JURNAL TEKNOLOGI INFORMASI
LPKIA
Jurnal Teknologi Informasi
Volume 6 No.1 | Juli 2026
https://jurnal.lpkia.ac.id/index.php/jti/index
P-ISSN 2303-1069
E-ISSN 2808-7410

PENILAIAN TINGKAT KAPABILITAS DEPARTEMEN TI PT. VISI KARYA PRAKARSA MENGGUNAKAN COBIT 5 (DOMAIN APO4, APO12, APO13, DAN DSS05)

Sri Kurniasih[1], Khoirunisa Mujahidah Salman [2]
[1]Fakultas Teknologi Informasi dan Digital, Program Studi Sistem Informasi,
Institut Digital Ekonomi LPKIA
sri.kurniasih@lpkia.ac.id[1], khoirunisams@gmail.com[2],

Abstrak

PT Visi Karya Prakarsa merupakan perusahaan yang memanfaatkan Teknologi Informasi (TI) untuk menunjang proses bisnisnya, dengan fokus utama pada pengembangan produk aplikasi bernama Antrique—sebuah aplikasi antrian berbasis web dan mobile. Meskipun pemanfaatan TI telah berjalan dengan baik, masih ditemukan kekurangan dalam penerapannya, khususnya pada aspek keamanan. Hal ini terbukti dengan terjadinya insiden keamanan (*security incident*) berupa peretasan (*hacking*) pada aplikasi Antrique.

Untuk mencegah terulangnya insiden serupa, diperlukan pemahaman mengenai tingkat kematangan tata kelola keamanan TI di perusahaan. Penelitian ini bertujuan untuk mengukur **Tingkat Kapabilitas (Capability Level)** keamanan TI pada Departemen TI PT Visi Karya Prakarsa dengan menggunakan Kerangka kerja (*framework*) **COBIT 5 pada domain proses APO04, APO12, APO13, dan DSS05**. Hasil penilaian kapabilitas ini diharapkan dapat mengidentifikasi titik lemah dan menghasilkan rekomendasi perbaikan yang berbasis bukti, sehingga berbagai kerentanan dapat diatasi secara sistematis.

Penelitian diawali dengan pengumpulan data melalui observasi, wawancara, dan penyebaran kuesioner. Data kemudian dianalisis untuk menghitung Tingkat Lapabilitas (***Capability Level***) kondisi *as-is*, melakukan analisis kesenjangan (***Gap Analysis***), dan merumuskan rekomendasi. Hasil penilaian menunjukkan level kapabilitas pengelolaan inovasi **(APO04)** berada pada level 2.2 (*Managed Process*), pengelolaan layanan keamanan **(DSS05)** pada level 2.6 (*Established Process*), serta pengelolaan risiko **(APO12)** dan keamanan **(APO13)** masing-masing pada level 2.3 (*Managed Process*), temuan ini mengindikasikan bahwa seluruh proses memerlukan peningkatan kematangan yang berkelanjutan untuk ketahanan keamanan TI perusahaan secara terstruktur.

Kata kunci : Audit SI, Keamanan SI, COBIT 5, Domain APO & DSS

1 Pendahuluan

Di era perkembangan informasi yang pesat saat ini, peran tata kelola keamanan Teknologi Informasi (TI) menjadi krusial untuk menjamin kualitas dan ketersediaan layanan TI suatu perusahaan [1]. Penerapan tata kelola TI yang baik merupakan prasyarat untuk menghindari kendala dalam kegiatan operasional [2]. Sebagai bagian integral dari tata kelola perusahaan, tata kelola TI berfokus pada sistem dan teknologi informasi, kinerja dan manajemen risiko [3]. Salah satu standar global yang digunakan dalam tata kelola teknologi informasi adalah **COBIT 5 (*Control Objectives for Information and Related Technology*)**, Standar COBIT versi 5 mengukur pada tata kelola teknologi informasi yang sesuai dengan tujuan bisnis Perusahaan [4].

P-ISSN 2303 – 1069
E-ISSN 2808 - 7410

Penelitian ini berfokus pada penilaian domain **APO (*Align*, *Plan*, *and***

(*Manage Security*), **APO12 (*Manage Risk*)**, **APO04 (*Manage Innovation*)**, dan **DSS05 (*Manage Security Services*)**.

