

# Evaluasi Penerapan *Information Technology Risk Governance* Berdasarkan COSO ERM pada PT. Agro

Matias Andika Yuwono\*<sup>1</sup>, Lena Ellitan<sup>2</sup>

<sup>12</sup>Fakultas Bisnis, Universitas Katolik Widya Mandala

<sup>12</sup>Kota Surabaya, Indonesia

Email: [1andika.yuwono@gmail.com](mailto:1andika.yuwono@gmail.com), [2lena@ukwms.ac.id](mailto:2lena@ukwms.ac.id)

## Abstract

*In this digital era, where every organisation heavily relies on information technology (IT) for its daily operations, ensuring good IT risk management through Information Technology Risk Governance (ITRG) becomes crucial. The risks emerging from this dependency are diverse and complex, ranging from cybersecurity threats to IT system failures to data breaches, all of which can potentially cause significant financial loss and reputation damage. Effective implementation of ITRG not only protects the company from these risks but also enhances the quality of information produced for decision-making. With these various issues, PT. Agro also aims to enhance the company's value in terms of data security, effective data processing, and producing relevant reports for the company's leaders. PT. Agro conducts an ITRG evaluation in the information technology (IT) division using a triangulation approach involving interviews with IT managers, which financial managers and internal audit managers then confirm. This step aims to ensure effective ITRG implementation in the IT division. The ITRG assessment of the IT division is based on the governance and culture component of COSO ERM, which includes five main principles: risk supervision, operational structure, desired culture, commitment to core values, and attracting, developing, and retaining competent individuals. The research results indicate that the IT division of PT. Agro has effectively implemented these five principles, thus PT. Agro has successfully applied ITRG, hoping to provide effective data information services to relevant stakeholders.*

**Keywords:** Information Technology Risk Governance, ERM, COSO ERM, ITRG

## Abstraksi

*Di era digital ini, di mana setiap organisasi sangat bergantung pada teknologi informasi (TI) untuk operasi sehariannya, memastikan pengelolaan risiko TI yang baik melalui Information Technology Risk Governance (ITRG) menjadi sangat krusial. Risiko yang muncul dari ketergantungan ini sangat beragam dan kompleks, mulai dari ancaman keamanan siber, kegagalan sistem TI, hingga pelanggaran data, yang semuanya berpotensi menyebabkan kerugian finansial besar dan kerusakan reputasi. Penerapan ITRG yang efektif tidak hanya melindungi perusahaan dari risiko tersebut tetapi juga meningkatkan kualitas informasi yang dihasilkan untuk pengambilan keputusan. Dengan berbagai macam permasalahan tersebut, PT. Agro juga ingin meningkatkan nilai perusahaan terhadap pengamanan data, pengolahan data secara efektif, hingga menghasilkan laporan yang relevan bagi pemimpin perusahaan. PT. Agro melakukan evaluasi ITRG di divisi information technology (IT) dilakukan dengan pendekatan triangulasi, melibatkan wawancara dengan manajer IT, yang kemudian dikonfirmasi oleh manajer keuangan dan manajer audit internal. Langkah ini bertujuan untuk memastikan*

*penerapan ITRG yang efektif di divisi IT. Penilaian ITRG divisi IT berdasarkan komponen governance and culture dari COSO ERM, yang mencakup lima prinsip utama, termasuk pengawasan risiko, struktur operasional, budaya yang diinginkan, komitmen terhadap nilai inti, serta menarik, mengembangkan, dan mempertahankan individu yang kompeten. Dari hasil penelitian yang dilakukan memberikan hasil bahwa divisi IT PT. Agro telah menerapkan kelima prinsip ini dengan baik, dengan demikian PT. Agro telah berhasil menerapkan ITRG secara efektif sehingga diharapkan PT. Agro dapat memberikan pelayanan data informasi yang efektif kepada stakeholder yang berkepentingan.*

**Kata Kunci:** Information Technology Risk Governance, ERM, COSO ERM, ITRG

## 1. PENDAHULUAN

Penerapan *Information Technology Risk Governance* (ITRG) menjadi semakin penting di era digital saat ini, di mana organisasi bergantung secara luas pada teknologi informasi (TI) untuk operasi sehari-hari. Ketergantungan ini membawa risiko yang beragam dan kompleks, termasuk ancaman keamanan siber, kegagalan sistem TI, dan pelanggaran data, yang semuanya dapat menyebabkan kerugian finansial yang signifikan dan kerusakan reputasi. Selain itu, regulasi yang berkembang terkait privasi data dan keamanan siber mendorong organisasi untuk mengimplementasikan strategi manajemen risiko TI yang komprehensif. Kegagalan dalam mengelola risiko TI ini tidak hanya dapat menimbulkan konsekuensi hukum, tetapi juga mengganggu kelancaran operasi bisnis [1]. Oleh karena itu, penerapan ITRG. menjadi krusial sebagai upaya untuk mengidentifikasi, mengelola, dan memitigasi risiko TI secara efektif, memastikan kepatuhan terhadap standar dan regulasi, serta mempertahankan integritas dan keandalan sistem dan data organisasi.

