

## ENSURE RISK OPTIMISATION IMPLEMENTASI TEKNOLOGI INFORMASI MENGUNAKAN KERANGKA KERJA COBIT 5

**Sarmini**

Jurusan Sistem Informasi, Program Studi Sistem Informasi  
STMIK AmikomPurwokerto  
Email: sarmini@amikompurwokerto.ac.id

**Satria Pandu Adipurwoko**

Jurusan Sistem Informasi, Program Studi Sistem Informasi  
STMIK AmikomPurwokerto  
Email: satriapandu20@gmail.com

### ABSTRAK

Belum adanya panduan dan referensi utama yang harus dipergunakan sebagai standar penentuan strategi dalam menangani berbagai risiko yang dihadapi dan belum adanya pemantauan implementasi manajemen risiko untuk memastikan tata cara pengelolaan risiko dijalankan sungguh-sungguh menunjukkan STMIK Amikom Purwokerto belum secara serius memperhatikan masalah dan risiko-risiko yang mungkin terjadi terkait implementasi TI yang dapat merugikan organisasi. Oleh karena itu, untuk mengatasi dan mengelola risiko yang dapat mengganggu jalannya proses bisnis dan menimbulkan kerugian, maka diperlukan manajemen risiko untuk meminimalisir risiko-risiko yang mungkin terjadi. Salah satu kerangka kerja yang dapat digunakan untuk mengevaluasi manajemen risiko TI adalah COBIT 5 khususnya pada domain EDM03 (*Ensure Risk Optimisation*) dan proses APO12 (*Manage Risk*) yang membahas secara terperinci mengenai manajemen risiko TI. Tujuan penelitian yang dilakukan adalah mengukur tingkat kapabilitas subdomain proses EDM03 (*Ensure Risk Optimisation*) untuk mengetahui dan memastikan sejauh mana proses optimasi risiko implementasi TI pada STMIK Amikom Purwokerto. Hasil pengukuran tingkat kapabilitas proses domain EDM03 *Ensure Risk Optimisation* berada pada di *level 0 (Incomplete Process)*, hal ini menunjukkan bahwa proses EDM03 tidak diimplementasikan atau gagal mencapai tujuannya. Pada tingkatan ini, hanya ada sedikit bukti atau bahkan tidak ada bukti adanya pencapaian sistematis dari tujuan proses tersebut.

**Kata kunci:** risiko; manajemen risiko; EDM03; COBIT 5.

### ABSTRACT

*The absence of the main guidelines and references that must be used as a standard for determining strategies in dealing with various risks faced and the absence of monitoring the implementation of risk management to ensure that risk management procedures are implemented really shows that STMIK Amikom Purwokerto has not seriously considered the problems and risks may occur related to IT implementation that can harm the organization. Therefore, to overcome and manage risks that can disrupt business processes and cause losses, risk management is needed to minimize the risks that may occur. One framework that can be used to evaluate IT risk management is COBIT 5 especially in the EDM03 (Ensure Risk Optimization) and APO12 (Manage Risk) domains that discuss in detail about IT risk management. The purpose of the research is to measure the level of EDM03 process subdomain capability (Ensure Risk Optimization) to determine and ascertain the extent of the risk optimization process of IT implementation at STMIK Amikom Purwokerto. The measurement results of the EDM03 Ensure Risk Optimization domain process capability level are at level 0 (Incomplete Process), this indicates that the EDM03 process is not implemented or fails to achieve its objectives. At this level, there is little evidence or even evidence of systematic achievement of the purpose of the process.*

**Keywords:** risk; risk management; EDM03, COBIT 5.

## 1. PENDAHULUAN

Implementasi Teknologi Informasi (TI) dianggap menjadi hal yang penting bagi organisasi/perusahaan untuk meningkatkan efektifitas dan efisiensi kinerja organisasi/perusahaan. Penerapan TI merupakan salah satu cara yang efektif untuk mengimplementasikan dan mengeksekusi strategi-strategi dalam perusahaan [1]. Akan tetapi implementasi TI pada organisasi/perusahaan tidak selalu berjalan sesuai dengan yang diharapkan. Sebagaimana mata uang yang memiliki dua sisi,

implementasi TI di satu pihak memberikan manfaat serta keuntungan yang luar biasa bagi organisasi/perusahaan namun di pihak lain implementasi TI juga menimbulkan risiko-risiko yang dapat merugikan organisasi/perusahaan. Maka dari itu, implementasi TI harus diiringi dengan pengelolaan yang tepat dan relevan sehingga dapat meminimalisasi risiko-risiko yang mungkin timbul di dalam proses bisnis [2]. Risiko adalah segala hal yang mungkin berdampak pada kemampuan organisasi dalam mencapai tujuan-tujuannya [3].

