bahwa pengelolaan dan penerapan teknologi informasi berjalan dengan baik sesuai dengan prinsip-prinsip *good corporate governance* dan peraturan yang berlaku.

2. Kerangka Teori

2.1. Risk IT Framework

Risk IT merupakan suatu *framework* yang didasarkan pada seperangkat prinsip-prinsip penuntun untuk pengelolaan yang efektif dari *Risk* IT *Framework* 2nd *edition* pelengkap COBIT versi 2019 (ISACA, 2020), *Risk* IT *framework* ini merupakan suatu *framework* komprehensif untuk tata kelola dan pengendalian usaha solusi berbasis IT dan layanan. *Risk* IT *framework* menjelaskan risiko terkait IT dan memungkinkan untuk mengidentifikasi risiko terkait IT yang melebihi penilaian teknis yang sempit dan karenanya memerlukan pertimbangan tingkat perusahaan yang holistik. Mengintegrasikan pengelolaan risiko terkait IT ke dalam proses *Enterprice Risk Management* (ERM) secara keseluruhan dan mengevaluasi risiko dan respons IT dalam konteks toleransi risiko perusahaan secara keseluruhan. Komponen *Risk* IT *Framewor*k dan penyelarasan dengan COBIT 2019 ditampilkan pada Gambar 1.

Gambar 1. Komponen Risk IT Framework

2.2. COBIT 2019

COBIT (*Control Objectives for Information and Related Technology*) versi 2019 (ISACA, 2019b) merupakan suatu standar dan panduan untuk aktivitas dan kontrol tata kelola Teknologi Informasi (TI).

Copyright ©2024, JSINBIS, p-ISSN: 2502-2377, e-ISSN: 2088-3587
On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/58584

COBIT versi ini membantu dalam mengoptimalkan investasi perusahaan dengan menggunakan TI, memastikan penyampaian layanan yang berkualitas, serta menyediakan ukuran yang jelas dalam menghadapi kesalahan atau kegagalan. Seiring dengan kemajuan teknologi dari waktu ke waktu, ISACA telah mengeluarkan beberapa versi COBIT, mulai dari versi 1 sampai versi 5, lalu versi 2019. Salah satu *framework* terbaru yang dikeluarkan oleh ISACA adalah COBIT versi 2019, yang merupakan pengembangan dari versi sebelumnya, yaitu COBIT versi 5. COBIT 2019 diperbarui dengan mempertimbangkan pada aspek perkembangan teknologi terkini yang dapat berdampak pada pengelolaan informasi dan teknologi dalam suatu organisasi atau perusahaan. Dalam COBIT 2019 terdapat *Governance and Management Objectives* pada COBIT dikelompokan menjadi lima domain, antara lain:

1) Domain EDM (*Evaluate, Direct and Monitor*) merupakan domain tata kelola, untuk mengevaluasi opsi strategik, mengarahkan manajemen senior pada opsi strategik yang dipilih, serta mengawasi pencapaian dari strategi yang dijalanlan;
2) Domain APO (*Align, Plan, and Organize*) mencakup keseluruhan organisasi, strategi, dan aktivitas penunjang untuk Teknologi dan Informasi terhadap proses bisnis;
3) Domain BAI (*Build, Acquire and Implement*) mencakup definisi, akusisi, dan implementasi dari solusi Teknologi dan Informasi serta integrasinya terhadap proses bisnis;
4) Domain DSS (*Deliver, Service and Suport*) mencakup pelaksanaan operasional dan bantuan dari layanan teknologi dan informasi termasuk keamanan;
5) Domain MEA (*Monitor, Evaluate, and Assess*) mencakup pemantauan kinerja dan kesesuaian dari Teknologi dan Infirmasi pada target kinerja internal, sasaran kontrol internal, dan kewajiban pada pihak eksternal.

Perusahaan didukung dalam merancang sistem tata kelola dengan menggunakan berbagai faktor desain yang telah disediakan. Dalam proses perancangan sistem tata kelola, terdapat 11 aspek dalam menentukan *design factors* yang harus dipertimbangkan agar proses yang di pilih dapat lebih fokus terhadap tujuan perusahaan pada tahun tersebut (ISACA, 2019b).

2.3. Domain EDM-03 COBIT 2019

Domain EDM (*Evaluate, Direct and Monitor*) adalah tahapan untuk melakukan evaluasi pada sisi strategik, mengarahkan manajemen senior pada pilihan strategik yang dipilih serta melakukan pengawasan pencapaian dari strategi yang di rencanakan dan telah dijalankan.