PT. Visi Karya Prakarsa merupakan perusahaan yang bergerak di bidang Teknologi Informasi (TI). PT. Visi Karya Prakarsa memiliki produk TI berupa aplikasi untuk antrian yang bernama Antrique. Antrique merupakan aplikasi antrian yang dimana customer dapat mengambil serta memonitoring antrian tanpa harus mengunjungi tempat, dan bisa dijalankan melalui daring dari manapun [5]]. Namun, berdasarkan hasil observasi dan wawancara dengan staf departemen TI, menyebutkan bahwa aplikasi yang dibangun dengan menggunakan bahasa pemrograman PHP dengan *framework* YII mempunyai banyak celah untuk *hacker* mengakses *website* tersebut. Selain itu, jika menggunakan bahasa pemrograman PHP, *hacker* masih bisa memasukan *code* program *javascript* ke dalam form registrasi yang terdapat di *website* aplikasi tersebut. Dapat disimpulkan secara keseluruhan bahwa permasalahannya adalah terjadi *hacking*, karena tidak adanya *monitoring* aplikasi dan *maintenance* secara berkala, juga jumlah pegawai yang kurang pada bagian *cyber security*.

Berdasarkan latar belakang tersebut, maka penelitian ini bertujuan untuk mengetahui tingkat kapabilitas **(*capability level*)** tata kelola keamanan TI di departemen TI dengan kebutuhan pada proses domain APO, dan DSS dalam Departemen TI berdasarkan *framework* COBIT versi 5. Penilaian dilakukan dengan menganalisis kesenjangan (*gap*) antara kondisi nyata (*as-is*) dan kondisi yang diharapkan (*to-be*) pada proses-proses COBIT 5 yang telah disebutkan. Hasil penelitian diharapkan dapat menjadi strategi rekomendasi untuk standarisasi proses perbaikan, baik dalam pembangunan sistem baru maupun pengembangan sistem informasi lainnya yang ada di Deprtemen TI pada PT Visi Karya Prakarsa.

1.1 Identifikasi Masalah

Berdasarkan latar belakang, permasalahan yang dapat diidentifikasi adalah:

1. Kurangnya *monitoring* aplikasi dan *maintenance* berkala mengakibatkan terjadinya *hacking*, sehingga menjadi ancaman serius terhadap aplikasi Antrique di departemen TI.
2. Keterbatasan jumlah pegawai untuk menangani keamanan *cyber* menyebabkan kerentanan terhadap serangan *cyber* dan kesulitan dalam menjaga keamanan sistem.
3. Kombinasi dari kedua masalah di atas menyebabkan tingkat kapabilitas departemen TI dalam pengelolaan keamanan informasi menjadi tidak terukur dan lemah. sehingga dapat berdampak terhadap keamanan informasi dan keamanan sistem perangkat lunak aplikasi Antrique di PT. Visi Karya Prakarsa.

1.2 Tujuan Perancangan

Berdasarkan identifikasi masalah, tujuan dari penelitian ini adalah:

1. Mengukur tingkat kapabilitas keamanan aplikasi menggunakan COBIT 5 agar aplikasi Antrique ter-monitoring secara berkala serta mengidentifikasi inovasi teknologi baru, sehingga meminimalisir terjadinya *hacking*.
2. Memberikan rekomendasi menambah pegawai khusus untuk *cyber security* dalam menjaga keamanan sistem aplikasi Antrique berdasarkan kebutuhan Departemen TI di perusahaan menggunakan COBIT 5.
3. Mengukur tingkat kapabilitas pada perangkat lunak Antrique di perusahaan, terkait dengan kebutuhan pada identifikasi permasalahan dengan menggunakan COBIT 5 berfokus pada domain APO 04, APO 12, APO 13 dan DSS 05. Sehingga diharapkan tidak terjadi permasalahan yang berulang.

2. Tinjauan Pustaka

Audit Sistem Informasi

Audit Sistem Informasi adalah proses evaluasi terhadap sistem, proses, atau produk dalam suatu perusahaan. Audit bertujuan untuk mengetahui apakah sistem sudah sesuai dengan standar, regulasi, dan praktik yang telah disetujui.[6]

Penilaian Tingkat Kapabilitas

Penilaian tingkat kapabilitas merupakan

P-ISSN 2303 – 1069
E-ISSN 2808 - 7410

proses yang dilakukan untuk mengetahui kondisi tingkat kapabilitas TI pada perusahaan saai ini (*as is*) dan dapat mengetahui yang akan diharapkan (*to be*) [7]

COBIT 5 (*Control Objectives for Information and Related Technology*)

Menurut ISACA, COBIT 5 adalah *framework* untuk membantu perusahaan dalam mencapai tujuan tata kelola dan manajemen TI sesuai dengan proses bisnis perusahaan dengan mengoptimalkan tingkat resiko penggunaan sumber daya dan mempertimbangkan kepentingan eksternal dan internal Perusahaan.[8]