Perusahaan yang melakukan penerapan ITRG secara efektif dapat meningkatkan kualitas informasi yang dihasilkan bagi kepentingan perusahaan. Namun hingga saat ini masih cukup banyak perusahaan yang belum melakukan penerapan ITRG secara efektif, sehingga dapat merugikan bagi perusahaan tersebut sendiri seperti data tidak memiliki kualitas yang baik, sehingga informasi untuk pengambilan keputusan tidak dapat diandalkan [2]. Apabila ITRG pada sebuah perusahaan diterapkan dengan baik, maka analisis data dapat dilakukan dengan lebih mudah untuk pengambilan keputusan strategis. Penerapan ITRG yang baik juga dilakukan pada sektor Badan Usaha Milik Negara (BUMN) dan swasta, karena salah satu manfaat penerapan ITRG adalah untuk perlindungan data masyarakat. Oleh karena itu dengan penerapan ITRG membutuhkan kerja sama seluruh bagian dan membutuhkan dukungan dari manajemen puncak untuk dapat menerapkan ITRG secara efektif dan efisien pada perusahaan [3]. Dengan demikian dapat disimpulkan bahwa penerapan ITRG memberikan banyak manfaat bagi perusahaan baik dalam pengolahan data secara efektif untuk pengambilan keputusan, dan juga penerapan perlindungan data yang baik untuk meningkatkan kepercayaan *stakeholder*.

Dalam konteks bisnis yang dinamis dan teknologi yang terus berkembang, penting bagi perusahaan untuk membentuk kerangka tata kelola perusahaan yang kuat.

*Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM)* sebagai kerangka kerja manajemen risiko, menjadi sangat relevan karena memberikan pendekatan holistik dalam mengidentifikasi, menilai, mengelola, dan memantau risiko secara menyeluruh dalam organisasi. Hal tersebut juga dijelaskan oleh Zain (2022)[4] yang menekankan pentingnya pendekatan ini dalam menghadapi risiko yang terus berkembang. COSO ERM memungkinkan perusahaan untuk memahami dan mengelola risiko secara komprehensif, bukan hanya dari sudut pandang individu atau departemen, namun dari keseluruhan organisasi. Seperti yang diuraikan oleh Karanja (2017) [5], pendekatan ini memungkinkan pembuatan keputusan yang lebih tepat dan berdasar informasi yang lengkap.

Penerapan COSO ERM tidak hanya mengurangi potensi kerugian tetapi juga berpotensi meningkatkan keuntungan. Organisasi dengan manajemen risiko yang baik sering kali mendapatkan kepercayaan lebih tinggi dari *stakeholder*, termasuk investor, pelanggan, dan karyawan. Seperti ditunjukkan oleh Nurlaela dan Suhendi (2021) [6], kepatuhan terhadap regulasi di berbagai industri sering kali membutuhkan manajemen risiko yang efisien, dan penerapan COSO ERM memfasilitasi pemenuhan persyaratan tersebut. Dengan memahami risiko dan interaksinya, perusahaan dapat mengalokasikan sumber daya lebih efisien, mengoptimalkan operasi, dan mencapai tujuan strategis dengan lebih efektif [7]. Pendekatan ini membuka jalan untuk operasional yang lebih aman dan strategi bisnis yang lebih kuat dalam lingkungan yang cepat berubah dan penuh dengan tantangan teknologi.

Pentingnya akan penerapan ITRG ini juga dipahami oleh PT. Agro. Sebagai perusahaan yang sedang berkembang yang bergerak dalam bidang perdagangan dan distribusi, PT. Agro menyadari pentingnya kecepatan pengolahan data hingga penggunaan informasi untuk pengambilan keputusan bagi manajemen. PT. Agro memiliki divisi *information technology (IT)* untuk mengelola segala data perusahaan, dan untuk memastikan divisi IT telah menerapkan ITRG yang efektif, maka akan dilakukan evaluasi penerapan ITRG pada divisi IT berdasarkan COSO ERM. Penelitian yang dilakukan adalah studi kualitatif yang mengambil PT. Agro sebagai studi kasus. Fokus utama penelitian ini adalah pada divisi IT di PT. Agro, terutama terkait dengan penerapan Tata Kelola Risiko TI (ITRG) dalam perusahaan. Data dikumpulkan dari kegiatan operasional sehari-hari perusahaan, memberikan wawasan tentang bagaimana ITRG diintegrasikan dengan budaya dan nilai inti PT. Agro. Dalam proses penelitian ini, konfirmasi dan wawancara akan dilakukan dengan beberapa kunci personil di perusahaan. Ini termasuk manajer IT, yang memiliki peran sentral dalam penerapan ITRG, serta manajer audit internal dan manajer keuangan. Mereka merupakan pengguna utama fasilitas dan program yang disediakan oleh divisi IT. Dengan berbicara kepada para manajer ini, penelitian bertujuan untuk memahami bagaimana penerapan ITRG memengaruhi operasional dan pengambilan keputusan dalam berbagai divisi di PT. Agro.