EDM-03, yang dikenal sebagai proses "*Ensured Risk Optimization*", berfokus untuk memastikan bahwa perusahaan telah memahami, mengartikulasikan, dan mengkomunikasikan selera dan toleransi risiko. Selain itu, risiko yang terkait dengan pemanfaatan teknologi informasi (TI) telah diidentifikasi dan dikelola dengan baik. Tujuan dari EDM-03 adalah untuk memastikan bahwa risiko terkait TI tidak melebihi selera dan toleransi risiko perusahaan. Selain itu, dampak risiko TI terhadap nilai perusahaan diidentifikasi dan dikelola dengan baik, dan potensi kegagalan kepatuhan dapat diminimalkan. EDM-03 memiliki 3 komponen proses sebagai berikut:

1) EDM03.01 *Evaluate risk management* dengan *output* yang diharapkan terdapat Panduan tingkat risiko, Dokumen evaluasi pelaksanaan manajemen risiko dan Persetujuan tingkat toleransi risiko;
2) EDM03.02 *Direct risk management* dengan output yang diharapkan terdapat Persetujuan terhadap proses pengukuran manajemen risiko, Deskripsi sasaran utama yang harus dipantau dari kegiatan manajemen risiko dan Kebijakan manajemen risiko;
3) EDM03.03 *Monitor risk management* dengan *output* yang diharapkan terdapat Dokumen pelaksanaan tindakan perbaikan terhadap ketidaksesuaian pelaksanaan manajemen risiko dan Penyampaian permasalahan manajemen risiko kepada *board* atau Manajemen.

2.4. Domain APO-12 COBIT 2019

Domain APO (*Align, Plan and Organize*) adalah tahapan yang mencakup keseluruhan organisasi, strategi, dan aktivitas penunjang untuk Teknologi dan Informasi dalam mendukung pencapaian dari strategi yang di rencanakan dan telah dijalankan Perusahaan.

APO-12, yang dikenal sebagai "*Managed Risk*", melibatkan proses terus-menerus dalam mengidentifikasi, menilai, dan mengurangi risiko yang terkait dengan teknologi informasi (TI) sesuai dengan batas toleransi yang ditetapkan oleh manajemen eksekutif perusahaan. Tujuan dari APO-12 adalah untuk mengintegrasikan manajemen risiko TI dengan manajemen risiko perusahaan secara keseluruhan dan mencapai keseimbangan antara biaya dan manfaat dalam pengelolaan risiko perusahaan yang terkait dengan TI. APO-12 memiliki 6 komponen proses sebagai berikut:

1) APO12.01 *Collect data* dengan *output* yang diharapkan terdapat daftar faktor risiko dan permasalahan risiko yang ada, data kejadian-kejadian risiko dan faktor-faktor yang berkontribusi terhadap kejadian risiko tersebut dan data risiko yang berkaitan dengan lingkungan operasional;
2) APO12.02 *Analyze risk* dengan *output* yang di harapkan terdapat Hasil analisa risiko, Skenario risiko TI dan ruang lingkup analisa risiko;

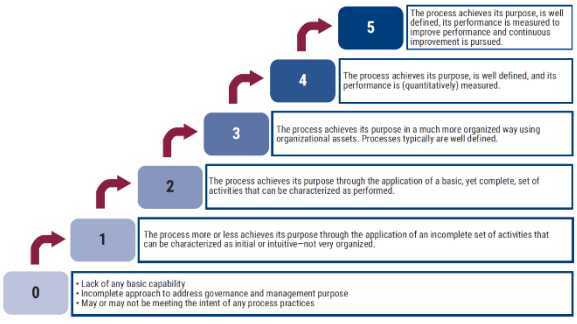
On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/58584

3) APO12.03 *Maintain a risk profile* dengan *output* yang di harapkan terdapat Profil risiko gabungan, termasuk status dari tindakan pengelolaan risiko tersebut dan dokumen skenario risiko berdasarkan bisnis dan fungsinya;
4) APO12.04 *Articulate risk* dengan *output* yang di harapkan terdapat Laporan analisa risiko dan profil risiko yang disampaikan kepada para pemangku kepentingan (*stakeholder*), Hasil *assessment* risiko dari pihak eksternal dan daftar peluang-peluang untuk meningkatkan penerimaan risiko yang lebih besar;
5) APO12.05 *Define a risk management action portofolio* dengan *output* yang di harapkan terdapat usulan-usulan proyek untuk mengurangi risiko.
6) APO12.06 *Respond to risk* dengan *output* yang di harapkan terdapat penyampaian dampak risiko, Penyebab utama dari risiko yang ada dan rencana respon terhadap kejadian insiden dari risiko yang ada.