Domain COBIT 5

Kerangka kerja COBIT 5 disusun dengan 5 domain yang dimana setiap domain memiliki penjelasan rinci dan terdapat panduan secara umum yang bertujuan untuk tata kelola TI dan manajemen Perusahaan [8]. Menurut ISACA [8], lima domain yang ada pada COBIT 5 adalah:

1. ***Evaluate, Direct and Monitor*** **(EDM)**
   Proses yang terdapat dalam domain EDM, meliputi proses pengendalian yang berkaitan dengan pengendalian pemangku kepentingan, proposisi nilai, optimalisasi resiko, dan sumber daya, termasuk aktivitas dan kegiatan yang difokuskan pada pengevaluasian pilihan strategi, serta memberikan pengarahan TI dan pemonitoran.
2. ***Align, Plan, and Organize*** **(APO)**
   Proses yang terdapat pada domain APO, meliputi proses penyesuaian, perencanaan, dan penataan agar Teknologi Informasi (TI) dapat berperan dengan maksimal dalam mencapai tujuan bisnis perusahaan.
3. ***Build, Acquire, and Implement*** **(BAI)**
   Proses yang terdapat pada domain BAI, meliputi proses membentuk, mencapai, dan menerapkan sistem yang sesuai dengan proses bisnis.
4. ***Delivery, Service and Support*** **(DSS)**
   Proses yang terdapat pada domain DSS, meliputi proses memberikan layanan dukungan atau layanan yang sesungguhnya untuk bisnis, seperti manajemen data dan perlindungan informasi yang berkaitan dengan proses bisnis.
5. ***Monitoring, Evaluation and Assess*** **(MEA)**
   Proses yang terdapat pada domain MEA, meliputi proses pemantauan, evaluasi, dan manajemen pengelolaan proses-proses yang dilakukan oleh divisi monitoring bersifat independen dapat dilakukan dari dalam atau luar perusahaan dan lembaga profesional alternatif lainnya.

Sedangkan dalam penelitian ini, domain COBIT 5 yang digunakan adalah:

1. ***Align, Plan, and Organize*** **(APO)**
   Pemilihan sub domain APO 04 (*Manage Innovation*) adalah difokuskan pada inovasi dalam pengelolaan Teknologi Informasi.
   Pemilihan sub domain APO 12 (*Manage Risk*) adalah untuk berfokus pada manajemen dan pengendalian resiko.
   Pemilihan sub domain APO 13 (*Manage Security*) adalah untuk berfokus pada pengelolaan keamanan informasi.
2. ***Delivery, Service and Support*** **(DSS)**
   Pemilihan sub domain DSS 05 (*Manage Security Services*) adalah difokuskan pada pengelolaan monitoring dan keamanan aplikasi oleh pegawai *cyber security*

Perhitungan Tingkat Kapabilitas

Pada jurnal [9] yang berjudul "Pengukuran Level Kapabilitas (*Capability Level*) Tata Kelola Teknologi Informasi Pada Koperasi Unit Desa Mino Saroyo Cilacap Menggunakan Cobit 5", dijelaskan mengenai hasil pemerolehan dari perhitungan kuesioner yang direkapitulasi untuk dapat Level Kapabilitas. Maka dapat dipaparkan dengan rumus penilaian sebagai berikut:

1. Menghitung Tingkat Kematangan (*Maturity Level*)

$$\text{Rata} - \text{rata} = \frac{\Sigma \text{ Jumlah skor masing} - \text{masing Responden}}{\Sigma \text{ Jumlah Responden}}$$

2. Menghitung Hasil Tingkat Kematangan

$$\text{Maturity Level} = \frac{\Sigma \text{ Jumlah skor rata} - \text{rata}}{\Sigma \text{ Jumlah Pertanyaan}}$$

3. Menghitung Level Kapabilitas

$$\text{Level Kapabilitas} = \frac{\Sigma \text{ Nilai Kapabilitas}}{\Sigma \text{ Jumlah Domain}}$$

Dalam penelitian ini, dilakukan perbedaan istilah antara nilai kapabilitas dengan tingkat kapabilitas. Level kapabilitas bisa bernilai tidak

P-ISSN 2303 – 1069
E-ISSN 2808 - 7410

bulat (bilangan desimal), yang dimana mempersentasikan semua proses pencapaian menuju kapabilitas tertentu. Sedangkan yang dimaksud dengan nilai kapabilitas yaitu lebih mempresentasikan langkah-langkah atau kelas yang akan dicapai dalam proses kapabilitas, dan dinyatakan dalam bentuk bilangan bulat

3. Hasil Pembahasan

Pemetaan & Pemilihan Domain COBIT 5

Panduan dalam pemetaan dan pemilihan domain serta proses yang relevan, telah difasilitasi oleh COBIT 5, termasuk proses agar penilaian yang dilakukan sesuai dengan kebutuhan penelitian dan merujuk pada tujuan-tujuan strategis penelitian dalam hal penilaian pengendalian internal sistem pada perusahaan PT. Visi Karya Prakarsa khususnya pada bagian Departemen TI.