*Information Technology Risk Governance (ITRG)* adalah proses yang mencakup kebijakan dan metode manajemen untuk memastikan penggunaan teknologi informasi

yang efisien dan efektif dalam sebuah organisasi. Proses ini meliputi tahapan perencanaan, implementasi, serta *monitoring* dan evaluasi. Tujuan utamanya adalah untuk memastikan bahwa pemanfaatan sumber daya teknologi informasi (TI) mendukung tercapainya tujuan organisasi [8]. ITRG mengintegrasikan elemen-elemen seperti kepemimpinan, struktur organisasi, dan proses yang memastikan bahwa ada kesesuaian antara strategi dan tujuan perusahaan dengan penggunaan teknologi informasi.

Lebih lanjut, ITRG juga sangat terkait dengan keputusan yang diambil oleh manajemen senior organisasi [9]. Berdasarkan berbagai sumber, tata kelola teknologi informasi dapat dipahami sebagai kumpulan aktivitas yang dilakukan oleh manajemen senior dan eksekutif dalam sebuah organisasi. Aktivitas ini bertujuan untuk mengatur teknologi informasi yang dimiliki agar dapat mendukung kinerja organisasi dan menyelaraskan dengan strategi bisnis yang dijalankan.

Manajemen risiko adalah kumpulan langkah-langkah yang dilakukan oleh perusahaan untuk mengenali, menilai, mengatur, dan mengendalikan risiko yang mungkin muncul. Hal ini bertujuan untuk mengurangi efek negatif dan memastikan perusahaan dapat mencapai sasarannya [4], [10], [11]. COSO ERM mendefinisikan manajemen risiko sebagai proses yang melibatkan integrasi antara budaya organisasi, kemampuan, dan praktik yang berkaitan dengan strategi dan pelaksanaan tugas perusahaan, yang bertujuan untuk mengatur risiko agar dapat menambah, menjaga, dan meningkatkan nilai perusahaan [4], [12].

Penerapan kerangka kerja COSO ERM membutuhkan integrasi manajemen risiko ke dalam strategi dan tujuan keseluruhan perusahaan. Pendekatan ini memastikan bahwa manajemen risiko berlangsung secara menyeluruh di seluruh sektor perusahaan, mengingat bahwa setiap departemen memiliki risiko unik yang dapat mempengaruhi strategi dan hasil dari departemen tersebut, serta berdampak pada kinerja keseluruhan perusahaan [13]. Kerangka kerja COSO ERM mencakup lima komponen penting yang saling terhubung dan berinteraksi, seperti yang ditunjukkan dalam gambar1 yang diambil dari sumber COSO tahun 2017.



Gambar 1. Kerangka Kerja COSO ERM

Dengan mengadopsi COSO ERM, organisasi berkomitmen untuk memasukkan manajemen risiko ke dalam strategi dan kinerja perusahaan secara holistik [14]. Pendekatan ini mengakui bahwa risiko tersebar di berbagai departemen, di mana setiap bagian memiliki potensi untuk mempengaruhi strategi dan hasil keseluruhan perusahaan. Lima komponen utama dalam COSO ERM ini saling terkait untuk membentuk kerangka manajemen risiko yang efektif, salah satunya adalah *governance and culture*, yaitu tata kelola yang efektif menyediakan struktur bagi organisasi dalam mengenali, mengevaluasi, dan mengatasi risiko, sementara budaya organisasi yang solid mendukung keputusan yang etis dan bertanggung jawab. Berikut penjelasan dari kelima prinsip pada komponen tersebut:

- a. *Exercise Board Risk Oversight*: Peran penting dewan direksi adalah dalam mengawasi manajemen risiko. Ini termasuk mengkritisi keputusan strategis dan operasional, memastikan manajemen memiliki pemahaman yang tepat tentang risiko, dan memastikan strategi organisasi selaras dengan tujuan dan nilai-nilai inti perusahaan [10]–[12]. Dewan harus memiliki pengetahuan yang mendalam tentang risiko yang dihadapi oleh organisasi dan beroperasi secara independen dari manajemen untuk memastikan praktik manajemen risiko yang memadai dan efektif.
- b. *Establish Operating Structures*: Struktur operasional yang efisien mendukung manajemen risiko yang baik. Ini termasuk pembentukan jalur pelaporan yang jelas, alokasi tanggung jawab, dan sistem komunikasi yang efektif [10]–[12]. Struktur ini harus sesuai dengan ukuran dan kompleksitas organisasi, serta memungkinkan pelaporan yang akurat dan pengambilan keputusan yang cepat dalam menghadapi risiko.
- c. *Defines Desired Culture*: Budaya organisasi yang ideal harus mendukung manajemen risiko dengan mendorong perilaku yang bertanggung jawab dan etis. Ini termasuk mendorong transparansi, integritas, dan kejujuran [10]–[12]. Budaya ini harus memfasilitasi karyawan untuk melaporkan masalah tanpa rasa takut akan retribusi dan menggalakkan diskusi terbuka mengenai risiko dan peluang.
- d. *Demonstrates Commitment To Core Value*: Nilai inti organisasi harus jelas dan diinternalisasi di seluruh organisasi. Ini harus tercermin dalam setiap aspek operasional, dari proses pengambilan keputusan hingga interaksi sehari-hari antar karyawan. Komitmen terhadap nilai-nilai ini harus ditegaskan melalui kebijakan, prosedur, dan sistem insentif yang menegaskan pentingnya nilai-nilai ini bagi keberhasilan organisasi [10]–[12].
- e. *Attracts, Develops, and Retains Capable Individuals*: Organisasi harus berusaha mengembangkan dan mempertahankan tenaga kerja yang berkualitas. Ini termasuk investasi dalam pelatihan dan pengembangan, serta menciptakan jalur karier yang jelas yang memungkinkan karyawan untuk berkembang [10]–[12]. Manajemen harus menetapkan ekspektasi yang jelas dan memberikan umpan balik yang membantu karyawan memahami kontribusi mereka terhadap manajemen risiko di organisasi.

## 2. METODE PENELITIAN

### 2.1. Pendekatan Penelitian

Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus, yang berfokus pada PT. Agro, khususnya pada divisi *Information Technology* (IT). Divisi ini dipilih karena divisi IT yang memberikan segara layanan IT bagi seluruh divisi PT. Agro. Penelitian ini berlandaskan pada paradigma naturalis, yang merupakan pendekatan utama dalam memahami perilaku manusia dari konteks perilaku itu sendiri. Pendekatan ini membutuhkan pemahaman dan adaptasi terhadap kondisi sosial yang dihadapi selama penelitian, untuk mendapatkan jawaban atas rumusan masalah yang telah ditetapkan.

### 2.2. Subyek dan Lokasi Penelitian

Dalam penelitian ini, para informan yang dipilih adalah manajer dari divisi IT, manajer divisi *finance*, serta manajer audit internal. Alasan pemilihan mereka adalah karena mereka memiliki peran langsung dalam mengatasi masalah operasional perusahaan dan terlibat dalam proses pengambilan keputusan untuk menangani masalah tersebut. Tempat penelitian ini berlangsung di PT. Agro yang terletak di Surabaya Barat, Jawa Timur. Lokasi ini terpilih sebagai pusat pengumpulan data dan informasi yang relevan untuk memecahkan masalah yang dihadapi dalam penelitian. Informasi lebih lanjut mengenai karakteristik dan kriteria dari informan-informan ini tersedia dalam Tabel 1.

Tabel 1. Informasi Data Narasumber Penelitian

Jabatan	Kriteria
Manajer <i>Information Technology</i> (Informan 1)	Memahami insiden atau masalah yang terjadi
	Mengalami pengaruh dari risiko yang muncul
	Mengalami secara langsung dalam menghadapi masalah yang terjadi
	Membuat kebijakan pada divisi IT
Manajer <i>Finance</i> (Informan 2)	Memahami insiden atau masalah yang terjadi
	Sebagai pihak yang menggunakan jasa divisi IT
Manajer Internal Audit (Informan 3)	Sebagai pihak yang melakukan penilaian secara independen
	Memiliki pengetahuan akan budaya, serta nilai perusahaan

### 2.3. Jenis dan Sumber Data

Studi ini menggunakan data kualitatif termasuk prosedur operasional standar, deskripsi pekerjaan, dan aktivitas perusahaan. Data kuantitatif yang digunakan meliputi notulen *meeting*, *log data* IT, *software update report*, dan sebagainya. Data dikumpulkan melalui sumber primer dan sekunder, dengan data primer didapatkan melalui

pengamatan langsung dan wawancara, sedangkan data sekunder berasal dari dokumen notulen rapat, laporan *key performance indicator* divisi IT, laporan penyelesaian komplain divisi IT, dan sebagainya.