2.5. Pengukuran Kematangan Tata Kelola TI

Secara umum tingkat efekfitas komponen IT *Governance* akan berkorelasi dengan profil kepatuhan terhadap regulasi dan juga tingkat kematangan IT *Governance*. Tingkat kematangan IT *Governance* dapat dinilai dalam dua perspektif, perspektif level proses TI dan perspektif level organisasi. Untuk penentuan tingkat kematangan per proses, dapat digunakan COBIT *Capability Maturity Model* (CMM) (ISACA, 2023b) atau COBIT *Process Assessment Model* (PAM). Sesuai dengan yang dipersyaratkan, kami akan menggunakan COBIT CMM.

Tingkat kematangan setiap proses memiliki makna tertentu berdasarkan COBIT 2019 sebagaimana ditunjukkan Gambar 2.



Gambar 2. Makna Setiap Tingkatan IT *Maturity*

COBIT *Performance Management Model*, sebagian besar selaras dengan konsep *extends* CMMI® *Development* V2.0 dimana:

1) Aktivitas proses berasosiasi dengan tingkat kapabilitas, yang terdapat pada COBIT® 2019 *Framework*: *Governance and Management Objectives guide*;
2) Tipe komponen tata kelola dan manajemen lainnya (misal struktur organisasi dan informasi), direncanakan akan mampunyai definisi tingkat kapabilitas tersendiri dalam perkembangan COBIT di masa depan;
3) *Maturity levels* berasosiasi dengan fokus area, misal kumpulan dari objektif tata kelola dan manajemen, serta komponen yang mendasarinya dan akan tercapai apabila semua tingkat kapabilitas yang diperlukan dicapai.

Perhitungan skala *rating* atribut proses, sebagai berikut:

1) *Not achieved* (N) → pencapaian 0 s.d. 15%
   Ada sedikit atau bahkan tidak terdapat *evidence* pencapaian atribut aktifitas yang terdefinisi pada proses TI yang sedang dinilai.
2) *Partially achieved* (P) → pencapaian 15% s.d. 50%
   Ada beberapa *evidence* atau bukti pelaksanaan mengenai pendekatan yang dilakukan dan beberapa pencapaian terhadap atribut terdefinisi pada proses TI yang sedang dinilai.
3) *Largely achieved* (L) → pencapaian 50% s.d. 85%
   Ada *evidence* atau bukti pelaksanaan yang menunjukkan adanya pendekatan sistematis serta adanya pencapaian signifikan terhadap atribut terdefinisi dari proses TI yang dinilai. Beberapa kelemahan terkait pencapaian atribut boleh muncul dalam proses tersebut.
4) *Fully achieved* (F) → pencapaian 85% s.d. 100%
   Ada *evidence* atau bukti pelaksanaan yang menunjukkan bahwa pendekatan yang dilakukan telah komplit dengan menggunakan pendekatan yang sistematis serta adanya pencapaian penuh terhadap atribut terdefinisi dari proses TI yang dinilai. Tidak terdapat kelemahan yang cukup signifikan terkait pencapaian atibut aktiftas dalam proses tersebut.

Contoh ilustrasi *Rating Process Capability* EDM 03 tertera pada Tabel 1.

Tabel 1. *Rating Process Capability*

Process Name	*Level 0*	*Level 1*	*Level 2*		*Level 3*		*Level 4*		*Level 5*	
EDM-03		PA 1.1	PA 2.1	PA 2.2	PA 3.1	PA 3.2	PA 4.1	PA 4.2	PA 5.1	PA 5.2
Rating by Criteria	87,50 %	87,50 %	93,75%	88,89%	90,91%	85,71%	85,71 %	41,67 %		
Capability Level Achieved	1	1	1	2	2	3	3	3		

- Jika *rating* masih N (*Not Achieved*) atau P (*Partially Achieved*) maka tidak layak mendapat nilai level penuh, misalnya pada *assessment* PA 1.1 maka dinilai masih level 0.
- Jika rating sudah L (*Large Achieved*) maka layak mendapat nilai level penuh tetapi belum layak untuk melanjutkan *assessment process attribute* level berikutnya, misalnya pada PA1.1 maka dinilai level 1.

- Jika rating sudah F (Fully Achieved) maka layak mendapat nilai level penuh dan juga layak untuk melanjutkan *assessment* ke *process attribute* berikutnya, misalnya pada PA1.1 maka dinilai level 1, dan berlanjut ke assessment PA 2.1 dan PA 2.2.