Tabel berikut merupakan identifikasi proses COBIT 5:

Tabel 1 Identifikasi Proses Domain COBIT 5

Domain	***Align, Plan, and Organize* (APO)**	**Keterangan**
APO 04	Kelola Inovasi	Menganalisis strategi perencanaan dan arsitektur perusahaan melalui teknologi yang sudah ada, serta inovasi bisnis dan proses TI
APO 12	Kelola Resiko	Mengidentifikasi, menilai dan mengurangi resiko terkait TI dalam tingkat toleransi yang ditetapkan oleh perusahaan.
APO 13	Kelola Keamanan	Mendefinisikan, mengoperasikan, dan memantau sistem untuk manajemen keamanan informasi.
Domain	***Delivery, Service and Support* (DSS)**	**Keterangan**
DSS 05	Kelola Layanan Keamanan	Menetapkan dan mempertahankan peran keamanan informasi dan hak akses serta melakukan pemantauan keamanan.

Setelah melakukan pengumpulan data, wawancara untuk memahami proses bisnis yang berjalan dan kebutuhan data dan informasi dalam melakukan audit, maka peneliti melakukan audit berdasarkan tahapan audit SI.

Langkah-langkah audit yang dilakukan pada Departemen TI di PT. Visi Karya Prakarsa adalah sebagai berikut:

1. **Tahap 1 – Perencanaan**
   Tahapan pertama yaitu tahapan perencanaan. Pada tahap ini dilakukan pembatasan ruang lingkup (*scope*), objek yang akan diaudit (Departemen TI), pemahaman proses bisnis perusahaan, serta persiapan dan perencanaan terhadap proses pengumpulan data dan menentukan inputan untuk diolah pada tahap selanjutnya yaitu tahapan pengumpulan dan pengolahan data
2. **Tahap 2 – Pengumpulan & Pengolahan Data**
   Pada tahapan selanjutnya adalah pengumpulan dan pengolahan. Di dalam tahap ini, pertanyaan wawancara untuk mengetahui proses bisnis perusahaan dan pernyataan form kuesioner untuk mengetahui kondisi di perusahaan saat ini (*as is*), disusun berdasarkan standar COBIT 5 yang dilakukan kepada karyawan di Departemen TI pada PT. Visi Karya Prakarsa
3. **Tahap 3 – Pelaporan**
   Setelah dilakukan tahapan pengumpulan data, data yang didapat akan diolah untuk dihitung berdasarkan perhitungan *capability level*. Perhitungan *capability level* ini dilakukan mengacu pada hasil wawancara dan hasil responden penyebaran form kuesioner. Hasil dari perhitungan *capability level* yang menggambarkan situasi saat ini (*as is*) dan keadaan yang diharapkan (*to be*) dan menjadi panduan untuk dilakukan analisis kesenjangan (GAP *Analyst*)
4. **Tahap 4-Analisis Laporan Hasil**
   Pada tahapan terakhir yaitu analisis laporan hasil, menganalisis laporan hasil audit yang berbentuk usulan strategi rekomendasi perbaikan dan diserahkan kepada pihak Departemen TI di PT. Visi Karya Prakarsa

Dalam penelitian ini, metode pengumpulan data dilakukan dengan melakukan wawancara dengan naraumber yaitu CTO Departemen TI PT. Visi Karya Prakarsa untuk mengetahui proses bisnis yang sedang berjalan di perusahaan.

P-ISSN 2303 – 1069
E-ISSN 2808 - 7410

Kuesioner diajukan dengan beberapa pernyataan dengan jumlah responden 15 orang, yaitu karyawan Departemen TI menggunakan *rating scale* 0 - 5. Kemudian Hasil Responden dari kuesioner akan diolah untuk perhitungan *capability level*.