Risiko implementasi TI dalam organisasi harus dikelola dengan baik agar implementasi TI dapat memberikan dampak yang baik bagi organisasi dan risiko dari penggunaan TI dapat diminimalisasi [4]. TI harus terbebas dari risiko-risiko yang menghambat pencapaian objektifitas perusahaan [5]. Untuk mengantisipasi atau mengurangi kemungkinan terjadinya risiko tersebut maka diperlukan analisis manajemen risiko TI [6]. Penilaian penerapan manajemen risiko TI dibutuhkan agar perusahaan mampu mencapai sasaran dan tujuan yang telah ditetapkan [7]. Pelaksanaan manajemen resiko TI harus dinilai untuk mengetahui tingkat kapabilitas proses optimasi risiko yang telah dilaksanakan [8]. Optimasi risiko bertujuan agar risiko mampu dikelola dengan baik untuk memastikan agar perusahaan memiliki *risk appetite* dan toleransinya dimengerti serta secara terus menerus mengidentifikasi, menilai dan mengurangi risiko yang berhubungan dengan TI [9].

Belum adanya panduan dan referensi utama yang harus dipergunakan sebagai standar penentuan strategi dalam menangani berbagai risiko yang dihadapi dan belum adanya pemantauan implementasi manajemen risiko untuk memastikan tata cara pengelolaan risiko dijalankan sungguh-sungguh menunjukkan STMIK Amikom Purwokerto belum secara serius memperhatikan masalah dan risiko-risiko yang mungkin terjadi terkait implementasi TI yang dapat merugikan organisasi. Oleh karena itu, untuk mengatasi dan mengelola risiko yang dapat mengganggu jalannya proses bisnis dan menimbulkan kerugian, maka diperlukan manajemen risiko untuk meminimalisir risiko-risiko yang mungkin terjadi.

Salah satu kerangka kerja yang dapat digunakan untuk mengevaluasi manajemen risiko TI adalah COBIT 5 khususnya pada domain EDM03 (*Ensure Risk Optimisation*) dan proses APO12 (*Manage Risk*) yang membahas secara terperinci mengenai manajemen risiko TI [10]. Kerangka kerja COBIT 5 *for Risk* memberikan panduan komprehensif tentang tata kelola risiko dan manajemen atas organisasi TI dan menyediakan skumpulan proses TI yang merepresentasikan aktivitas yang dapat dikendalikan berfokus pada domain *Evaluate, Direct, Monitor* (EDM) yang mana terdapat proses dalam memastikan tata kelola organisasi, penyampaian nilai/manfaat dari investasi TI, optimalisasi risiko dan transparansi *stakeholder* [11]. 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 [12].

Pengukuran optimasi risiko penggunaan TI di STMIK Amikom Purwokerto bertujuan untuk memastikan risiko organisasi yang berkaitan dengan implementasi TI tidak melampaui toleransi risiko, dampak dari risiko penggunaan TI dapat diidentifikasi dan potensi kegagalan dapat diminimalisasi. Pengukuran optimasi risiko dilakukan dengan menilai tingkat kapabilitas pada proses EDM03 (*Ensure Risk Optimisation*) pada organisasi saat ini dan mendapatkan adanya analisis kesenjangan. Hasil pengukuran tingkat kapabilitas untuk merumuskan langkah-langkah perbaikan yang dapat dilakukan untuk meningkatkan optimasi risiko implementasi TI di STMIK Amikom Purwokerto sehingga dapat meminimalisir adanya risiko-risiko TI yang mungkin terjadi di masa yang akan datang dan tentunya implementasi TI dapat mendukung pencapaian tujuan organisasi.

## 2. METODOLOGI PENELITIAN

Langkah-langkah yang dilakukan dalam penelitian untuk mengetahui tingkat kapabilitas domain proses EDM03 – *Ensure Risk Optimisation* di STMIK Amikom Purwokerto berdasarkan panduan COBIT 5 adalah sebagai berikut:

### 2.1 Metode Pengumpulan Data

Pengumpulan data penelitian, data-data yang terkait dengan penelitian dikumpulkan, dengan analisis tingkat kapabilitas yang bersifat kuantitatif yang akan diperoleh dari proses *assesment* secara langsung ke pihak yang terkait menggunakan *checklist* yang diadopsi dari *assesment tool template* COBIT 5 dari ISACA.