2.6. RACI Chart Tata Kelola TI

RACI *Chart* ialah definisi kewenangan yang dimiliki individu dalam suatu organisasi/perusahaan (Ariesta *et al*., 2022). Pendefinisian peran/tingkatan dalam RACI Chart terbagi menjadi 4 yaitu *Responsible* (R), *Accountable* (A), *Consulted* (C), dan *Informed* (I). Namun pada COBIT 2019 hanya pihak yang memiliki posisi *Responsible* dan *Accountable* saja yang dapat dijadikan responden penelitian.

2.7. Kerangka Penelitian

Kerangka penelitian yang dilakukan pada seperti langkah-langkah sebagai berikut ini:

1) Membuat perencanaan audit
   Dalam melakukan perencanaan audit ini, beberapa kegiatan yang dilakukan dalam mengembangkan pemahaman audit, seperti
   a. Melakukan identifikasi risiko untuk mengetahui risiko apa saja yang tinggi yang dapat dipilih untuk dijadikan ruang lingkup dalam melakukan audit yang lebih efisien;
   b. Membuat audit program untuk mengetahui tujuan dalam melakukan audit tata kelola teknologi informasi;
   c. Membuat kuisioner audit yang akan digunakan sebagai kertas kerja audit dalam melakukan wawancara, observasi dan pemeriksaan terhadap dokumen perusahaan atas pelaksanaan suatu proses kegiatan.
2) Melakukan pelaksanaan audit
   Dalam pelaksanaan audit dilakukan sesuai dengan program audit dan kuisioner yang telah buat sebelumnya. Metode pelaksanaan audit dilakukan dengan cara berikut:
   a. Wawancara kepada Manajemen *auditee* dalam pelaksanaan proses bisnis;
   b. Melakukan observasi lapangan terhadap pelaksanaan proses bisnis Perusahaan;
   c. Melakukan pengecekan terhadap dokumen perusahaan, seperti laporan hasil pelaksanaan pekerjaan, dokumen kebijakan dan prosedur, dokumen hasil operasional yang digunakan sebagai bukti pendukung bahwa pekerjaan sudah dilakukan sesuai prosedur dan peraturan yang berlaku;
   d. Melakukan perhitungan tingkat *maturity level* tata kelola manajemen risiko perusahaan.
3) Melakukan pelaporan audit
   Dalam proses pelaporan audit ini, auditor melakukan konfirmasi hasil audit dan tingkat maturity tata kelola manajemen risiko kepada Manajemen audit dan juga beberapa temuan audit yang perlu di tindaklanjuti oleh Manajemen auditee agar pengendalian dan pengelolaan risiko Perusahaan sesuai dengan tujuan Perusahaan. Dalam proses pelaporan ini akan disepakati tindaklanjut yang akan dilakukan oleh Manajemen dalam jangka pendek dan juga dalam jangka panjang.

Dari langkah-langkah audit tata kelola teknologi di atas, dibuat dalam diagram blok yang menggambarkan jadwal dalam pelaksanaan audit, sesuai Tabel 2.

Tabel 2. Jadwal pelaksanaan audit

No	*Task Name*	W1	W2	W3	W4	W5	W6
1	*Kick Off* dan Entry Meeting						
2	Perencanaan Audit						
	a. *Risk Assesment*						
	b. Pembuatan Program Audit						
3	Pelaksanaan Audit						
	a. Analisa dokumen kebijakan dan prosedur						
	b. Analisa efektifitas desain dan kontrol tata kelola manajemen risiko TI						
	c. Analisa temuan dan konfirmasi						
4	Pelaporan Audit						
	a. Melakukan konfirmasi hasil audit tingkat *maturity*						
	b. Melakukan *Exit Meeting*						
	c. Penyusunan Laporan Akhir						

3. Metode

Dalam penelitian tata kelola manajemen risiko TI ini, penulis menerapkan suatu metode kualitatif deskriptif dengan kerangka kerja COBIT 2019 dan tinjauan literatur yang mencakup penelitian sebelumnya tentang evaluasi tingkat kematangan tata kelola manajemen risiko teknologi informasi berdasarkan *framework* COBIT 2019 (ISACA, 2019a). Sumber literatur yang digunakan meliputi berbagai referensi buku, jurnal, dan situs *web* terkait. Studi literatur ini memberikan landasan teori yang relevan dengan topik penelitian.