#### 2.4. Metode Pengumpulan Data

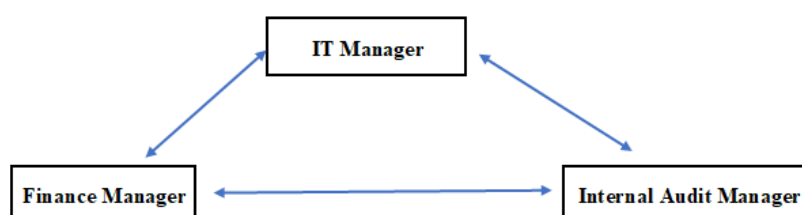
Dalam penelitian ini, pengumpulan data dilakukan melalui wawancara, observasi, dan dokumentasi. Wawancara dilaksanakan secara terstruktur dengan pedoman wawancara sebagai alat bantu, sementara observasi dilakukan secara terstruktur dengan pedoman observasi. Metode dokumentasi membutuhkan berbagai dokumen pendukung proses penerapan manajemen risiko terhadap *Information Technology Risk Governance* pada PT. Agro

#### 2.5. Teknik Analisis Data

Metode analisis data dalam studi ini mengacu pada kerangka kerja yang dirinci oleh Miles dan Huberman, seperti yang dijelaskan dalam literatur Sugiyono (2018) [15], terbagi dalam empat langkah. Langkah pertama adalah pengambilan data, yang melibatkan metode seperti wawancara, survei, observasi, dan pengumpulan dokumen. Langkah kedua adalah reduksi data, yaitu proses penyederhanaan, fokus pada elemen-elemen kunci, dan pengorganisasian data. Langkah ketiga adalah presentasi data, umumnya berbentuk narasi tekstual. Langkah terakhir adalah membuat kesimpulan, yang diambil dari hasil reduksi data dan memberi jawaban terhadap pertanyaan penelitian. Kesimpulan ini bersifat tentatif dan dapat berubah jika tidak ada dukungan bukti yang memadai, tetapi menjadi lebih kuat dan kredibel ketika didukung oleh bukti yang valid dan konsisten [16].

#### 2.6. Validitas Data

Pada penelitian ini menggunakan triangulasi sumber yaitu mengumpulkan serta mencari kebenaran informasi tertentu melalui berbagai sumber [17]. Pada penelitian ini dilakukan wawancara dengan memberikan berbagai pertanyaan kepada pihak-pihak tertentu yang memiliki peranan penting sekaligus sebagai penanggung jawab atas kegiatan operasional PT. Agro, yaitu kepada jenjang manajerial untuk divisi IT, *finance*, dan internal audit yang dapat dilihat pada Gambar 2. Hal ini dilakukan dengan tujuan memperoleh hasil wawancara yang akurat dalam proses penerapan ITRG berdasarkan COSO ERM di PT. Agro, sehingga akan diperoleh data serta informasi yang valid dari sumber yang berbeda.



Gambar 2. Triangulasi Tiga Sumber Data

### 3. HASIL DAN PEMBAHASAN

Pembahasan Untuk memastikan bahwa *Integrated Technology Risk Governance* (ITRG) berfungsi efektif, langkah pertama adalah memahami prinsip-prinsip governance dan budaya dalam *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) *Enterprise Risk Management* (ERM), yang berjumlah lima. Pertama, prinsip pengawasan risiko oleh dewan, yang menekankan peran dewan direksi dalam mengawasi manajemen risiko, mengaudit keputusan kritis, dan memastikan manajemen risiko sesuai dengan nilai dan strategi organisasi. Khususnya di Divisi IT, setiap kegiatan seperti pembaruan program, *backup* data, analisis data, dan pembuatan jaringan TI harus didasarkan pada manajemen risiko yang solid. Identifikasi risiko di TI dilakukan melalui *brainstorming*, yang merupakan diskusi kelompok tidak terstruktur untuk mengidentifikasi risiko potensial [18]. Dipandu oleh fasilitator, sesi ini menghasilkan ide-ide baru untuk menghadapi risiko dalam proyek atau organisasi, yang kemudian didokumentasikan untuk tindakan selanjutnya. Divisi IT di perusahaan ini telah mengambil langkah-langkah penting untuk memastikan pengawasan efektif atas manajemen risiko. Salah satu langkah utamanya adalah integrasi analisis risiko ke dalam perencanaan strategis. Ini dilakukan untuk menyesuaikan arah strategis divisi IT dengan tujuan keseluruhan perusahaan. Dengan cara ini, manajer IT dapat membuat keputusan yang lebih tepat dalam mengalokasikan sumber daya, tidak hanya untuk menangani risiko yang ada tetapi juga untuk memanfaatkan peluang yang muncul. Selain itu, divisi IT juga menetapkan *key performance indicators* (KPI) yang sejalan dengan tujuan strategis perusahaan dan tingkat toleransi risikonya. KPI ini sangat penting dalam mengukur efektivitas pengelolaan risiko. Mereka dipantau secara berkala, dan penyesuaian dilakukan sesuai dengan perubahan kondisi bisnis dan lingkungan. Pendekatan ini memastikan bahwa perusahaan dapat bertindak secara proaktif dalam mengidentifikasi dan mengatasi berbagai risiko yang mungkin muncul.