- a. Wawancara, proses ini dilakukan untuk mengumpulkan informasi dan data. Hasilnya akan digunakan sebagai data pendukung dari hasil pengukuran tingkat kapabilitas proses.
- b. Kuesioner dalam penelitian ini dirancang untuk mengetahui *capability level* pengelolaan operasional TI yang telah berjalan di STMIK AMIKOM Purwokerto. Kuesioner diberikan kepada responden merupakan pernyataan tertulis, pernyataan yang dibuat mengacu pada kerangka kerja COBIT 5 subdomain proses EDM03.

- c. Dokumentasi digunakan untuk mendapatkan gambaran dari sudut pandang subjek melalui suatu media tertulis dan dokumen lainnya yang ditulis atau dibuat langsung oleh subjek yang bersangkutan.

## 2.2 Metode Analisis Data

Proses ini dilakukan setelah pengolahan data, analisa data yang dilakukan terdiri dari analisa tingkat kapabilitas yang ada saat ini, tingkat kapabilitas yang diharapkan dan analisis kesenjangan serta penyusunan rekomendasi.

- a. Analisa tingkat kapabilitas saat ini berdasarkan pada data hasil wawancara dan survelience pengisian checklist kuesioner terhadap pengelola dan pengguna TI di STMIK Amikom Purwokerto.
- b. Analisa kesenjangan atas tingkat kapabilitas saat ini dengan tingkat kapabilitas yang diharapkan. Dengan demikian bisa diketahui seberapa jauh jangkauan yang harus dicapai sampai tujuan organisasi tercapai.
- c. Rekomendasi, setelah dilakukan perhitungan tingkat kapabilitas dan analisis kesenjangan, maka langkah berikutnya adalah membuat rekomendasi untuk tata kelola TI yang lebih efektif dan dapat mencapai level yang diharapkan berdasarkan hasil analisis yang telah dilakukan pada domain proses EDM03 yaitu Ensure Risk Optimisation.

## 3. HASIL DAN PEMBAHASAN

### 3.1 Perhitungan Capability Level Saat Ini (As Is) Domain Proses EDM03 Ensure Risk Optimisation.

Proses *Ensure Risk Optimisation* berfokus pada pengelolaan risiko dan toleransi risiko yang berhubungan dengan nilai TI perusahaan. Memastikan bahwa risiko TI perusahaan tidak melebihi kemampuan dan toleransi perusahaan dalam menerima risiko, serta mengidentifikasi dan mengelola dampak dari risiko TI terhadap nilai-nilai pada perusahaan, dan mengurangi terjadinya kegagalan.

Ringkasan mengenai hasil pencapaian *level* beserta rincian secara spesifik mengenai penilaian proses ini adalah sebagai berikut:

**Tabel 1. Ensure risk optimisation – EDM03**

<i>Tujuan</i>										
<b>Proses</b>	<b>Level 0</b>	<b>Level 1</b>	<b>Level 2</b>	<b>Level 3</b>		<b>Level 4</b>		<b>Level 5</b>		
<i>Manage operations</i>		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
<b>Rating berdasarkan presentase</b>	100%	38,9%								
<b>Rating berdasarkan warna</b>										

Rincian penilaian *proses Ensure Risk Optimisation* pada *level 1* dijelaskan melalui tabel 2 berikut ini.

**Tabel 2. Ensure risk optimisation EDM03 Level 1  
EDM03 Ensure Risk Optimisation**

<b>Governance Practice</b>	<b>Outputs</b>	<b>Exist</b>	<b>Score</b>
EDM03.01 <i>Evaluate risk management</i>	<i>Risk appetite guidance</i>	—	
	<i>Approved risk tolerance levels</i>	√	33,33%
	<i>Evaluation of risk management activities</i>	—	
EDM03.02 <i>Direct risk management</i>	<i>Risk management policies</i>	—	
	<i>Key objectives to be monitored for risk management</i>	—	33,33%
	<i>Approved process for measuring risk management</i>	√	
EDM03.03 <i>Monitor risk management</i>	<i>Remedial actions to address risk management deviations</i>	—	50%
	<i>Risk management issues for the board</i>	√	
<i>Average Score</i>			38,89%

a. *Evaluate risk management*

Proses “*Evaluate risk management*” pada STMIK Amikom Purwokerto dinyatakan tidak lulus dengan skor 33,33%, karena:

- 1) *Risk appetite guidance*  
STMIK Amikom Purwokerto belum memiliki *risk appetite guidance*.
- 2) *Approved risk tolerance level* dibuat berdasarkan perhitungan dan analisa dampak yang dilakukan oleh penanggung jawab Departemen dimana terdiri dari *unlikely, rare, possible, likely, almost certain*. Kemudian setelah itu akan ditentukan ekspektasi risiko yang terdiri dari *low, medium, high*.
- 3) *Evaluation of risk management activities*  
Tidak ada evaluasi dari kegiatan-kegiatan manajemen risiko yang dilakukan oleh STMIK AMIKOM Purwokerto.

b. *Direct risk management*

Proses “*Direct risk management*” pada STMIK Amikom Purwokerto dinyatakan tidak lulus dengan skor 33,33%, karena:

- 1) *Risk management policies* belum dibuat oleh STMIK Amikom Purwokerto, semua hal terkait dengan risiko belum memiliki SOP maupun kebijakan secara tertulis.
- 2) Tidak ada analisis dan perhitungan yang dilakukan oleh penanggung jawab Departemen TI terhadap *key objectives* yang akan dimonitor oleh *risk management*.
- 3) Walaupun STMIK Amikom Purwokerto belum memiliki *risk management policies* secara tertulis namun melalui rapat yang dilakukan secara berkala menentukan proses yang disetujui untuk mengukur *risk management*.

c. *Monitor risk management*

Proses “*Monitor risk management*” pada STMIK Amikom Purwokerto dinyatakan tidak lulus dengan skor 50%, karena:

- 1) *Remedial actions to address risk management deviations* tidak dilakukan karena *risk* masih kurang mendapatkan perhatian di STMIK Amikom Purwokerto.
- 2) Ada laporan *risk management issues for the board* walaupun laporan belum dibuat secara tertulis masih sebatas laporan yang disampaikan dalam rapat dengan *stakeholder* karena *risk* masih kurang mendapatkan perhatian.

Dari hasil penilaian *capability level*, proses *Ensure Risk Optimisation* berada di *level 0*, karena proses ini hanya memperoleh status *partially achieved* di *level 1* yaitu 38,89% sehingga tidak dapat lulus *level 1*.

### 3.2 *Capability Level yang diharapkan dan Analisis Kesenjangan*

Analisis kesenjangan dilakukan untuk mengetahui seberapa besar kesenjangan yang ada antara target *capability level* saat ini dengan kondisi yang diharapkan yaitu *Established Process (level 3)*. Berdasarkan hasil penilaian *capability level* pada proses *EDM03 Ensure Risk Optimisation* yang telah

dilakukan maka dapat disimpulkan bahwa *capability level* proses EDM03 *Ensure Risk Optimisation* pada STMIK AMIKOM Purwokerto saat ini berada pada di *level 0 (Incomplete Process)* dan memiliki *gap* sebesar 2 untuk mencapai *level 3 (Established Process)* yang menjadi target *capability level* yang diharapkan. Hal ini menunjukkan bahwa proses EDM03 *Ensure Risk Optimisation* pada STMIK Amikom Purwokerto Proses tidak lengkap; Proses tidak diimplementasikan atau gagal mencapai tujuannya. Pada tingkatan ini, hanya ada sedikit bukti atau bahkan tidak ada bukti adanya pencapaian sistematis dari tujuan proses tersebut.

### 3.3 Rekomendasi

Dalam prakteknya, COBIT tidak mengidentifikasi prioritas-prioritas proses yang harus dilakukan. Prioritas didasarkan pada kebutuhan organisasi/institusi. Untuk mencapai target *capability level* organisasi/institusi, maka perlu untuk melengkapi proses EDM03 dengan *output-output* yang harus ada untuk mencapai *level 1*, yaitu:

- a. Proses EDM03.01- disarankan pada organisasi/institusi untuk segera membuat *Risk Appetite Guidance*.
- b. Pada poin EDM03.02 – *Direct Risk Management* disarankan untuk segera dibuatkan kebijakan untuk manajemen risiko dan menentukan/menganalisa *key objective* yang akan dimonitor oleh *risk management*.
- c. Pada poin EDM03.03 – Monitor Risk Management disarankan agar segera dibuatkan tindakan remedial jika terjadi deviasi oleh risk management.