Setelah menyelesaikan studi literatur, kami mengumpulkan data melalui dokumen perusahaan, melakukan wawancara, observasi lapangan, dan penyebaran kuesioner kepada pihak terkait sesuai dengan struktur organisasi pada divisi TI. Wawancara diterapkan agar mendapatkan pemahaman yang mendalam tentang wawasan, pandangan, persepsi, atau aspek-aspek terkait tata kelola manajemen risiko

On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/58584

teknologi informasi dalam perusahaan. Observasi juga digunakan sebagai salah satu metode pengumpulan data perusahaan, yang membantu dalam merekam aktivitas di setiap proses tata kelola dan memperoleh pemahaman tentang keadaan lapangan yang sebenarnya. Selanjutnya, kami juga melakukan pengumpulan data dari Perusahaan dan melalui penyebaran formulir kuesioner dengan beberapa pertanyaan terkait pelaksanaan aktifitas di setiap proses manajemen risiko TI.

Kuesioner ini dibuat untuk mencapai beberapa tujuan penelitian, yaitu untuk mengetahui tingkat kematangan tata kelola manajemen risiko sistem informasi dalam perusahaan. Dalam penelitian ini, kami menggunakan formulir *tools* untuk melakukan penilaian tingkat kematangan menggunakan standar COBIT 2019 dari ISACA.

Setelah memperoleh data dari wawancara, observasi, dokumen dan penyebaran kuesioner, kami melakukan pengolahan data dan evaluasi. Data yang kami peroleh kemudian diolah untuk mengevaluasi tata kelola manajemen risiko sistem informasi yang saat ini berjalan di perusahaan. Setelah mendapatkan tingkat kematangan tata kelola manajemen risiko sistem informasi yang sedang berjalan saat ini (as-is) dan tingkat maturitas manajemen risiko TI yang diharapkan (to-be), dalam hal ini penulis melakukan evaluasi kesenjangan (*gap analysis*) antara kedua tingkat kematangan tersebut. Evaluasi terhadap kesenjangan ini bertujuan untuk memudahkan tindakan perbaikan untuk meningkatkan tata kelola manajemen risiko sistem informasi yang akan diterapkan oleh manajemen perusahaan khusus nya bagian manajemen risiko teknologi informasi.

4. Hasil dan Pembahasan

4.1. Hasil assessment

Berikut ini hasil *assessment* tata kelola manajemen risiko teknologi informasi yang telah di ukur melalui metode wawancara, observasi dan pemeriksaan terhadap dokumen yang telah berjalan di Perusahaan. Proses EDM-03 *Ensured risk optimazation* berada pada *level maturity* di level 3 dan pada proses APO-12 *Managed risk* berada pada level *maturity* di level 3 sehingga tercapai dari nilai target yang telah di tetapkan Perusahaan sesuai Tabel 3.

4.2. Analisa kesenjangan (gap) pada Proses EDM-03

Berikut ini adalah gap pada aktifitas pada EDM-03 pada level 3 sampai level 4 yang belum di implementasikan secara optimal yaitu:

1. Tidak terdapat pelatihan khusus terkait manajemen risiko secara regular;
2. Tidak melakukan pemantauan dan pengukuran efektifitas penerapan kontrol tata kelola risiko dan melakukan analisis terhadap penyebab setiap penyimpangan dan melakukan tindakan perbaikan secara terus menerus.

Tabel 3. Nilai maturitas manajemen risiko TI

No.	ID	*Objectives*	Nilai *Assess*	Nilai Target	Gap
A	**EDM03**	***Ensured Risk Optimization***			
1	EDM03.01	*Evaluate risk management*	3	3	0
2	EDM03.02	*Direct risk management*	3	3	0
3	EDM03.03	*Monitor risk management*	3	3	0
B	**APO12**	***Managed Risk***			
4	APO12.01	*Collect data*	3	3	0
5	APO12.02	*Analyse risk*	3	3	0
6	APO12.03	*Maintain a risk profile*	3	3	0
7	APO12.04	*Articulate risk*	3	3	0
8	APO12.05	*Define a risk management action portfolio*	3	3	0
9	APO12.06	*Respond to risk*	3	3	0
Rata-rata Nilai Maturitas Manajemen Risiko TI			**3**	**3**	**0**

4.3. Analisa kesenjangan (gap) pada Proses APO-12

Berikut ini adalah gap pada aktifitas pada APO-12 pada level 3 sampai level 4 yang belum di implementasikan secara optimal yaitu:

1) Belum terdapat *business impact analysis* (BIA) untuk melakukan analisa risiko TI terhadap dampak bisnis;
2) Belum terdapat *cost and benefit* analisis untuk melakukan mitigasi risiko TI;
3) Belum terdapat daftar kritikalitas aset TI berdasarkan layanan TI dan infrastruktur TI;
4) Belum terdapat *Key Risk Indicator* (KRI) atau Indikator Risiko Utama (IRU);
5) Belum terdapat dokumen hasil pemeriksaan terhadap kejadian buruk dan kerugian yang telah terjadi di masa lalu atau terhadap peluang yang terlewatkan dan menganalisa penyebab utama dan membuat respon tindakan perbaikan.