Komponen *establish operating structures* pada COSO ERM menyoroti kebutuhan akan struktur organisasi yang jelas dalam divisi untuk mendukung pengelolaan risiko efektif. Hal ini melibatkan penentuan jelas terhadap pembagian tugas dan tanggung jawab, interaksi antar-unit bisnis, dan penetapan pihak yang bertanggung jawab atas keputusan khusus. Tujuannya agar setiap anggota di divisi IT memahami peran mereka dalam mengelola risiko dan dapat memberikan kontribusi terbaik untuk divisi dan perusahaan secara keseluruhan. Dalam divisi IT perusahaan, setiap bagian memegang peranan khusus dalam mengelola risiko IT. Sistem pengembangan bertanggung jawab atas pekerjaan *programmer* dan analis dalam mengimplementasikan serta memelihara sistem yang ada. Sementara itu, manajemen proyek menangani perencanaan dan pelaksanaan proyek IT masa depan, termasuk pembelian dan pengembangan program yang membutuhkan dukungan IT. Bagian *help desk* berfokus pada menangani pertanyaan dan isu teknis dari pengguna atau klien. Manajemen data mengurus arsitektur data dan mengelola data sebagai aset penting perusahaan. Keamanan informasi fokus pada pengamanan data server dan data lokal. Terakhir, administrator sistem bertanggung



jawab atas pemeliharaan sistem komputer utama *multi*-pengguna, yang mencakup berbagai jaringan seperti jaringan lokal (LAN), jaringan area lokal nirkabel (WLAN), jaringan area luas, jaringan area pribadi, jaringan area penyimpangan hingga, serta intranet dan *extranet*.

Evaluasi berikutnya adalah terhadap komponen ketiga yaitu *defines desired culture*. Pada perusahaan terdapat dua jenis budaya utama yang diterapkan oleh manajemen, yaitu budaya kekeluargaan dan budaya BISA. Kedua budaya tersebut juga diterapkan pada divisi IT, dimana budaya kekeluargaan dibangun dengan menumbuhkan rasa persatuan, kepercayaan, dan saling mendukung antar karyawan, mirip dengan hubungan kekeluargaan. Sedangkan budaya BISA dibentuk pada divisi IT agar setiap karyawan divisi IT untuk terbuka terhadap perubahan, tidak gentar menghadapi tantangan, serta proaktif dan persisten dalam menyelesaikan masalah hingga mencapai solusi. Untuk mensosialisasikan budaya perusahaan, beberapa metode diterapkan secara aktif. Salah satunya adalah melalui pengiriman *newsletter* perusahaan secara rutin. Buletin ini dikirimkan melalui email perusahaan untuk secara berkala memperbarui dan mengingatkan karyawan tentang nilai-nilai budaya organisasi. Metode lain yang penting adalah melalui teladan dari manajer IT. Peran manajer IT sangat penting karena karyawan sering mengambil contoh dari perilaku pimpinan mereka. Teladan ini membantu mempraktikkan nilai-nilai budaya perusahaan secara langsung. Selain itu, nilai budaya juga diintegrasikan ke dalam kebijakan divisi IT. Hal ini melibatkan penggabungan nilai-nilai budaya ke dalam dokumen resmi divisi IT, seperti kode etik, panduan karyawan, dan proses evaluasi kinerja. Langkah yang dilakukan tersebut memiliki peranan penting untuk memperkuat dan memastikan penerapan nilai-nilai tersebut dalam kegiatan sehari-hari karyawan.

Evaluasi prinsip berikutnya pada COSO ERM yang diterapkan pada perusahaan adalah *Demonstrates Commitment To Core Value*. Prinsip ini mengacu pada tindakan nyata yang diambil oleh sebuah organisasi untuk memastikan bahwa nilai-nilai intinya tidak hanya dipahami, tetapi juga diterapkan dan diintegrasikan ke dalam setiap aspek dari operasi bisnisnya. Ini berarti bahwa nilai-nilai tersebut dijadikan dasar dalam pengambilan keputusan, perilaku karyawan, dan strategi perusahaan secara keseluruhan. Hasil evaluasi tersebut dapat dilihat pada tabel 2 berikut ini.

Tabel 2. Penerapan *Value* Pada Divisi IT

Nilai ( <i>Value</i> )	Deskripsi
<i>Integrity</i>	Diharapkan divisi IT memiliki sikap berpegang teguh pada prinsip kejujuran, transparansi, dan keadilan, tidak hanya dalam mematuhi hukum tetapi juga dalam menjunjung tinggi etika dan moralitas.