## 4. KESIMPULAN

Berdasarkan hasil perhitungan rata-rata tingkat kapabilitas yang dilakukan pada proses domain EDM03 *Ensure Risk Optimisation*, diperoleh hasil tingkat kapabilitas saat ini proses *Ensure Risk Optimisation* di STMIK Amikom Purwokerto berada pada di *level 0 (Incomplete Process)* dan memiliki *gap* sebesar 3 untuk mencapai *level 3 (Established Process)* yang menjadi target *capability level* yang diharapkan. Hal ini menunjukkan bahwa proses EDM03 *Ensure Risk Optimisation* tidak diimplementasikan atau gagal mencapai tujuannya. Pada tingkatan ini, hanya ada sedikit bukti atau bahkan tidak ada bukti adanya pencapaian sistematis dari tujuan proses tersebut.

Untuk dapat memastikan proses optimalisasi risiko implementasi TI di STMIK Amikom Purwokerto maka perlu untuk dibuat panduan mengenai batas toleransi risiko secara umum di organisasi/institusi dan dilakukan evaluasi dari kegiatan-kegiatan *risk management* secara berkala sehingga dapat menghasilkan kebijakan terkait manajemen risiko serta langkah-langkah penanggulangan apabila terjadi penyimpangan dalam manajemen risiko.

## DAFTAR PUSTAKA

- [1] H. Jogiyanto, *Sistem Teknologi Informasi*. Andi Yoyakarta, 2005.
- [2] F. T. Riadi, A. D. Manuputty, and A. Saputra, "Evaluasi Manajemen Risiko Keamanan Informasi Dengan Menggunakan COBIT 5 Subdomain EDM03 ( Ensure Risk Optimisation ) ( Studi Kasus : Satuan Organisasi XYZ – Lembaga ABC )," vol. 2, no. 1, pp. 1–10, 2018.
- [3] IT Governance Institute, "IT Governance Institute," in *COBIT 4.1 Rolling Meadows*, 2007.
- [4] R. E. Putri, "Model Penilaian Kapabilitas Proses Optimasi Risiko TI Berdasarkan COBIT 5," *Semin. Nas. Inform.*, pp. 252–258, 2015.
- [5] N. M. Rahmania, Suprpto, and A. R. Perdanakusuma, "Penilaian Kapabilitas Manajemen Risiko Teknologi Informasi Menggunakan Kerangka Cobit 5 ( Studi Kasus : Daerah Operasional ( DAOP ) XX )," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 12, pp. 6828–6836, 2018.
- [6] G. M. Husein and R. V. Imbar, "Analisis Manajemen Risiko Teknologi Informasi Penerapan Pada Document Management System di PT . Jabar Telematika ( JATEL )," *J. Tek. Inform. dan Sist. Inf.*, vol. 1, no. 2, pp. 75–87, 2015.
- [7] Y. I. Putri, Suprpto, and A. D. Herlambang, "Penilaian Kapabilitas Penerapan Manajemen Risiko Teknologi Informasi Menggunakan Kerangka Kerja COBIT 5 ( Studi pada PDAM Kota Malang Jawa Timur )," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 11, pp. 4855–4862, 2018.
- [8] N. D. Setyaningrum, Suprpto, and A. Kusyanti, "Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan Framework COBIT 5 ( Studi Kasus : PT . Kimia Farma ( Persero ) Tbk – Plant Watudakon )," *J. Pengemb. Teknol. Inf. dan Ilmu Komput.*, vol. 2, no. 1, pp. 143–152, 2018.
- [9] ISACA, *Process Assessment Model (PAM): Using COBIT 5*. USA : Rolling Meadows, 2013.
- [10] N. Z. Firdaus and Suprpto, "Evaluasi Manajemen Risiko Teknologi Informasi Menggunakan COBIT 5 IT Risk ( Studi Kasus : PT . Petrokimia Gresik )," *J. Pengemb. Teknol. Inf. dan Ilmu*

- Komput.*, vol. 2, no. 1, pp. 91–100, 2018.
- [11] R. Puspita, Murahartawaty, and E. K. Umar, “Perancangan Manajemen Risiko Teknologi Informasi Pada Core Processes EDM03 Dan Key Supporting Processes EDM01 , EDM02 , dan EDM05 Menggunakan Framework COBIT 5 (Studi Kasus : Dinas Komunikasi dan Informatika Pemerintah Kota Bandung),” in *e-Proceeding of Engineering*, 2016, vol. 3, no. 2, pp. 3255–3262.
- [12] M. D. Rahmatya, A. Hadiana, and I. Maliki, “Pengukuran Manajemen Risiko TI di PT. X Menggunakan COBIT 5,” 2011.