Evaluasi Manajemen Risiko Keamanan Informasi Dengan Menggunakan COBIT 5 Subdomain EDM03 (*Ensure Risk Optimisation*) (Studi Kasus : Satuan Organisasi XYZ – Lembaga ABC)

Fransisca Tiarawati Riadi [1], Augie David Manuputty [2], Alhadi Saputra [3]
[1] *Program Studi Sistem Informasi, Universitas Kristen Satya Wacana*
Jl. Diponegoro 52-60, Salatiga
682014028@student.uksw.edu
[2] *Program Studi Sistem Informasi, Universitas Kristen Satya Wacana*
Jl. Diponegoro 52-60, Salatiga
augiemanuputty@gmail.com
[3] *Peneliti Sistem Informasi, Satuan Organisasi XYZ - Lembaga ABC*
Jakarta
alhadi.saputra@gmail.com

Abstract*— The importance of using Information Technology (IT) can't be separated from the risks that will likely occur. XYZ's organizational unit has implemented information security risk management using the ISO 31000:2009 standard to minimize those risks. Implementation of information security risk management is done so that XYZ's organizational unit can know the optimization of risk managed by the XYZ organization unit is going well and give a significant impact. So the XYZ organizational unit needs to do an evaluation to determine of capability level in ensuring the optimization of risk that has been implemented by the organization unit to IT services. The COBIT Framework 5 is used to evaluate information security risk management by performing capability level measurements that focus on the subdomain EDM03 (Ensure Risk Optimization). The results of this study on the subdomain EDM03 has a capability level at the level of 1 performed process category largely achieved with a value of 78.29%. At this level the process that the organization implements achieves its process objectives.The benefits of this research for XYZ's organizational units can help information security risk management and implementation of the ISO 31000 framework achieve optimum value in support of ICT services at the ABC Institute.
Keywords: COBIT 5,* EDM03 (*Ensure Risk Optimisation*), *Risk Management

Intisari— Pentingnya penggunaan Teknologi Informasi (TI) tidak bisa dipisahkan dari risiko-risiko yang akan mungkin terjadi. Satuan organisasi XYZ sendiri telah menerapkan manajemen risiko keamanan informasi menggunakan standar ISO 31000:2009 untuk meminimalisir risiko-risiko tersebut. Penerapan manajemen risiko keamanan informasi dilakukan agar satuan organisasi XYZ dapat mengetahui optimasi risiko yang dikelola satuan organisasi XYZ sudah berjalan dengan baik dan memberikan dampak yang signifikan. Sehingga satuan organsasi XYZ perlu melakukan evaluasi untuk mengetahui tingkat kapabilitas dalam memastikan optimasi risiko yang telah dilaksanakan satuan organisasi terhadap layanan TI. *Framework* COBIT 5 digunakan untuk melakukan evaluasi manajemen risiko keamanan informasi dengan melakukan pengukuran tingkat kapabilitas yang memfokuskan pada subdomain EDM03 (*Ensure Risk Optimisation*). Hasil penelitian ini pada subdomain EDM03 memiliki tingkat kapabilitas pada *level* 1 *performed process* kategori *largely achieved* dengan nilai 78,29%. Pada *level* ini proses yang diimplementasikan organisasi mencapai tujuan prosesnya. Manfaat penelitian ini bagi satuan organisasi XYZ dapat membantu manajemen risiko keamanan informasi dan pengimplementasi *framework* ISO 31000 mencapai nilai optimal dalam mendukung layanan TIK di Lembaga ABC.
Kata Kunci: COBIT 5, EDM03 (*Ensure Risk Optimisation*), Manajemen Risiko

I. PENDAHULUAN

Penggunaan Teknologi Informasi (TI) saat ini begitu penting bagi organisasi sebagai alat bantu untuk mendapatkan, mengolah, memproses, menyusun, menyimpan dan memanipulasi data dan informasi. Data dan informasi disusun untuk menghasilkan informasi yang berkualitas, yaitu informasi yang relevan, akurat dan tepat waktu. Pada dasarnya data dan informasi dapat digunakan untuk keperluan pribadi, bisnis, pemerintahan dan dapat juga sebagai sumber informasi yang strategis dalam pengambilan keputusan. Hal ini menjadi bukti dengan banyaknya organisasi yang terus menerapkan dan mengembangkan teknologi informasi untuk membantu meningkatkan kinerja organisasi. Penerapan Teknologi Informasi pada organisasi tidak selalu berjalan sesuai dengan yang diharapkan, sehingga menimbulkan risiko-

risiko yang dapat merugikan organisasi. Oleh karena itu untuk mengelola risiko yang dapat mengganggu jalannya proses bisnis dan menimbulkan kerugian, maka diperlukan manajemen risiko untuk meminimalisir risiko-risiko tersebut.

Satuan Organisasi XYZ pada Lembaga ABC yang mempunyai tugas melaksanakan pengelolaan infrastruktur dan tata kelola teknologi informasi, pengembangan sistem informasi, serta penyusunan standar di Lembaga ABC [1]. Salah satu sasaran strategis satuan organisasi XYZ yaitu melakukan modernisasi seluruh fasilitas dan layanan TIK Lembaga ABC [2]. Untuk mencapai sasaran strategis, maka satuan organisasi XYZ perlu adanya fasilitas yang mendukung proses bisnisnya. Modernisasi seluruh fasilitas dilakukan dengan cara meningkatkan kualitas yang disesuaikan dengan perkembangan teknologi mutakhir saat ini. Modernisasi tidak bisa dipisahkan dengan risiko-risiko yang akan mungkin terjadi, sehingga satuan organisasi XYZ menerapkan Sistem Manajemen Keamanan Informasi (SMKI) diimplementasikan pada manajemen risiko keamanan informasi untuk meminimalisir potensi risiko terkait pertukaran dokumen dan informasi pada perangkat Teknologi Informasi yang mendukung layanan TIK Lembaga ABC. Dalam meminimalisir potensi risiko terkait pertukaran dokumen dan informasi yang dapat mengganggu jalannya proses bisnis Lembaga ABC, satuan organisasi XYZ telah melakukan manajemen risiko keamanan informasi untuk membantu memastikan tercapainya tujuan penyelenggaraan layanan TI berdasarkan daftar aset yang terkait dengan layanan TI.

Tujuan utama proses manajemen risiko TI di satuan organisasi XYZ yaitu melindungi aset organisasi dan kemampuan penyelenggaraan layanan TI yang mendukung proses bisnis Lembaga ABC. Satuan Organisasi XYZ juga telah menerapkan manajemen risiko keamanan informasi menggunakan standar ISO 31000:2009 sejak tahun 2016. Namun yang menjadi pertanyaan saat ini adalah dengan adanya manajemen risiko keamanan informasi apakah optimasi risiko yang dikelola satuan organisasi XYZ sudah berjalan dengan baik dan memberikan dampak yang signifikan? Untuk menjawab pertanyaan tersebut, maka perlu dilakukan evaluasi manajemen risiko keamanan informasi guna mengetahui tingkat kapabilitas dalam memastikan optimasi risiko yang telah dilaksanakan satuan organisasi XYZ terhadap layanan TI, sehingga satuan organisasi XYZ dapat mengetahui sudah sejauh mana menerapkan manajemen risiko keamanan informasi.