Nilai (Value)	Deskripsi
<i>Agility</i>	Divisi IT diharapkan menjadi divisi yang penuh inovasi serta dapat beradaptasi dengan kecepatan dan efisiensi dalam menghadapi perubahan pasar atau tantangan internal. Ini berarti bahwa divisi IT wajib menyediakan fasilitas bagi perusahaan agar manajemen dapat mengambil keputusan secara efektif dalam mengimplementasikan strategi baru.
<i>Collaboration</i>	Penerapan nilai ini pada divisi IT untuk memahami pentingnya kerja tim dan sinergi antar karyawan untuk mencapai tujuan bersama. Ini mencakup berbagi pengetahuan, mendukung satu sama lain, dan menggabungkan keahlian untuk menghasilkan hasil yang lebih baik.
<i>Excellence</i>	Dengan menerapkan ketiga nilai sebelumnya, maka diharapkan divisi IT tidak hanya memenuhi ekspektasi perusahaan tetapi melampaui ekspektasi perusahaan, dan terus-menerus mencari cara untuk meningkatkan performa divisi IT.

Prinsip terakhir dalam COSO ERM yang diterapkan oleh divisi IT adalah *Attracts, Develops, and Retains Capable Individuals*. Prinsip ini berfokus pada pentingnya memiliki karyawan yang memiliki keahlian, pengetahuan, dan pengalaman yang sesuai untuk mencapai tujuan organisasi. Divisi IT menerapkan prinsip ini dengan cara memberikan pelatihan secara rutin kepada tim divisi IT, dan juga sertifikasi untuk meningkatkan kompetensi mereka sebagai divisi IT. Selain itu juga memberikan jenjang karier yang baik bagi anggota divisi IT yang memiliki kompetensi, sehingga proses kaderisasi pada divisi IT dapat berjalan dengan efektif.

Kelima prinsip tersebut secara langsung sudah ditanyakan kebenarannya kepada manajer IT, yang kemudian dipastikan terhadap manajer *finance* yang merupakan salah satu *user* utama produk IT. Pernyataan manajer IT tersebut telah disetujui kebenarannya oleh manajer divisi *finance*, dimana divisi IT telah cukup baik menerapkan proses ITRG sehingga dapat memberikan hasil yang positif bagi pelayanan IT pada PT. Agro. Sedangkan penerapan ITRG berdasarkan budaya serta nilai perusahaan, juga telah dikonfirmasi kepada manajer internal audit, yang memang sangat paham akan budaya serta nilai yang berlaku pada PT. Agro

#### 4. KESIMPULAN

Semakin pesatnya perkembangan teknologi yang ada, maka akan banyak risiko yang timbul pada pengelolaan informasi teknologi pada perusahaan. Oleh karena itu sangat penting bagi perusahaan untuk memiliki ITRG yang efektif, sehingga perusahaan dapat menciptakan langkah yang tepat dalam mengendalikan serta melindungi data perusahaan. Divisi IT memiliki peranan penting dalam memberikan pelayanan bagi perusahaan, baik dari segi penginputan data, pengolahan data hingga penyajian data oleh

karena itu divisi IT perlu menerapkan ITRG yang efektif perlu dukungan penerapan ERM yang baik juga, sehingga seluruh kegiatan yang dilakukan berbasis manajemen risiko sehingga ketika perusahaan dihadapkan dengan keadaan yang tidak pasti, perusahaan dapat memiliki persiapan yang matang bahkan dapat memanfaatkan peluang yang ada.

Evaluasi ITRG di divisi IT PT. Agro dijalankan melalui pendekatan triangulasi. Pendekatan ini melibatkan tahapan wawancara dengan manajer IT, diikuti dengan konfirmasi dari manajer keuangan dan manajer audit internal. Langkah ini bertujuan untuk memastikan bahwa ITRG diterapkan dengan efektif di divisi IT. Dasar penilaian ITRG divisi IT berdasarkan komponen *governance and culture* COSO ERM dengan lima prinsip yang menaungi, mulai dari *exercise board risk oversight, establish operating structures, defines desired culture, demonstrates Commitment to core value, dan attracts, develops, and retains capable individuals*. Hasil konfirmasi dengan ketiga manajer tersebut ternyata divisi IT telah menerapkan kelima prinsip tersebut dengan baik, sehingga dapat disimpulkan bahwa divisi IT PT. Agro telah menerapkan ITRG dengan efektif.

## 5. SARAN

Penelitian ini memiliki keterbatasan hanya menilai *Information Technology Risk Governance* (ITRG) berdasarkan salah satu komponen COSO ERM saja, untuk penelitian selanjutnya disarankan dapat dilakukan evaluasi penerapan ITRG berdasarkan COBIT ataupun membahas pada komponen COSO ERM lainnya seperti *strategic objective setting* hingga *performance* yang akan lebih membahas manajemen risiko IT pada kegiatan operasional sehari-hari.