4.4. Rekomendasi pada Proses EDM-03

Berikut ini adalah rekomendasi aktifitas pada EDM-03 pada level 3 sampai level 4 yang perlu di implementasikan secara optimal yaitu:

1. Pelatihan khusus terkait manajemen risiko secara regular;
2. Melakukan pemantauan dan pengukuran efektifitas penerapan kontrol tata kelola risiko dan melakukan analisis terhadap penyebab setiap

Copyright ©2024, JSINBIS, p-ISSN: 2502-2377, e-ISSN: 2088-3587
On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/58584

penyimpangan dan mekukan tindakan perbaikan secara terus menerus.

4.5. Rekomendasi pada Proses APO-12

Berikut ini adalah rekomendasi aktifitas pada APO-12 pada level 3 sampai level 4 yang perlu di implementasikan secara optimal yaitu:

1) Membuat *business impact analysis* (BIA) untuk melakukan analisa risiko TI terhadap dampak bisnis;
2) Membuat *cost* and *benefit* analisis untuk melakukan mitigasi risiko TI;
3) Membuat daftar kritikalitas aset TI berdasarkan layanan TI dan infrastruktur TI;
4) Membuat *Key Risk Indicator* (KRI) atau indikator Risiko Utama (IRU);
5) Membuat dokumen hasil pemeriksaan terhadap kejadian buruk dan kerugian yang telah terjadi di masa lalu atau terhadap peluang yang terlewatkan dan menganalisa penyebab utama dan membuat respon tindakan perbaikan.

Dalam penelitian ini terdapat beberapa rekomendasi dan risiko yang dapat terjadi dalam proses peningkatan tingkat maturitas Tata Kelola Teknologi Informasi perusahaan, oleh karena itu perlu dilakukan mitigasi dan monitoring terhadap tindaklanjut hasil *assessment* sesuai Tabel 4.

Tabel 4. Rekomendasi dan risiko hasil *assessment*

No	Rekomendasi	Risiko	Penyebab	Dampak
1	Pelatihan khusus terkait manajemen risiko secara regular	Pelatihan khusus terkait manajemen risiko tidak dilaksanakan secara regular	Kesibukan risk agent dalam mengerjakan pekerjaan operasional	Risk agent tidak mendapatkan pengembangan pengetahuan terkait manajemen risiko
2	Melakukan pemantauan dan pengukuran efektifitas penerapan kontrol tata kelola risiko dan melakukan analisis terhadap penyebab setiap penyimpangan dan mekukan tindakan perbaikan secara terus menerus.	Tidak melakukan pemantauan dan pengukuran efektifitas penerapan kontrol tata kelola risiko dan melakukan analisis terhadap penyebab setiap penyimpangan dan mekukan tindakan perbaikan secara terus menerus.	Kesibukan terhadap pencapaian operasional Perusahaan	Penerapan manajemen risiko Teknologi Informasi tidak dapat di ukur efektifitas penerapan kontrol yang berjalan.
3	Membuat business impact analysis (BIA) untuk melakukan analisa risiko TI terhadap dampak bisnis	Tidak membuat business impact analysis (BIA) untuk melakukan analisa risiko TI terhadap dampak bisnis	Kurang nya pemahaman dalam pembuatan business impact analysis (BIA)	Tidak dapat membuat perencanaan yang tepat terhadap penanganan risiko
4	Membuat cost and benefit analisis untuk melakukan mitigasi risiko TI	Tidak membuat cost and benefit analisis untuk melakukan mitigasi risiko TI	Kurang nya pemahaman dalam pembuatan cost and benefit analisis	Tidak dapat membuat perencanaan yang tepat terhadap penanganan risiko
5	Membuat daftar kritikalitas aset TI berdasarkan layanan TI dan infrastruktur TI	Tidak membuat daftar kritikalitas aset TI berdasarkan layanan TI dan infrastruktur TI	Belum memiliki daftar layanan dan infrastruktur TI	Tidak terdapat prioritas penanganan layanan dan infrastruktur TI secara maksimal
6	Membuat Key Risk Indicator (KRI) atau indikator Risiko Utama (IRU)	Tidak membuat Key Risk Indicator (KRI) atau indikator Risiko Utama (IRU)	Belum melakukan identifikasi dan manajemen risiko teknologi informasi pada seluruh aspek layanan dan infrastruktur TI	Tidak terdapat prioritas dan indikator risiko utama dalam penanganan layanan dan infrastruktur TI secara maksimal
7	Membuat dokumen hasil pemeriksaan terhadap kejadian buruk dan kerugian di masa lalu atau terhadap peluang yang terlewat dan menganalisa penyebab utama dan membuat respon tindakan perbaikan	Tidak membuat dokumen hasil pemeriksaan terhadap kejadi buruk dan kerugian di masa lalu atau terhadap peluang yang terlewat dan menganalisa penyebab utama dan membuat respon tindakan perbaikan	Belum ada kebijakan dan prosedur terkait review terhadap kejadian buruk dan kerugian yang pernah terjadi dan peluang yang terlewat.	Tidak terdapat pembelajaran terhadap kejadian buruk dan kerugian yang pernah terjadi serta peluang yang terlewat sehingga tidak dapat di analisa