Framework COBIT 5 (*Control Objectives for Information and Related Technology)* yang dapat digunakan untuk melakukan evaluasi manajemen risiko keamanan informasi dalam memastikan optimasi risiko. Salah satu pengukuran yang dilakukan dalam COBIT 5 yaitu pengukuran tingkat kapabilitas (*capability level*) yang memfokuskan pada subdomain EDM03 (*Ensure Risk Optimisation*). Hasil akhir dari penelitian ini adalah mengetahui tingkat kapabilitas kondisi saat ini dalam memastikan optimasi risiko dan dapat menjadi bahan evaluasi serta rekomendasi untuk satuan organisasi XYZ. Manfaat penelitian ini bagi satuan organisasi XYZ yaitu dapat membantu manajemen risiko keamanan informasi dan pengimplementasi *framework* ISO 31000 mencapai nilai optimal dalam mendukung fasilitas dan layanan TIK di Lembaga ABC.

II. TINJAUAN PUSTAKA

A. Penelitian Terdahulu

Penelitian yang dilakukan oleh Nurfitri dan Suprapto dengan judul Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 *IT Risk* (Studi Kasus : PT. Petrokimia Gresik) dengan permasalahan yang dihadapi yaitu padatnya proses bisnis yang berjalan di PT. Petrokimia Gresik, mengakibatkan aktivitas pengelolaan risiko menjadi kurang optimal, sehingga masih ditemukan risiko yang dapat menghambat jalannya proses bisnis perusahaan. Penelitian ini bertujuan memberikan rekomendasi berupa saran maupun usulan yang dapat digunakan oleh perusahaan untuk meminimalisir terjadinya risiko–risiko yang tidak diinginkan. COBIT 5 menyediakan dua proses yang berkaitan dengan penerapan manajemen risiko yaitu subdomain APO012 (*Manage Risk*) dan EDM03 (*Ensure Risk Optimisation*). Sehingga dari penelitian ini diketahui pengelolaan risiko yang telah dicapai PT. Petrokimia Gresik, hasil *capability level* untuk subdomain APO12 pada *Level* 3 (*Established Process)* sedangkan EDM03 pada *Level* 2 (*Managed Process)* dan target yang ingin dicapai untuk subdomain EDM03 dan APO12 adalah 1 *level* diatasnya. Dari hasil yang sudah diketahui maka diberikan rekomendasi pada proses evaluasi, langkah mitigasi dalam penerapan dan perbaikan manajemen risiko teknologi informasi [3].

Selanjutnya penelitian yang dilakukan oleh M. Habibullah dan Suprapto dengan judul Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Kerangka Kerja COBIT 5 (Studi Kasus Pada Perum Jasa Tirta I Malang) dengan permasalahan yang dihadapi yaitu meminimalisir risiko terhadap sistem telemetri yang berfungsi sebagai sistem *monitoring* penanggulangan banjir. Penelitian ini bertujuan memberikan rekomendasi dan strategi mitigasi yang dapat dipergunakan Perum Jasa Tirta I Malang dalam melakukan perbaikan penerapan manajemen risiko teknologi informasi. COBIT 5 digunakan oleh peneliti dalam melakukan evaluasi manajemen risiko TI dengan 2 subdomain yaitu subdomain EDM03 (*Ensure Risk Optimisatin*) dan APO12 (*Manage Risk*). Sehingga dari penelitian ini diketahui penerapan manajemen risiko TI yang telah dicapai Perum Jasa Tirta I Malang hasil *capability level* untuk EDM03 (*Ensure Risk Optimisatin*) dan APO12 (*Manage Risk*) pada *Level* 2 (*Managed Process)* dan target yang ingin dicapai untuk subdomain EDM03 dan APO12 adalah 1 *level* diatasnya. Dari hasil yang sudah diketahui maka diberikan rekomendasi strategi mitigasi terhadap skenario risiko untuk bahan pertimbangan rencana perbaikan manajemen risiko Teknologi Informasi (TI) di Perum Jasa Tirta I Malang [4].

Berdasarkan beberapa penelitian yang pernah dilakukan terkait Evaluasi Manajemen Risiko Teknologi Informasi menggunakan *Framework* COBIT 5. Maka berbeda dengan penelitian ini yang membahas tentang Evaluasi Manajemen

JUTEI Edisi Volume.2 No.1 April 2018
ISSN 2579-3675, e-ISSN 2579-5538
DOI 10.21460/jutei.2018.12.53

Risiko Keamanan Informasi yang hanya berfokus pada subdomain EDM03 (*Ensure Risk Optimisatin*) guna memastikan optimasi risiko pada Manajemen Risiko Keamanan Informasi yang telah dikelola satuan organisasi XYZ sudah berjalan dengan baik dan memberikan dampak yang signifikan terhadap Layanan TI Lembaga ABC.

B. Dasar Teori

- Manajemen Risiko

Manajemen risiko adalah kegiatan terkoordinasi untuk mengarahkan dan mengendalikan organisasi berkenaan dengan risiko [5]. Sehingga risiko yang ditimbulkan tidak memberikan dampak yang signifikan dan merugikan organisasi untuk itu dibutuhkan proses mengidentifikasi, mengukur risiko, serta membentuk strategi untuk mencegah terjadinya risiko. Maka kontrol dan pengukuran kinerja manajemen risiko perlu dilakukan oleh semua pihak dengan menentukan risiko mana yang harus mendapat perhatian dan pada *level* mana risiko dapat diterima oleh organisasi [6]. Untuk mengetahui efektivitas terhadap kontrol dan pengukuran kinerja manajemen risiko organisasi dalam mengelola risikonya, efektivitas tersebut dilihat dari keberhasilan organisasi dalam menjaga risiko agar tetap berada dibawah batas toleransi (*Risk Tolerance* yaitu tingkat toleransi yang dapat diterima bahwa manajemen bersedia membiarkan adanya risiko tertentu karena perusahaan mengejar tujuannya [7]) dan selera (*Risk Appetite* yaitu jumlah risiko pada tingkat yang besar, bahwa entitas bersedia untuk menerima dalam mencapai misinya [8]) yang ditetapkan.

- Keamanan Informasi

Keamanan informasi adalah memastikan bahwa di dalam organisasi, informasi dilindungi dari penyebaran kepada pengguna yang tidak berwenang (kerahasiaan), modifikasi (integritas) yang tidak benar, dan akses tidak terpakai bila diperlukan (ketersediaan) [9]. Namun dengan banyak informasi yang disimpan di sebuah organisasi maka banyak juga risiko yang akan terjadi seperti kerusakan, kehilangan informasi yang bersifat pribadi bisa tersebar ke pihak yang tidak bertanggung jawab [10]. Keamanan informasi tidak bisa hanya disandarkan pada *tools* atau teknologi keamanan informasi, melainkan perlu adanya pemahaman dari organisasi tentang apa yang harus dilindungi dan menentukan secara tepat solusi yang dapat menangani permasalahan kebutuhan keamanan informasi [11]. Untuk melakukan pengelolaan terkait permasalahan kebutuhan keamanan informasi yang akan mungkin terjadi, maka dibutuhkan manajemen risiko keamanan informasi.

Manajemen risiko keamanan informasi merupakan salah satu persyaratan yang harus dilakukan perusahaan untuk mengimplementasikan Sistem Manajemen Keamanan Informasi (SMKI) [12]. SMKI diimplementasi sebagai sebuah rencana manajemen untuk melindungi aset informasi dari seluruh gangguan keamanan dan mengimplementasikan kontrol keamanan yang telah disesuaikan dengan kebutuhan organisasi.