Rekapitulasi Jawaban Responden Kuesioner Kondisi Saat ini (*As is*)

Tabel 2. Level Kapabilitas Kondisi Saat Ini

Domain	Maturity Level	Nilai Kapabilitas
APO 04	2,2	2
APO 12	2,3	2
APO 13	2,3	2
DSS 05	2,6	3

Berdasarkan perhitungan, diperoleh jumlah nilai kapabilitas dari proses domain tersebut yaitu 9, kemudian dibandingkan dengan jumlah domain, menghasilkan 2,3, maka dapat disimpulkan bahwa tingkat kematangan kondisi perusahaan saat ini berada pada level 2 yaitu *Managed Process*. Artinya, proses yang diimplementasikan dan dikelola oleh perusahaan masih direncanakan, dipantau, dan disesuaikan dengan tujuan bisnis perusahaan, kemudian hasilnya ditetapkan dan dikontrol.

Saat ini, yang terjadi pada perusahaan adalah:

1. Pada APO 04, yaitu pengelolaan dan penerapan inovasi teknologi dalam mendukung tujuan perusahaan, Departemen IT sudah mulai menerapkan pengelolaan inovasi teknologi, tetapi masih mencari dan merencanakan inovasi teknologi terbaru untuk pengembangan aplikasi
2. Pada APO 12, fokus pada pengelolaan risiko TI untuk melindungi aset perusahaan dan memastikan bahwa risiko tetap berada pada tingkat yang ditetapkan. PT. Visi Karya Prakarsa sudah menerapkan pengelolaan risiko tetapi belum menetapkan cara mitigasi dan penanganan dari risiko yang telah dikelola.
3. Pada APO 13, yaitu pengelolaan dan peningkatan keamanan informasi dalam perusahaan untuk melindungi data dan aset dari ancaman keamanan, PT. Visi Karya Prakarsa telah mengelola dan menerapkan keamanan, tetapi belum menetapkan prosedur atau SOP dan standar dalam keamanan aplikasnya, sehingga ada beberapa ancaman yang tidak terdeteksi
4. Pada DSS 05, yaitu pengelolaan layanan keamanan TI dan kontrol akses untuk melindungi aset, data dan infrastruktur dan ancaman yang tidak sah, PT. Visi Karya Prakarsa dalam kontrol akses, perlindungan aset, data, dan infrastruktur, sudah menerapkan pengelolaan layanan keamanan TI, tetapi belum mensortir setiap inputan yang masuk, sehingga ancaman yang masuk tidak bisa diprediksi karena kurangnya *monitoring* keamanan dari pegawai *cyber security*.

Rekapitulasi Jawaban Responden Kuesioner Kondisi yang diharapkan (*To Be*)

Tabel 3. Level Kapabilitas Kondisi yang diharapkan

Domain	Maturity Level	Nilai Kapabilitas
APO 04	4,5	5
APO 12	4,5	5
APO 13	4,5	5
DSS 05	5,3	5

Berdasarkan perhitungan, diperoleh jumlah nilai kapabilitas dari proses domain tersebut yaitu 20, kemudian dibandingkan dengan jumlah domain, menghasilkan 5, maka dapat disimpulkan bahwa tingkat kematangan kondisi perusahaan yang diharapkan berada pada level 5 yaitu *Optimizing Process*. Artinya yang diharapkan oleh perusahaan adalah proses yang telah diimplementasikan, ditingkatkan secara terus-menerus sehingga memenuhi tujuan Perusahaan

Analisa Kesenjangan (GAP *Analyst*)

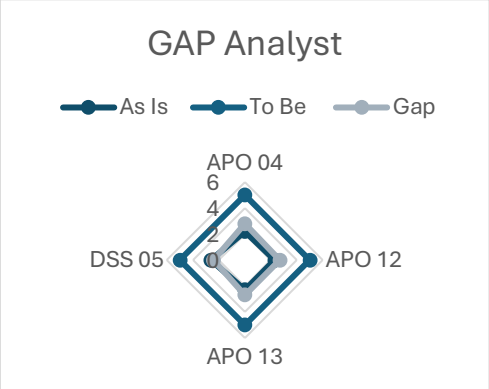
Berdasarkan hasil perhitungan rekapitulasi yang telah dilaksanakan, dapat diidentifikasi adanya ketidaksesuaian antara kondisi saat ini (*as is*) dengan kondisi yang diharapkan (*to be*) di dalam setiap domain proses. Berikut merupakan kesenjangan (GAP *Analyst*) dari proses pada domain APO 04, APO 12, APO 13, dan DSS 05:

Tabel 4. Analisa Kesenjangan

P-ISSN 2303 – 1069
E-ISSN 2808 - 7410

Domain	Kondisi Saat Ini (*As Is*)	Kondisi yang diharapkan (*To Be*)	GAP
APO 04	2,2	4,5	2,3
APO 12	2,3	4,5	2,2
APO 13	2,3	4,5	2,2
DSS 05	2,6	5,3	2,7
Rata-rata	2,3	4,7	2,4

Grafik analisis kesenjangan kondisi perusahaan saat ini dengan yang diharapkan:



Gambar 1. Grafik analisis kesenjangan kondisi perusahaan

Berdasarkan kondisi yang diharapkan (target yang harus dicapai) oleh perusahaan yaitu level 5, sedangkan diperoleh penilaian kondisi perusahaan saat ini sebesar 2,3, maka menunjukkan adanya kesenjangan sebesar 2,7 yang terjadi di dalam pemenuhan target tersebut.

Usulan Rekomendasi Perbaikan

Berdasarkan hasil perhitungan rekapitulasi responden yang telah didapatkan, terdapat beberapa hal yang perlu dipertimbangkan oleh Departemen TI PT. Visi Karya Prakarsa agar target yang diinginkan dapat tercapai. Beberapa usulan rekomendasi perbaikan tersebut, yaitu :

Tabel 4. Usulan rekomendasi Perbaikan untuk Departemen TI

Domain	**Keterangan**
APO 04	Tingkat kematangan kondisi perusahaan saat ini berada pada 2,2 yaitu *Managed Process*. Dalam proses pengelolaan dan penerapan inovasi teknologi untuk mendukung tujuan perusahaan, PT. Visi Karya Prakarsa sudah mulai menerapkan pengelolaan inovasi teknologi, tetapi masih mencari dan merencanakan inovasi teknologi terbaru untuk pengembangan dan keamanan aplikasi dari *hacking*. Usulan perbaikan: 1. Menulusuri informasi dan pemantauan terhadap inovasi perkembangan teknologi terbaru yang relevan dengan keamanan aplikasi, seperti mengganti Bahasa pemrograman dari *framework YII* menjadi *Laravel* dengan tingkat *secure* yang berbeda. 2. Mengimplementasikan rencana inovasi dan pemantauan. 3. Mengintegrasikan inovasi teknologi baru 4. Monitoring efektivitas terhadap penerapan teknologi baru dan melakukan evaluasi seperti area yang perlu dilakukan perbaikan dan penyesuaian. Dengan menerapkan usulan rekomendasi perbaikan ini, diharapkan perusahaan dapat terbuka terhadap inovasi teknologi baru dan mengimplementasikannya sehingga dapat mencegah ancaman *hacking*.
APO 12	Tingkat kematangan kondisi perusahaan saat ini berada pada 2,3 yaitu *Managed Process*. Dalam proses berfokus pada pengelolaan risiko TI untuk melindungi aset perusahaan dan memastikan bahwa risiko tetap berada pada tingkat yang ditetapkan, PT. Visi Karya Prakarsa sudah menerapkan pengelolaan risiko tetapi belum menetapkan cara mitigasi dan penanganan dari risiko yang telah dikelola. Usulan perbaikan: 1. Menetapkan prosedur / SOP untuk mitigasi risiko seperti langkah-langkah yang dapat diambil untuk mengurangi dampak risiko terhadap keamanan aplikasi.