## DAFTAR PUSTAKA

- [1] A. Irhandayaningsih, "Performance Measurement of Information Technology Governance in The Library of Diponegoro University Using COBIT Assessment Framework," *E3S Web of Conferences*, vol. 202, p. 15001, Nov. 2020, doi: 10.1051/e3sconf/202020215001.
- [2] K. Ayuwuragil, "Pelaku Industri Nilai Pengelolaan Data di Indonesia Buruk," <https://www.cnnindonesia.com/teknologi/20180208224330-185-274945/pelaku-industri-nilai-pengelolaan-data-di-indonesia-buruk>, Feb. 12, 2018.
- [3] I. Mardiah, "Dari e-Government ke IT Governance," <https://inet.detik.com/cyberlife/d-3334163/dari-e-government-ke-it-governance>, Nov. 01, 2016.
- [4] M. Zain, *Study Book CIA Part 1*. 2022.
- [5] E. Karanja, "Does the hiring of chief risk officers align with the COSO/ISO enterprise risk management frameworks?," *International Journal of Accounting & Information Management*, vol. 25, no. 3, pp. 274–295, Aug. 2017, doi: 10.1108/IJAIM-04-2016-0037.
- [6] R. Nurlaela and S. Suhendi, "Evaluasi Manajemen Risiko Tata Kelola TI berbasis COSO ERM Intergrated Framework pada Perguruan Tinggi XYZ," *Jurnal Informatika Terpadu*, vol. 7, no. 1, pp. 15–20, Mar. 2021, doi: 10.54914/jit.v7i1.316.

- [7] F. N. Arisandy *et al.*, "Kajian Teoritis Tentang Ukuran Perusahaan Dan Jumlah Dewan Direksi Terhadap Kinerja Keuangan Perusahaan Melalui Penerapan Model COSO Enterprise Risk Management," *Jurnal Akuntansi dan Pajak*, vol. 23, 2022.
- [8] P. D. Setyadi and E. S. Negara, "AUDIT STRATEGI TATA KELOLA IT PADA STMIK BINA NUSANTARA JAYA LUBUKLINGGAU MENGGUNAKAN FRAMEWORK COBIT 5," *CogITO Smart Journal*, vol. 8, no. 1, pp. 244–258, Jul. 2022, doi: 10.31154/cogito.v8i1.372.244-258.
- [9] M. Muthmainnah, S. Safwandi, M. Jannah, and V. Ilhadi, "Evaluasi Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 Proses Dss03 Dan Mea01 Di Universitas X," *Sisfo: Jurnal Ilmiah Sistem Informasi*, vol. 5, no. 1, May 2021, doi: 10.29103/sisfo.v5i1.4848.
- [10] Insitute Internal Auditor, *The IIA's CIA Learning System Part 1*. Insitute Internal Auditor, 2022.
- [11] B. Hock, C. Burch, K. Hock, and K. Kaluhiokalani, *CIA Part I Essentials of Internal Auditing*. 2019.
- [12] Gleim Publications, *Study Unit Four Risk Management*. 2021.
- [13] B. L. Handoko, D. Septianto, and A. Alyssa, "Aplikasi Penggunaan Enterprise Risk Management (ERM) Integrated Framework Coso Untuk Mendeteksi Risiko Kecurangan Pada Transaksi Tidak Biasa Unit Bisnis Pt. Doremi Pizza Indonesia [Application of Integrated Enterprise Risk Management (ERM) COSO Framework to Detect Fraud Risk in Unusual Transactions at PT. Doremi Pizza, Indonesia]," *DeReMa (Development Research of Management): Jurnal Manajemen*, vol. 14, no. 1, p. 134, May 2019, doi: 10.19166/derema.v14i1.1181.
- [14] S. Rikaz, A. D. Ulhaq, R. H. Mulyono, and R. Cahyaningtyas, "Perancangan COSO Enterprise Risk Management Pada Perusahaan Penerbit Dan Percetakan (Studi Kasus Pada CV.Gema Insani Press)," *3rd National Conference on Accounting and Fraud Auditing*, vol. 1, 2022.
- [15] Sugiyono, *Metode Penelitian Pendidikan Pendekatan Kuantitatif, kualitatif, dan R&D*. Bandung: Alfabeta, 2010.
- [16] A. M. Yusuf, *Metode Penelitian: Kuantitatif, Kualitatif, Dan Penelitian Gabungan*. Jakarta: Kencana, 2017.
- [17] A. Sanusi, *Metodologi Penelitian Bisnis*. Jakarta: Salemba Empat, 2019.
- [18] J. Tang and K. E. Karim, "Financial fraud detection and big data analytics – implications on auditors' use of fraud brainstorming session," *Managerial Auditing Journal*, vol. 34, no. 3, pp. 324–337, Mar. 2019, doi: 10.1108/MAJ-01-2018-1767.