- COBIT 5

COBIT (*Control Objectives for Information and Related Technology)* merupakan sebuah kerangka kerja untuk tata kelola TI (*IT Governance*) yang dikembangkan oleh ISACA (*Information System and Control Association*) pada tahun 1992. COBIT dapat membantu perusahaan dalam mencapai tujuan dengan tata kelola dan manajemen TI. Saat ini ISACA mengeluarkan versi terakhir COBIT yaitu COBIT 5. COBIT 5 memberikan kerangka kerja yang mencakup 5 domain pada area *governance* yaitu memastikan bahwa kebutuhan, kondisi dan pilihan pemangku kepentingan dievaluasi untuk menentukan tujuan perusahaan yang seimbang dan disepakati yang akan dicapai, menetapkan arah melalui prioritas dan pengambilan keputusan seta memantau kinerja dan kepatuhan terhadap arah dan tujuan yang disepakati khusus untuk domain EDM (*Evaluate, Direct, and Monitor*) dan pada area *management* yaitu perencanaan, pembangunan, menjalankan dan pemantauan kegiatan yang selaras dengan arahan yang ditetapkan oleh badan tata kelola untuk mencapai tujuan perusahaan khusus domain APO (*Align, Plan, and Organize*), BAI (*Build, Acquire, and Implement*), DSS (*Deliver, Service, and Support*) dan MEA (*Monitor, Evaluate, and Assess*) [13].
COBIT 5 memberikan penilaian *capability levels* untuk setiap proses yang digolongkan menjadi 6 tingkatan, yaitu [13]:

a. *Level* 0 *Incomplete Process*, Proses tidak diimplementasikan atau gagal untuk mencapai prosesnya tujuan. Pada tingkat ini, hanya sedikit atau tidak ada bukti dari pencapaian proses yang sistematis tujuan.
b. *Level* 1 *Performed Process* (satu atribut), Proses yang diimplementasikan mencapai tujuan prosesnya.
c. *Level* 2 *Managed process* (dua atribut), Proses yang telah dijelaskan sebelumnya sekarang diimplementasikan dengan cara yang dikelola (direncanakan, dipantau dan disesuaikan) dan produk kerjanya ditetapkan dengan tepat, dikendalikan dan terawat.
d. *Level* 3 *Established Process* (dua atribut), Proses yang telah dijelaskan sebelumnya sekarang beroperasi dalam batasan yang ditetapkan untuk mencapai hasil prosesnya.
e. *Level* 4 *Predictable process* (dua atribut), Proses yang telah dijelaskan sebelumnya sekarang beroperasi dalam batasan yang ditetapkan untuk mencapai hasil prosesnya.
f. *Level* 5 *Optimized process* (dua atribut), Proses prediksi yang telah dijelaskan sebelumnya terus ditingkatkan untuk memenuhi tujuan bisnis saat ini dan yang diproyeksikan.

Figure 4—Capability Levels and Process Attributes	
Process Attribute ID	**Capability Levels and Process Attributes**
	Level 0: Incomplete process
	Level 1: Performed process
PA 1.1	Process performance
	Level 2: Managed process
PA 2.1	Performance management
PA 2.2	Work product management
	Level 3: Established process
PA 3.1	Process definition
PA 3.2	Process deployment
	Level 4: Predictable process
PA 4.1	Process measurement
PA 4.2	Process control
	Level 5: Optimizing process
PA 5.1	Process innovation
PA 5.2	Process optimization
Source: This figure is adapted from ISO/IEC 15504-2:2003 with the permission of ISO at *www.iso.org*. Copyright remains with ISO.	

Gambar 1. *Capability Levels and Process Attributes*

COBIT 5 memberikan juga *rating levels* untuk setiap *capability levels* yang digolongkan menjadi 4 skala penilaian, yaitu [13]:

a. N (tidak tercapai), ada sedikit atau tidak ada bukti pencapaian atribut yang didefinisikan dalam proses yang dinilai.
b. P (sebagian dicapai), ada beberapa bukti dari pendekatan dan beberapa pencapaian, atribut didefinisikan dalam proses dinilai. Beberapa aspek pencapaian atribut mungkin tidak dapat diprediksi.
c. L (sebagian besar tercapai), ada bukti terhadap pendekatan sistematis dan pencapaian yang signifikan dari atribut yang didefinisikan dalam proses yang dinilai. Beberapa kelemahan yang terkait dengan atribut ini mungkin ada dalam proses yang dinilai.
d. F (sepenuhnya tercapai), ada bukti terhadap pendekatan yang lengkap dan sistematis serta pencapaian penuh dari atribut yang didefinisikan dalam proses yang dinilai. Tidak ada kelemahan signifikan yang terkait dengan atribut ini yang ada dalam proses yang dinilai.

Figure 6—Rating Levels		
Abbreviation	**Description**	**% Achieved**
N	Not achieved	0 to 15% achievement
P	Partially achieved	>15% to 50% achievement
L	Largely achieved	>50% to 85% achievement
F	Fully achieved	>85% to 100% achievement
Source: This figure is reproduced from ISO/IEC 15504-2:2003, with the permission of ISO/IEC at www.iso.org. Copyright remains with ISO/IEC.		

Gambar 2. *Rating Levels*

Dalam menentukan penilaian *capability level* digunakan *base practices* untuk aktivitas yang dilakukan dan *work product* untuk *output* yang dihasilkan oleh perusahaan dari setiap proses pada domain yang terpilih. Untuk menentukan domain yang akan digunakan maka perlu dilakukan pemetaan tujuan bisnis, TI dan menyelaraskannya dengan yang ada di organisasi, pemetaan *Enterprise Goals* ke dalam *IT-Related Goals.* Kemudian bedasarkan hasil pemetaan *Enterprise Goals* ke dalam *IT-Related Goals*. Setelah itu pemetaan *IT-Related Goals* ke dalam *Processes*.

Pada domain EDM (*Evaluate, Direct and Monitor*), proses tata kelola ini menangani tujuan pengelolaan pemangku kepentingan dalam melakukan penilaian, optimasi risiko dan sumber daya, mencakup praktik dan kegiatan yang ditujukan untuk mengevaluasi pilihan strategis, memberikan arahan kepada TI dan memantau hasilnya. Maka untuk memastikan optimasi risiko digunakan subdomain EDM03 (*Ensure Risk Optimisation*). Subdomain EDM03 bertujuan memastikan bahwa *risk appetite* dan toleransi dapat dipahami, diartikulasikan dan dikomunikasi, dan risiko terhadap nilai perusahaan yang terkait dengan penggunaan Teknologi Informasi teridentifikasi dan dikelola. Didalam subdomain EDM03 terdapat 3 *base pratices* dan *work product* untuk setiap praktik yang dilakukan yaitu [13]:

a. EDM03.01 *Evaluate Risk Management*, Memeriksa dan membuat penilaian tentang pengaruh risiko terhadap penggunaan TI saat ini dan masa depan di perusahaan secara berkelanjutan. Pertimbangkan apakah *risk appetite* perusahaan sesuai dan berisiko terhadap nilai perusahaan yang terkait dengan penggunaan TI diidentifikasi dan dikelola. Berikut ini adalah aktivitas dan *work product* EDM03.01. Untuk aktivitas EDM03.01 yaitu 1. *Determine the level of IT-related risk that the enterprise is willing to take to meet its objectives (risk appetite).* 2. *Evaluate and approve proposed IT risk tolerance thresholds against the enterprise's acceptable risk and opportunity levels.* 3. *Determine the extent of alignment of the IT risk strategy to enterprise risk strategy.* 4. *Proactively evaluate IT risk factors in advance of pending strategic enterprise decisions and ensure that risk-aware enterprise decisions are made.* 5. *Determine that IT use is subject to appropriate risk assessment and evaluation, as described in relevant international and national standards.* 6. *Evaluate risk management activities to ensure alignment with the enterprise's capacity for IT-related loss and leadership's tolerance of it.* Sedangkan untuk *work product* EDM03.01 yaitu panduan *risk appetite*, tingkat toleransi risiko yang disetujui dan evaluasi kegiatan manajemen risiko.
b. EDM03.02 *Direct Risk Management*, Menetapkan arahan penerapan manajemen risiko untuk memberikan keyakinan yang wajar bahwa penerapan pengelolaan risiko TI sesuai dalam rangka untuk memastikan bahwa risiko TI yang sebenarnya tidak melebihi kemauan dewan direksi. Berikut ini adalah aktivitas dan *work product* EDM03.02. Untuk aktivitas EDM03.03 yaitu 1. *Promote an IT risk-aware culture and empower the enterprise to proactively identify IT risk, opportunity and potential business impacts.* 2. *Direct the integration of the IT risk strategy and operations with the enterprise strategic risk decisions and operations.* 3. *Direct the development of risk communication plans*

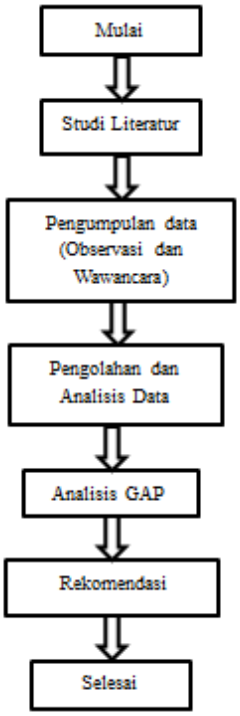
JUTEI Edisi Volume.2 No.1 April 2018
ISSN 2579-3675, e-ISSN 2579-5538
DOI 10.21460/jutei.2018.12.53

(covering all levels of the enterprise) as well as risk action plans. 4. *Direct implementation of the appropriate mechanisms to respond quickly to changing risk and report immediately to appropriate levels of management, supported by agreed-on principles of escalation (what to report, when, where and how).* 5. *Direct that risk, opportunities, issues and concerns may be identified and reported by anyone at any time. Risk should be managed in accordance with published policies and procedures and escalated to the relevant decision makers.* 6. *Identify key goals and metrics of risk governance and management processes to be monitored, and approve the approaches, methods, techniques and processes for capturing and reporting the measurement information.* Sedangkan untuk *work product* EDM03.02 yaitu kebijakan manajemen risiko, tujuan utama untuk dipantau untuk manajemen risiko dan proses yang disetujui untuk mengukur manajemen risiko.

c. EDM03.03 *Monitor Risk Management*, Memantau tujuan utama dan metrik dari proses manajemen risiko dan menetapkan berapa penyimpangan atau masalah akan diidentifikasi, dilacak dan dilaporkan untuk diperbaiki. Berikut ini adalah aktivitas dan *work product* EDM03.03. Untuk aktivitas EDM03.03 yaitu 1. *Monitor the extent to which the risk profile is managed within the risk appetite thresholds.* 2. *Monitor key goals and metrics of risk governance and management processes against targets, analyse the cause of any deviations, and initiate remedial actions to address the underlying causes.* 3. *Enable key stakeholders' review of the enterprise's progress towards identified goals*. 4. *Report any risk management issues to the board or executive committee.* Untuk *work product* EDM03.03 yaitu tindakan perbaikan untuk mengatasi penyimpangan manajemen risiko dan masalah manajemen risiko untuk dewan direksi.

III. METODOLOGI PENELITIAN

Penelitian ini menggunakan metode deskritif kualitatif. Deskritif kualitatif merupakan metode yang dilakukan dengan mengumpulkan data terlebih dahulu kemudian diklarifikasi, dianalisis kemudian diinterprestasikan untuk mendapatkan gambaran yang jelas mengenai objek penelitian [14]. Penelitian ini dilakukan dalam sebuah organisasi yang tidak ingin disebutkan nama lembaganya. Akan tetapi bersedia untuk dilakukan penelitian dan bersedia untuk menggunakan data-data yang ada dalam organisasi tersebut. Proses penelitian ini berdasarkan studi kasus terhadap satuan organisasi XYZ dengan melakukan observasi untuk mengetahui informasi terkait manajemen risiko keamanan informasi. Data dalam penelitian ini merupakan data primer diperoleh dari data yang dikumpulkan yaitu berdasarkan observasi, wawancara dan bukti dokumen. Kemudian data sekunder diperoleh dari sumber lain yaitu studi pustaka dan analisis penelitian terdahulu dengan mengumpulkan data secara lengkap berdasarkan tahapan penelitian yang telah disusun secara sistematis. Setelah itu nantinya hasil dari tahapan-tahapan ini akan menghasilkan tingkat kapabilitas EDM03 (*Ensure Risk Optimisation*).



Gambar 3. Tahapan Penelitian

a. Tahap awal dalam penelitian ini yaitu studi literatur didapatkan melalui buku, jurnal, artikel internet yang terkait atau pun buku elektronik yang berhubungan dengan evaluasi manajemen risiko dengan menggunakan subdomain EDM03 (*Ensure Risk Optimisation*) dan COBIT 5 agar peneliti dapat memahami studi kasus yang akan diteliti.
b. Tahap kedua dalam penelitian ini yaitu melakukan pengumpulan data melalui wawancara dan pengumpulan dokumen dengan narasumber yang dianggap dapat memberikan penjelasan dari studi kasus yang diteliti terkait evaluasi manajemen risiko keamanan informasi dengan berdasarkan *framework* tata kelola TI yang ada di COBIT 5 menggunakan *base practices* dan *work product* dari subdomain yang dipakai (EDM03 *Ensure Risk Optimisation*)**.** Untuk mendukung penerapan *base practices* digunakan aktivitas-aktivitas yang ada dalam COBIT 5 sebagai acuan pertanyaan pada tingkat kapabilitas.
c. Tahap ketiga dalam penelitian ini yaitu pengelolaan data dan analisa dari hasil observasi dan wawancara serta bukti dokumen yang ada berdasarkan *base practices* dan *work product* yang didapat, kemudian dilakukan pemetaan tujuan bisnis, TI dan proses serta menyelaraskannya dengan yang ada di organisasi.

Selanjutnya dilakukan perhitungan untuk mengetahui nilai suatu tingkat kapabilitas EDM03 (*Ensure Risk Optimisation*) dari temuan-temuan yang didapat.

d. Tahap keempat dalam peneilitian ini yaitu analisis *GAP* untuk memberikan skala perbandingan dari hasil tingkat kapabilitas saat ini dan target tingkat kapabilitas yang diharapkan oleh organisasi berdasarkan temuan-temuan dari hasil penelitian.

e. Tahap kelima dalam peneilitian ini yaitu memberikan rekomendasi sesuai dengan kebutuhan yang perlu dilakukan perbaikan dari hasil pengolahan dan analisis data.