P-ISSN 2303 – 1069
E-ISSN 2808 - 7410

	2. Meningkatkan pemantauan dan pengelolaan risiko secara berkala, seperti memantau aplikasi setiap hari, dan menggunakan *tools* yang dapat mendeteksi risiko. 3. Mendokumentasikan dan pelaporan risiko, mencakup potensi ancaman, tingkat parahnya ancaman, dan rencana mitigasi yang telah disiapkan. Dengan menerapkan usulan rekomendasi perbaikan ini, diharapkan perusahaan dapat memperkuat manajemen risiko TI, melindungi aset perusahaan dari ancaman, dan menjaga keamanan aplikasi.
APO 13	Tingkat kematangan kondisi perusahaan saat ini berada pada 2,3 yaitu *Managed Process*. Dalam proses pengelolaan dan peningkatan keamanan informasi dalam perusahaan untuk melindungi data dan aset dari ancaman keamanan, PT. Visi Karya Prakarsa telah mengelola dan menerapkan keamanan, tetapi belum menetapkan prosedur atau SOP dan standar dalam keamanan aplikasinya, sehingga ada beberapa ancaman yang tidak terdeteksi. Usulan perbaikan: 1. Menetapkan prosedur / SOP untuk keamanan aplikasi, termasuk identifikasi ancaman yang masuk, *scanning* kerentanan aplikasi, melakukan *code review* untuk memastikan aman dari celah inputan yang masuk, menjadwalkan audit keamanan, pengelolaan akses dan autentikasi, pemantauan dan *logging*, serta tanggapan insiden. 2. Memberikan pelatihan keamanan terhadap pegawai dalam pengelolaan keamanan dalam pengembangan aplikasi. 3. Menggunakan *tools* untuk mendeteksi anomali dalam meningkatkan monitoring aplikasi. 4. Melakukan evaluasi dan audit keamanan sesuai SOP yang ditetapkan untuk melakukan perbaikan berkelanjutan pada sistem keamanan aplikasi. Dengan menerapkan usulan rekomendasi perbaikan ini, diharapkan perusahaan dapat meningkatkan keamanan aplikasi, dan meminimalisir risiko ancaman *hacking*.
DSS O5	Tingkat kematangan kondisi perusahaan saat ini sudah mencapai level 2,6 yaitu *Established Process*. Dalam proses pengelolaan layanan keamanan TI dan kontrol akses untuk melindungi aset, data dan infrastruktur dan ancaman yang tidak sah, PT. Visi Karya Prakarsa dalam kontrol akses, perlindungan aset, data, dan infrastruktur, sudah menerapkan pengelolaan layanan keamanan TI, tetapi belum mensortir setiap inputan yang masuk, sehingga ancaman yang masuk tidak bisa diprediksi. Usulan perbaikan: 1. Merekrut pegawai *cyber security* minimal 2 orang untuk *monitoring*, pencegahan ancaman dan *maintenance* secara berkala, sehingga dapat memperkuat keamanan dan perlindungan terhadap ancaman yang masuk. 2. Melakukan pemantauan dan penyaringan atau *filtering* untuk semua inputan data yang masuk ke sistem, seperti email, file yang diupload, *code injection* dalam *field* inputan, serta alamat IP. 3. Membatasi hak akses sesuai dengan kebutuhan pekerjaan pegawai. Dengan menerapkan usulan rekomendasi perbaikan ini, diharapkan perusahaan dapat meningkatkan keamanan dari akses inputan yang tidak sah untuk melindungi aplikasi dari ancaman yang tidak terduga.

4. Kesimpulan dan Saran

Kesimpulan

P-ISSN 2303 – 1069
E-ISSN 2808 - 7410

Berdasarkan hasil penelitian yang telah dilakukan dapat diambil kesimpulan sebagai berikut :

1. Dalam pengelolaan inovasi teknologi di Departemen TI PT. Visi Karya Prakarsa, dengan tingkat kapabilitas proses Domain APO 04 (*Manage Innovation*) berada di level 2 (*Managed Process*) sebesar 2,2 dengan target berada pada level 5 (*Optimizing Process*) sebesar 4,5 yang menunjukkan bahwa sudah mulai menerapkan pengelolaan inovasi teknologi, tetapi masih mencari dan merencanakan inovasi teknologi terbaru untuk pengembangan dan keamanan aplikasi dari *hacking*. Untuk mencapai target dan meminimalisir terjadinya *hacking*, perlu mengambil tindakan seperti mengganti teknologi bahasa pemrograman *framework* YII menjadi *Laravel* dengan tingkat *secure* yang berbeda, dan memonitoring efektivitas pengimplementasian teknologi baru juga melakukan evaluasi seperti area yang perlu dilakukan perbaikan dan penyesuaian.

2. Dalam pengelolaan keamanan di Departemen TI PT. Visi Karya Prakarsa, dengan tingkat kapabilitas proses Domain DSS 05 (*Manage Security Services*) berada di level 3 (*Established Process*) sebesar 2,6 dengan target berada pada level 5 (*Optimizing Process*) sebesar 5,3 dan proses Domain APO 13 (*Manage Security*) berada di level 2 (*Managed Process*) sebesar 2,3 dengan target berada pada level 5 (*Optimizing Process*) sebesar 4,5 yang menunjukkan bahwa tidak adanya pegawai khusus dalam *cyber security* menghambat kemampuan perusahaan dalam menangani ancaman. Saat ini perusahaan telah mengelola dan menerapkan keamanan, tetapi belum menetapkan prosedur standar atau SOP dalam keamanan aplikasinya, sehingga ada beberapa ancaman yang tidak terdeteksi. Untuk mencapai target dan menjaga keamanan perusahaan, perlu diusulkan untuk merekrut pegawai *cyber security* minimal 2 orang untuk *monitoring*, pencegahan ancaman dan *maintenance* secara berkala, sehingga dapat memperkuat keamanan dan perlindungan terhadap ancaman yang masuk, juga menetapkan prosedur standar / SOP untuk keamanan aplikasi.