On-line: http://ejournal.undip.ac.id/index.php/jsinbis/article/view/58584

No	Rekomendasi	Risiko	Penyebab	Dampak
				penyebab utama dan tindakan perbaikan yang dilakukan.

Rekomensi di atas di ukur dari perkalian tingkat probabilitas risiko dengan dampak risiko sehingga didapatkan total level risiko *inherent* sesuai Tabel 5.

Tabel 5. Rekomendasi dan tingkat risiko *inherent*

No	Rekomendasi	***Probability* Risiko**	**Dampak Risiko**	**Tingkat Risiko *Inherent***
1	Pelatihan khusus terkait manajemen risiko secara regular	3	4	12
2	Melakukan pemantauan dan pengukuran efektifitas penerapan kontrol tata kelola risiko dan melakukan analisis terhadap penyebab setiap penyimpangan dan mekukan tindakan perbaikan secara terus menerus.	3	5	15
3	Membuat *business impact analysis* (BIA) untuk melakukan analisa risiko TI terhadap dampak bisnis	4	4	16
4	Membuat *cost and benefit* analisis untuk melakukan mitigasi risiko TI	4	4	16
5	Membuat daftar kritikalitas aset TI berdasarkan layanan TI dan infrastruktur TI	3	4	12
6	Membuat *Key Risk Indicator* (KRI) atau indikator Risiko Utama (IRU)	4	4	16
7	Membuat dokumen hasil pemeriksaan terhadap kejadian buruk dan kerugian di masa lalu atau terhadap peluang yang terlewat dan menganalisa penyebab utama dan membuat respon tindakan perbaikan	4	4	16

Untuk menjalankan rekomendasi dengan baik, diperlukan langkah-langkah mitigasi risiko untuk memastikan bahwa setiap rekomendasi diimplementasikan dengan baik sesuai tujuan, sebagai berikut:

Tabel 6. Mitigasi risiko dan tingkat risiko residual

No	Mitigasi	*Probability* Risiko	Dampak Risiko	Tingkat Risiko Residual
1	1. Membuat kamus kompetensi terhadap Risk Agent perusahaan. 2. Melakukan gap analisis kompetensi setiap tahun. 3. Membuat Traning Need Analisis terhadap risk agent. 4. Memasukkan KPI personil dalam pencapaian program training terhadap risk agent.	2	3	6
2	1. Membuat Laporan Monitoring Manajemen Risiko 2. Melakukan pengukuran efektifitas penerapan kontrol yang berjalan. 3. Membuat Laporan hasil review dari stakeholder utama terhadap realisasi kemajuan perusahaan menuju target.	2	2	4
3	Memberikan pelatihan manajemen risiko dan pembuatan business impact analysis (BIA).	2	3	6
4	Memberikan pelatihan manajemen risiko dan pembuatan cost and benefit analisis (CBA).	2	3	6
5	1. Membuat daftar katalog layanan dan infrastruktur TI. 2. Melakukan business impact analysis (BIA) terhadap layanan dan infrastruktur TI.	2	2	4

No	Mitigasi	*Probability* Risiko	Dampak Risiko	Tingkat Risiko Residual
6	Membuat membuat Key Risk Indicator (KRI) atau indikator Risiko Utama (IRU) sesuai tujuan Perusahaan jangka pendek dan jangka panjang.	2	3	6
7	1. Membuat kebijakan dan prosedur terkait review terhadap kejadian buruk dan kerugian yang pernah terjadi dan peluang yang terlewat. 2. Melakukan pelaporan setiap semester kepada Manajemen.	2	3	6

Untuk menjalankan seluruh rekomendasi hasil audit dengan baik, perlu mendapatkan dukungan dan komitmen dari Manajemen agar pencapaian tingkat *maturity* risiko teknologi informasi dapat tercapai dengan baik.