IV. PEMBAHASAN DAN HASIL

Pengukuran tingkat kapabilitas pada Satuan Organisasi XYZ berdasarkan analisis terhadap hasil wawancara, observasi serta bukti dokumen yang didapatkan kemudian disesuaikan dengan *framework* COBIT 5. Ada beberapa proses yang dilakukan untuk mengukur tingkat kapabilitas pada Satuan Organisasi XYZ yaitu memetakan tujuan bisnis, TI dan menyelaraskannya dengan yang ada di organisasi. Berikut beberapa tahapan tersbut:

Pemetaan ini dilakukan dengan menentukan P (*Primary Key*) tujuan bisnis organisasi ke dalam COBIT 5 pada *Enterprise Goals* yang sesuai dengan kondisi yang ada di organisasi. Dalam pemetaan ini dilakukan secara langsung berdasarkan visi misi yang ada pada satuan organisasi XYZ. Akan tetapi satuan organisasi XYZ tidak bersedia visi misi yang ada dalam organisasi dicantumkan, maka visi misi tersebut tidak dicantumkan dalam penelitian ini.

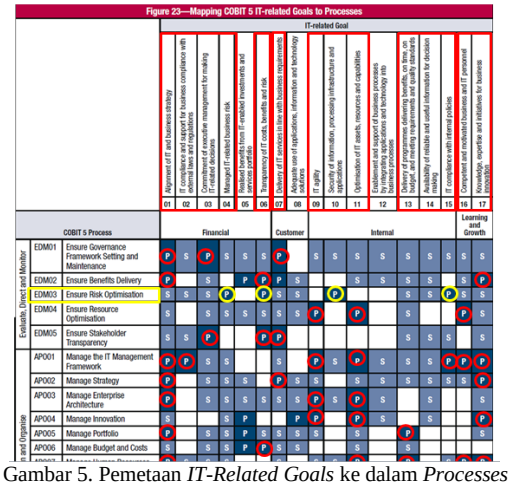
Figure 4—COBIT 5 Enterprise Goals

BSC Dimension	Enterprise Goal	Relation to Governance Objectives		
		Benefits Realisation	Risk Optimisation	Resource Optimisation
Financial	1. Stakeholder value of business investments	P		S
	2. Portfolio of competitive products and services	P	P	S
	3. Managed business risk (safeguarding of assets)		P	S
	4. Compliance with external laws and regulations		P	
	5. Financial transparency	P	S	S
Customer	6. Customer-oriented service culture	P		S
	7. Business service continuity and availability		P	
	8. Agile responses to a changing business environment	P		S
	9. Information-based strategic decision making	P	P	P
	10. Optimisation of service delivery costs	P		P
Internal	11. Optimisation of business process functionality	P		P
	12. Optimisation of business process costs	P		P
	13. Managed business change programmes	P	P	S
	14. Operational and staff productivity	P		P
	15. Compliance with internal policies		P	
Learning and Growth	16. Skilled and motivated people	S	P	P
	17. Product and business innovation culture	P		

Gambar 4. Pemetaan tujuan bisnis ke dalam *Enterprise Goals*

Kemudian dilanjutkan dengan pemetaan *Enterprise Goals* ke dalam *IT-Related Goals*. Ada 4 perspektif yang dipetakan pada *Enterprise Goals* ke dalam *IT-Related Goals* yaitu perspektif *financial*, perspektif *customer*, perspektif *internal* dan perspektif *learning and growth*. Berikut hasil pemetaan *Enterprise Goals* ke dalam *IT-Related Goals* pada setiap perspektif. Dalam perspektif *financial* terdapat 6 proses dan ada 5 proses yang terpilih untuk pemetaan dari *Enterprise Goals* ke dalam *IT-Related Goals* diantaranya *alignment of IT and business* strategy, *IT compliance and support for business copliance with external laws and regulations, Commitment of executive management for making IT-related decisions, Managed IT-related business risk* dan *Transparency of IT costs, benefits and risk.* Perspektif *customer* terdapat 2 proses dan hanya ada 1 proses yang terpilih untuk pemetaan dari *Enterprise Goals* ke dalam *IT-Related Goals* yaitu *Delivery of IT services in line with business requirments*. Perspektif *internal* terdapat 7 proses dan ada 6 proses yang terpilih untuk pemetaan dari *Enterprise Goals* ke dalam *IT-Related Goals* diantaranya *IT agility, Security of information, processing infrastructure and applications, Optimisatuon of IT assets, resources and capabilities, Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standarts, Availability of reliable and useful information for decision making* dan *IT compliance with internal policies*. Perspektif *learning and growth* terdapat 2 proses dan 2 proses tersebut terpilih untuk pemetaan dari *Enterprise Goals* ke dalam *IT-Related Goals* diantaranya *Competent and motivated business and IT personnel* dan *Knowledge, expertise and initiatives for business innovation.*

Bedasarkan hasil pemetaan *Enterprise Goals* ke dalam *IT-Related Goals*. Selanjutnya yaitu membuat pemetaan *IT-Related Goals* ke dalam *Processes*. Setelah dilakukan pemetaan *IT-Related Goals* ke dalam *Processes* ternyata ditemukan jumlah proses yang terpilih yaitu 36 proses dari 37 proses yang ada dalam COBIT 5. Namun penelitian ini hanya memfokuskan pada subdomain EDM03 (*Ensure Risk Optimisation*) dikarenakan satuan organisasi XYZ ingin meningkatkan kualitas seluruh fasilitas dan layanan TIK dengan meminimmalisir risiko-risiko yang akan mungkin terjadi. Sehingga peneliti melakukan evaluasi terhadap manajemen risiko keamanan informasi dalam optimasi risiko yang telah dikelola satuan organisasi XYZ.



Gambar 5. Pemetaan *IT-Related Goals* ke dalam *Processes*

A. Kondisi Saat Ini

Berdasarkan hasil wawancara dengan Kepala Sub Bidang Satuan Organisasi XYZ yaitu Bpk. F.A dalam melakukan wawancara peneliti menggunakan *base practices*. Untuk menerapkan *base practices* digunakan aktivitas-aktivitas dalam COBIT 5 sebagai acuan pertanyaan dan *work product* dari subdomain EDM03 (*Ensure Risk Optimisation*). Berikut setiap rincian *base pratice* terkait

JUTEI Edisi Volume.2 No.1 April 2018
ISSN 2579-3675, e-ISSN 2579-5538
DOI 10.21460/jutei.2018.12.53

aktivitas-aktivitas yang dilakukan dan *work product* EDM03 (*Ensure Risk Optimisation*):

1) EDM03.01 *Evaluate Risk Management*

Pada proses ini satuan organisasi XYZ sudah memeriksa dan membuat penilaian tentang pengaruh risiko terhadap penggunaan TI saat ini dan masa depan di Lembaga ABC secara berkelanjutan. Saat ini satuan organisasi XYZ sudah mengimplementasikan manajemen risiko keamanan informasi menggunakan framework ISO 31000. Proses untuk melakukan evaluasi manajemen risiko ada dalam dokumen tersebut terkait evaluasi risiko-risiko yang sudah diidentifikasi sebelumnya dan untuk melakukan identifikasi risiko TI yang ada pada Lembaga ABC dilakukan berdasarkan aset *register*. Berdasarkan hasil wawancara dari Bpk. F.A yang mengatakan bahwa:

> "... kami sudah memeriksa dan membuat penilaian pengaruh risiko terhadap penggunaan TI. Dalam melakukan *assessment* kami menggunakan dokumen Pedoman Umum Manajemen Risiko untuk proses identifikasi risiko, analisis dan evaluasi risiko, pengendalian risiko, pembuatan RTP (*Risk Treatment Plan*) dan pemantauan risiko. Proses identifikasi risiko yang kami lakukan berdasarkan aset *register*..."[1]

Adapun aktivitas-aktivitas yang dilakukan satuan organisasi XYZ untuk mencapai proses tersebut yaitu satuan organisasi XYZ sudah menentukan level risiko terkait TI yang berelasi dengan risiko Lembaga ABC berdasarkan kerugian dari 2 aspek yaitu kerahasiaan dan integritas pada suatu data dan informasi yang dikelola satuan organisasi XYZ dan ketersediaan informasi dalam menunjang operasional layanan satuan organisasi XYZ, satuan organisasi XYZ sudah mengevaluasi dan menyetujui batas toleransi risiko TI yang dapat diterima Lembaga ABC berdasarkan hasil dari perhitungan tingkat nilai risiko yang didapat dari nilai kecenderungan dikalikan nilai dampak dan toleransi risiko TI dapat diterima apabila Nilai Risiko Akhir (NRA) adalah rendah, penerimaan risiko juga dapat dilakukan apabila NRA dari suatu risiko bernilai sedang atau tinggi dan sudah tidak dapat dikontrol lagi, satuan organisasi XYZ sudah proaktif dalam mengevaluasi faktor risiko TI pada saat keputusan stategis Lembaga ABC tertunda dan satuan organisasi XYZ sadar akan keputusan yang diambil apabila terjadi perubahan terkait organisasi, teknologi, objektif dan proses bisnis, ancaman yang teridentifikasi, efektivitas dari kontrol yang telah diimplementasikan, kejadian eksternal, seperti perubahan dari lingkungan hukum dan peraturan, perubahan obligasi kontraktual, dan perubahan dari lingkungan sosial. Satuan organisasi XYZ juga sudah melakukan penilaian dan evaluasi risiko sesuai dengan standar internasional menggunakan *framework* ISO 31000 dan melakukan evaluasi kegiatan manajemen risiko terkait risiko-risiko yang belum bisa diterima pada tahun sebelumnya.

Dalam melakukan aktivitas-aktivitas tersebut satuan organisasi XYZ sudah mendokumentasinya dengan membuat dokumen Pedoman Umum Manajemen Risiko untuk keamanan informasi menggunakan *framework* ISO 31000 sebagai petunjuk mengenai pengembangan manajemen risiko di satuan organisasi XYZ, satuan organisasi XYZ sudah menyetujui *level* toleransi risiko TI dalam dokumen Pedoman Umum Manajemen Risiko untuk keamanan informasi menggunakan *framework* ISO 31000, toleransi risiko yang dapat diterima apabila risiko bernilai rendah, risiko diterima juga apabila suatu risiko bernilai sedang atau tinggi dan sudah tidak dapat dikontrol lagi, satuan organisasi XYZ juga sudah melakukan evaluasi kegiatan manajemen risiko ada dalam dokumen RTM (Rapat Tinjauan Manajemen) membahas terkait risiko-risiko yang sebelumnya belum bisa diterima. Namun saat ini masih ada kekurangan terhadap aktivitas yang belum dilakukan satuan organisasi XYZ yaitu belum ada keselarasan strategi risiko TI satuan organisasi XYZ sebagai bagian dari badan Lembaga ABC dengan stategi risiko Lembaga ABC itu sendiri.

2) EDM03.02 *Direct Risk Management*

Pada proses ini satuan organisasi XYZ sudah menetapkan arahan penerapan manajemen risiko untuk menjamin bahwa penerapan manajemen risiko keamanan informasi sesuai dalam rangka memastikan bahwa risiko TI yang sebenarnya tidak melebihi kemauan dewan direksi. Saat ini satuan organisasi XYZ menetapkan arahan penerapan manajemen risiko dalam dokumen Kebijakan Manajemen Risiko SMKI (Sistem manajemen keamanan informasi) bahwa proses identifikasi risiko mengikuti ketentuan mengenai penerapan manajemen risiko di lingkungan kerja satuan organisasi XYZ. Penerapan manajemen risiko di lingkungan kerja satuan organisasi XYZ sendiri menggunakan dokumen Pedoman Umum Manajemen Risiko untuk keamanan informasi menggunakan *framework* ISO 31000. Proses untuk arahan penerapan manajemen risiko ada dalam Pedoman Umum Manajemen Risiko untuk keamanan informasi menggunakan *framework* ISO 31000 terkait yang memberitahukan adanya risiko, pelaporan, *monitoring* dan rekomendasi serta fasilitasi dan *monitoring*. Berdasarkan hasil wawancara dari Bpk. F.A yang mengatakan bahwa:

> "... kami sudah menetapkan arahan penerapan manajemen risiko ada dalam dokumen Kebijakan Manajemen Risiko SMKI (Sistem manajemen keamanan informasi) dan untuk penerapan manajemen risiko kami menggunakan dokumen Pedoman Umum Manajemen Risiko untuk keamanan informasi menggunakan ISO 31000..."[2]

Adapun aktivitas-aktivitas yang dilakukan satuan organisasi XYZ untuk mencapai proses tersebut yaitu satuan organisasi XYZ sudah mempromosikan, memberdayakan dan mengarahkan budaya sadar risiko TI dalam mengidentifikasi risiko TI pada dokumen Kebijakan Manajemen Risiko SMKI (Sistem manajemen keamanan informasi) terkait peluang dan potensi dampak bisnis yang

[1] Wawancara 6 Oktober 2017

[2] Wawancara 9 Oktober 2017

dilaporkan oleh setiap orang yang berhubungan dengan satuan organisasi XYZ dalam sosialisasi *security awareness*, satuan organisasi XYZ juga sudah menetapkan arahan pengembangan rencana komunikasi risiko dalam dokumen Kebijakan Manajemen Risiko SMKI (Sistem manajemen keamanan informasi) terkait apa yang harus dilakukan penanggung jawab, *risk coordinator*, *risk officer* dan pegawai atau staff satuan organisasi XYZ dalam menemukan dan meminimalisir risiko yang ada, satuan organisasi XYZ sudah mengidentifikasi tujuan dan metrik utama manajemen risiko dalam dokumen *Risk Profile* untuk mengendalikan risiko berdasarkan proses menentukan aset kritikal, mendeskripsikan risiko, menilai risiko, mengontrol risiko dan melaksanakan tindakan dalam rangka mengurangi tingkat risiko hingga pada tingkatan yang yang dapat diterima.