3. Dalam pengelolaan risiko dan keamanan di Departemen TI PT. Visi Karya Prakarsa, dengan tingkat kapabilitas proses Domain APO 12 (*Manage Risk*) berada di level 2 (*Managed Process*) sebesar 2,3 dan proses Domain APO 13 (*Manage Security*) berada di level 2 (*Managed Process*) sebesar 2,3 dengan target berada pada level 5 (*Optimizing Process*) sebesar 4,5 yang menunjukkan bahwa dalam pengelolaan risiko TI untuk melindungi aset perusahaan, perusahaan sudah menerapkan pengelolaan risiko tetapi belum menetapkan cara mitigasi dan penanganan dari risiko yang telah dikelola. Kemudian telah mengelola dan menerapkan keamanan, tetapi belum menetapkan prosedur standar atau SOP dalam keamanan aplikasinya. Untuk mencapai target dan mengelola risiko serta menjaga keamanan perusahaan, diusulkan untuk meningkatkan pemantauan dan pengelolaan risiko, seperti memantau aplikasi setiap hari, dan menggunakan *tools* yang dapat mendeteksi risiko dan menetapkan prosedur standar / SOP untuk keamanan aplikasi dan mitigasi risiko, mencakup identifikasi ancaman yang masuk serta prosedur mitigasi risiko seperti langkah-langkah yang dapat diambil untuk mengurangi dampak risiko terhadap keamanan aplikasi

Saran

Berdasarkan kesimpulan yang telah diuraikan diatas, berikut merupakan saran yang dapat menjadi pertimbangan ataupun bahan evaluasi bagi Departemen TI PT. Visi Karya Prakarsa:

1. Bagian Departemen TI disarankan untuk lebih memperhatikan keamanan aplikasi untuk melindungi aplikasi dari ancaman yang tidak terduga.
2. Perusahaan diharapkan dapat mengimplementasikan semua usulan rekomendasi perbaikan pada proses APO 04, APO 12, APO 13, dan DSS 05.
3. Untuk penelitian selanjutnya, perlu melakukan evaluasi penilaian tingkat kapabilitas pada Departemen TI di PT. Visi Karya Prakarsa, dapat memilih domain dengan proses yang berbeda.

DAFTAR PUSTAKA

P-ISSN 2303 – 1069
E-ISSN 2808 - 7410

[1] A. Putri, “Audit Layanan Teknologi Informasi Tribun Lampung Menggunakan Framework ITIL (Information Technology Infrastructure Library),” 2018.

[2] J. R Refina, L. Intan, Abdurrahman, and I.Santosa, “Analisis dan perancangan taatkelola TI BUMN pad aproses pengelolaan investasi dan pengelolaan resiko TI menggunakan kerangka kerja COBIT 2019,” vol. 7, 2020.

[3] D. D. N. . Soleha and D.Dartono, “Penerapan Framework Cobit 5 untuk audit tatakelola keamann informasi pada kantor wilayah Kementrian Agama Provinsi Lampung,” 2021.

[4] R. Harold Michael, A. R. Tanaamah, and M. N. N. Sitokdana, “ANALISIS KINERJA TATA KELOLA TEKNOLOGI INFORMASI PADA DINAS PERPUSTAKAAN DAN KEARSIPAN DAERAH KOTA SALATIGA MENGGUNAKAN FRAMEWORK COBIT 5.0,” pp. 14–21, 2014.

[5] S. Kurniasih and B. B. Bhiswara, “Penerapan Metode Ward & Peppard,” vol. 16, pp. 1–9, 2022.

[6] S. Kurniasih and Yulani P.P, “Audit SI Pengendalan Imternal Untuk persediaan obat dan alat kesehatan PT Parit Padang Gobal,” *J. Komput. Bisnis*, vol. 15, 2022.

[7] and G. I. N. L. M. U. Tiasmi, I. M. Candiasa, “Analisis Tingkat Kapabilitas Layanan Perizinan Online Kabupaten Badung Menggunakan Framework COBIT 5,” *J. Eksplora Inf.*, vol. 10, pp. 167–175, 2021.

[8] Isaca, *Cobit 5 Business Framework*, vol. 23, no. 3. 2012.

[9] A. R.F.K and R.Setyadi, “PEngukuran level kapablitas tata kelola TI pada koperasi unit desa Mino Saroyo Cilacap menggunakan Cobit 5,” *JURIKOM (Jurnal Ris. Komputer)*, 2022.