5. Kesimpulan

Berdasarkan hasil *assessment* didapatkan rata-rata tingkat kematangan atau maturitas sebesar 3,00 (*Established*) untuk 2 proses COBIT 2019 yang dinilai relevan dengan Manajemen Risiko Teknologi Informasi. Dari hasil tersebut secara rerata umumnya proses-proses COBIT 2019 yang telah diterapkan di PT XYZ sudah berjalan dengan baik dengan tingkat maturitas manajemen risiko TI berada pada level 3 dan masih perlu inisiatif agar dapat mencapai tingkat kematangan 4 atau lebih baik lagi. Adapun tingkat kematangan 3 bermakna proses telah dikelola dan mencapai tujuannya dengan lebih teroganisir dengan menggunakan aset dan sumber daya organisasi. Proses telah terdefinisi dengan baik dengan adanya kebijakan dan *standard operating procedures* (SOP) untuk proses tersebut dan dijalankan sesuai manajemen risiko yang baik dan mendukung program *Good Corporate Governance* Perusahaan. Untuk mencapai tingkat kematangan yang lebih baik lagi maka setiap organisasi perlu memperhatikan komponen-komponen pembangun tata kelola TI. Terdapat 7 (tujuh) komponen-komponen penyusun Tata Kelola TI berdasarkan COBIT 2019 yaitu: Proses; Struktur organisasi; Prinsip, kebijakan, dan prosedur; Informasi; Budaya, etika, dan prilaku; SDM, kemampuan, dan kompetensinya; serta Layanan, aplikasi, dan infrastruktur.

Daftar Pustaka

Ariesta, A.D., Suprapto, Perdanakusuma, A.R., 2022. Evaluasi Tata Kelola dan Manajemen Risiko Teknologi Informasi pada PT. MyECO Teknologi Nusantara menggunakan Framework COBIT 2019 Proses EDM03 dan APO12. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 6(12), 5736-5745.

ISACA, 2019a. *COBIT 2019 Governance and Management Objectives* (*2018 ed)*. USA: ISACA.

ISACA, 2019b. COBIT 2019 *Introduction and Methodology (2019 ed)*. USA: ISACA.

ISACA, 2020. *ISACA Risk IT Framework (2020 ed)*. USA: ISACA.

ISACA, 2023a. *COBIT 2019 Framework and Methodology*. https://www.isaca.org/resources/cobit

ISACA, 2023b. *ISACA CMMI Performance Solutions*. https://cmmiinstitute.com/

ISACA, 2023c. *ISACA Risk IT Framework*. https://www.isaca.org/about-us/newsroom/press-releases/2020/isacas-risk-it-framework-offers-a-structured-methodology

ISACA, 2023d. *Maturity Model For COBIT 2019 based on CMMI*. https://www.isaca.org/resources/isaca-journal/issues/2021/volume-6/building-a-maturity-model-for-cobit-2019-based-on-cmmi

Juliandarini, Handayaningsih, S., 2013. Audit Sistem Informasi pada Digilib Universitas XYZ Menggunakan Kerangka Kerja COBIT 4.0. *Jurnal Sarjana Teknik Informatika*, 1(1), 276-286. http://dx.doi.org/10.12928/jstie.v1i1.2543

Negara, K.B.U.M., 2018. Panduan Penyusunan Pengelolaan Teknologi Informasi Badan Usaha Milik Negara. Jakarta: Kementrian Badan Usaha Milik Negara.

Umar, R., Riadi, I., Handoyo, E., 2019. Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI). *Jurnal Sistem Informasi Bisnis*, 9(1), 47-54. https://doi.org/10.21456/vol9iss1pp47-54

Windasari, I.P, Rochim, A.F., Alfiani, S.N., Kamalia, A., 2021. Audit Tata Kelola Teknologi Informasi Domain Monitor, Evaluate, and Asses dan Deliver, Service, Support Berdasarkan Framework COBIT 2019. *Jurnal Sistem Informasi Bisnis*, 11(2), 131-138. https://doi.org/10.21456/vol11iss2pp131-138

Wulandari, E., Atrinawati, L.H., Putra, M.G.L., 2022. Perancangan Tata Kelola Teknologi Informasi dengan Menggunakan Framework Cobit 2019 pada PT XYZ Balikpapan. *Journal of Computer and Information Technology*, 5(2), 127-138. http://doi.org/10.25273/doubleclick.v5i2.10067