Dalam melakukan aktivitas-aktivitas tersebut satuan organisasi XYZ sudah membuat dokumentasinya pada dokumen Kebijakan Manajemen Risiko SMKI (Sistem manajemen keamanan informasi), sudah ada dokumen proses penilaian risiko yang dibuat satuan organisasi XYZ dokumen *Risk Profile* yaitu dokumen terkait penjelasan terhadap identifikasi risiko-risiko dan evaluasi hasil penilaian risiko penyelenggaraan layanan teknologi informasi oleh satuan organisasi XYZ-Lembaga ABC. Namun saat ini masih ada kekurangan terhadap aktivitas yang belum dilakukan satuan organisasi XYZ yaitu belum adanya tujuan dan metrik utama proses tata kelola risiko yang diidentifikasi dan belum ada dokumentasi mekanisme dalam merespon secara cepat terkait perubahan risiko dan pelaporannya serta belum adanya arahan keputusan terkait risiko antara satuan organisasi XYZ sebagai bagian dari badan Lembaga ABC dengan Lembaga ABC itu sendiri.

3) EDM03.03 *Monitor Risk Management*

Pada proses ini satuan organisasi XYZ sudah memantau tujuan utama dan metrik dari proses manajemen risiko dan menetapkan berapa penyimpangan atau masalah akan diidentifikasi, dilacak dan dilaporkan untuk perbaikan. Saat ini satuan organisasi XYZ memantau tujuan utama dan metrik dari proses manajemen risiko di dokumen Pedoman Umum Manajemen Risiko yaitu mengendalikan risiko berdasarkan proses menentukan aset kritikal, mendeskripsikan risiko, menilai risiko, mengontrol risiko dan melaksanakan tindakan dalam rangka mengurangi tingkat risiko hingga pada tingkatan yang yang dapat diterima. Proses untuk melakukan *monitoring* ada dalam dokumen Pedoman Umum Manajemen Risiko untuk keamanan informasi menggunakan *framework* ISO 31000 yaitu bentuk *monitoring* terhadap pelaksanaan pengendalian risiko yang dilaksanakan berdasarkan *progress* status yang dilakukan dalam melaksanakan kontrol yang telah ditetapkan. Berdasarkan hasil wawancara dari Bpk. F.A yang mengatakan bahwa:

> "... kami sudah memantau tujuan utama dan metrik dari proses manajemen risiko, tujuan utama dan metrik dari proses manajemen risiko ada dalam dokumen Pedoman Umum Manajemen Risiko. Kemudian hasil *assessment* dari identifikasi risiko dan hasil evaluasi penilaian risiko terhadap penyelanggaraan layanan teknologi risiko yaitu dokumen *Risk Profile* dalam dokumen *Risk Profile* ada bagian terkait RTP (*Risk Treatment Plan*) untuk risiko-risiko yang belum bisa diterima. RTP (*Risk Treatment Plan*) tersebut akan kami *monitoring*, *monitoring* RTP (*Risk Treatment Plan*) dilakukan untuk mengetahui apakah setelah dibuatkan kontrol, risiko yang ada sebelumnya bernilai tinggi sudah turun nilai risikonya..."[3]

Adapun aktivitas-aktivitas yang dilakukan satuan organisasi XYZ untuk mencapai proses tersebut yaitu saat ini satuan organisasi XYZ sudah melakukan pemantauan dan perbaikan *profil* risiko yang dikelola dalam batas *risk appetite* pada ada RTP (*Risk Treatment Plan*) berdasarkan hasil *assessment* risiko yang sebelumnya belum bisa diterima dan dibuatkan RTP (*Risk Treatment Plan*: Menentukan langkah yang perlu diambil untuk meminimalkan kemungkinan maupun dampak terjadinya risiko) untuk tahun depan, kemudian dilakukan *assessment* kembali untuk mengetahui apakah tahun ini risiko yang sebelumnya sudah ada penurunan nilai risikonya atau belum, satuan organisasi XYZ juga melibatkan Kepala Satuan Organisasi XYZ dalam meninjau ulang sasaran yang sudah tercapai dan melaporkan masalah manajemen risiko kepada Kepala Satuan Organisasi XYZ terkait risiko-risiko yang sebelumnya belum bisa diterima pada dokumen RTM (Rapat Tinjauan Manajemen).

Dalam melakukan aktivitas-aktivitas tersebut satuan organisasi XYZ sudah mendokumentasinya dengan membuat dokumen *Risk Profile* yang didalamnya ada RTP (*Risk Treatment Plan*) tindakan perbaikan terkait risiko yang pada tahun sebelumnya belum bisa diterima dan untuk dokumentasi dalam melaporkan masalah-masalah manajemen risiko kepada Kepala Satuan Organisasi XYZ ada dalam dokumen RTM (Rapat Tinjauan Manajemen), masalah yang dilaporkan kepada Kepala Satuan Organisasi XYZ yaitu risiko-risiko yang belum bisa diterima pada tahun 2016 yang berjumlah 16 dan dibuatkan RTP untuk diterapkan pada tahun 2017. Kemudian dilakukan evaluasi lagi untuk mengetahui jumlah risiko sesudah diterapkannya RTP maka hasil dari RTP yang sudah diterapkan diketahui risiko sisa yang belum bisa diterima Lembaga ABC berjumlah 6. Namun saat ini masih ada kekurangan terhadap aktivitas yang belum dilakukan satuan organisasi XYZ yaitu belum melakukan pemantauan terkait tujuan dan metrik utama proses tata kelola risiko.

Berdasarkan setiap rincian *base pratice* terkait aktivitas-aktivitas yang dilakukan dan *work product* yang didapatkan. Untuk mengetahui hasil tingkat kapabilitas dalam memastikan optimasi risiko pada manajemen risiko keamanan informasi didapat dari perhitungan berdasarkan wawancara menggunakan *base practices* yang dimana untuk penerapan *base practices* digunakan aktivitas-aktivitas sebagai acuan pertanyaan dan *work product* dari subdomain EDM03 (*Ensure Risk Optimisation*). Dalam mememnuhi setiap *level* pada COBIT 5 *Base Practices* (BP) dan *Work Product* (WP) harus bernilai 100% (*Fully*

[3] Wawancara 9 Oktober 2017

JUTEI Edisi Volume.2 No.1 April 2018
ISSN 2579-3675, e-ISSN 2579-5538
DOI 10.21460/jutei.2018.12.53

Achieved). Ada 3 BP dan WP pada EDM03 (*Ensure Risk Optimisation*), untuk itu nilai pada masing-masing BP dan WP yaitu 33,3%. Perhitungan didapat dari jumlah pertanyaan yang terpenuhi dibagi jumlah seluruh pertanyaan ditambahkan jumlah *Work Product* (WP) yang ada dibagi jumlah seluruh *Work Product* (WP) dikalikan 33,3%.

Tabel I. Perhitungan *Capability Level*

Proses dalam domain	Jumlah Pertanyaan	Pertanyaan yang terpenuhi	Jumlah WP	WP yang ada	Nilai untuk setiap BP dan WP EDM03	Nilai yang dicapai dalam BP dan WP
EDM03-BP1 : Evaluate risk management.	10	8	3	3	33,33%	29,88%
EDM03-BP2 : Direct risk management	6	3	3	2	33,33%	19,36%
EDM03-BP3 : Monitor risk management	4	3	2	2	33,33%	29,05%
					Total	78,29%

Maka hasil analisis perhitungan yang didapat untuk tingkat kapabilitas dalam memastikan optimasi risiko pada manajemen risiko keamanan informasi telah mencapai *level* 1 *performed process* kategori *largerly achieved* dengan nilai 78,29% yang berarti proses yang diimplementasikan satuan organisasi XYZ mencapai tujuan prosesnya. Namun masih ada beberapa aktivitas yang belum dilakukan satuan organisasi XYZ dan belum didokumentasikan yaitu keselarasan strategi risiko TI satuan organisasi XYZ sebagai bagian dari badan Lembaga ABC dengan stategi risiko Lembaga ABC itu sendiri, tujuan dan metrik utama proses tata kelola risiko yang diidentifikasi dan dokumentasi mekanisme dalam merespon secara cepat terkait perubahan risiko dan pelaporannya serta arahan keputusan terkait risiko antara satuan organisasi XYZ sebagai bagian dari badan Lembaga ABC dengan Lembaga ABC itu sendiri serta pemantauan terkait tujuan dan metrik utama proses tata kelola risiko.

B. Analisis GAP

Berdasarkan perhitungan *capability level* saat ini untuk Manajemen Risiko Keamanan Informasi pada subdomain EDM03 (*Ensure Risk Optimisation*) di satuan organisasi XYZ yaitu berada pada *level* 1 *performed process* kategori *largely achieved* dengan nilai 78,29%. *Level* target yang ingin dicapai oleh satuan organisasi XYZ yaitu berada pada *level* 2 *Managed process*. Sehingga untuk memenuhi *level* 2 *Managed process*, satuan organisasi XYZ harus mencapai kategori *Fully achieved* dengan nilai 100% pada *level* 1 dan *GAP* yang dimiliki satuan organisasi XYZ yaitu sebesar 21,71%.

Tabel II. Hasil Analsis *GAP*

Subdomain	Hasil pengukuran *capability level*	*Rating by criteria*	*GAP*
EDM03 (*Ensure Risk Optimisation*)	78,29%	L	21,71%

C. Rekomendasi

Berdasarkan hasil evaluasi manajemen risiko keamanan informasi satuan organisasi XYZ dengan menggunakan *capability level* disusunlah beberapa rekomendasi yang dapat digunakan untuk membantu manajemen risiko keamanan informasi dan pengimplementasi *framework* ISO 31000 mencapai nilai optimal dalam mendukung layanan TIK di Lembaga ABC. Berikut ini adalah hasil rekomendasi yang telah dibuat berdasarkan subdomain EDM03 (*Ensure Risk Optimisation*). Maka hasil rekomendasi yang diberikan kepada satuan organisasi XYZ untuk memenuhi aktivitas-aktivitas dan *work product* yang belum terpenuhi yaitu:

1. Lembaga ABC perlu membuat kebijakan manajemen risiko agar satuan organisasi XYZ sebagai bagian dari badan Lembaga ABC bisa menyelaraskan strategi risiko TI dengan stategi risiko Lembaga ABC itu sendiri.
2. Satuan Organisasi XYZ perlu membuat Kebijakan Tata Kelola Risiko.
3. Satuan Organisasi XYZ perlu adanya dokumentasi tertulis yaitu SOP Penanganan Risiko dalam merespon secara cepat terkait perubahan risiko dan pelaporannya.
4. Lembaga ABC perlu menetapkan arahan keputusan integrasi strategi dan pelaksanaan risiko yang ada di satuan organisasi XYZ.
5. Satuan Organisasi XYZ harus membuat tujuan dan metrik utama proses tata kelola risiko dan melakukan *monitoring* terkait tujuan dan metrik utama tersebut.

V. KESIMPULAN

Evaluasi manajemen risiko keamanan informasi pada satuan organisasi XYZ dengan menggunakan COBIT 5 subdomain EDM03 (*Ensure Risk Optimisation*) memiliki tingkat kapabilitas pada *level* 1 *performed process* kategori *largely achieved* dengan nilai 78,29%. Pada *level* ini proses yang diimplementasikan organisasi mencapai tujuan prosesnya. Dokumentasi pada manajemen risiko keamanan informasi dari setiap *base pratices* dan *work product* sudah cukup baik. Meskipun dalam teknis pelaksanaannya masih ada *base pratices* dan *work product* yang belum sepenuhnya dilakukan dan belum memberikan dampak yang begitu signifikan. Sehingga hasil dari penelitian ini dapat membantu satuan organisasi XYZ untuk meningkatkan optimasi risiko dan mendokumentasikan setiap proses serta pengimplementasi *framework* ISO 31000 dapat dioptimalkan dengan baik dalam mendukung fasilitas dan layanan TIK di Lembaga ABC.

DAFTAR PUSTAKA

[1] Lembaga ABC, 2015. PERKA No 8 2015 tentang Organisasi dan Tata Kerja Lembaga ABC. Jakarta.

[2] Rencana Strategis Satuan Organisasi XYZ, 2016-2020. Jakarta.

[3] N.Z. Firdaus dan S., "Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 *IT Risk* (Studi Kasus : PT. Petrokimia Gresik)," J-ptiik, vol.2, no.1, pp.91-100, 2018. S

[4] M.H. Arief dan S., "Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Kerangka Kerja COBIT 5 (Studi Kasus Pada Perum Jasa Tirta I Malang),"J-ptiik, vol.2, no.1, pp.101-110,2018.

[5] ISACA. "*Glossary* ISACA" Internet: https://www.isaca.org/Pages/Glossary.aspx?tid=1794&char=R, [18 Oktober 2017].

[6] D.N. Setyaningrum, S. dan A.Kusyanti "Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan *Framework* COBIT 5 (Studi Kasus : PT. Kimia Farma (Persero) Tbk – Plant Watudakon)," J-ptiik, vol.2, no.1, pp.143-152, 2018.

[7] ISACA. "*Glossary* ISACA" Internet: https://www.isaca.org/Pages/Glossary.aspx?tid=1798&char=R, [25 Oktober 2017].

[8] ISACA. "*Glossary* ISACA" Internet: https://www.isaca.org/Pages/Glossary.aspx?tid=1787&char=R, [25 Oktober 2017].

[9] ISACA. "*Glossary* ISACA" Internet: https://www.isaca.org/Pages/Glossary.aspx?tid=1486&char=I, [18 Oktober 2017].

[10] E.L. Putra, B.C. Hidayanto dan H.M. Astuti, "Evaluasi Keamanan Informasi Pada Divisi *Network of Broadband* PT. Telekomunikasi Indonesia Tbk. Dengan Menggunakan Indeks Keamanan Informasi (KAMI)," Jurnal Teknik Pomits, vol.3, no.2, 2014.

[11] B.Supradono, "Manajemen Risiko Keamanan Informasi Dengan Menggunakan Metode *Octave* (*Operationally Critical Threat, Asset and Vulnerability Evaluation*)," Media Elektrika, vol.2, no1, pp.4-8, 2009.

[12] H.Syahrial, "*Prototype Information Security Risk Assessment Tool* Berbasis *Lotus Notes* Dalam Rangka Penerapan Sistem Manajemen Keamanan Informasi ISO 27001," dalam Seminar Nasional Teknologi Informasi dan Komunikasi Terapan, Semarang, 2014.

[13] ISACA, COBIT® 5 *Process Assessment Model*, Rolling Meadows: ISACA, 2012.

[14] W. D. Sari, F. S. Papilaya dan A.D. Manuputty, "Evaluasi Pengendalian Aplikasi pada Sistem Informasi Keuangan dan Akuntansi Satya Wacana (SIKASA),"Jsii, vol.2, no.1, 2017.

JUTEI Edisi Volume.2 No.1 April 2018
ISSN 2579-3675, e-ISSN 2579-5538
DOI 10.21460/jutei.2018.12.53