Kumpulan jurnaL Ilmu Komputer (KLIK)
Volume 07, No. 2 Juni 2020
ISSN: 2406-7857

ANALISIS AUDIT TATA KELOLA KEAMANAN TEKNOLOGI INFORMASI MENGGUNAKAN FRAMEWORK COBIT 5 PADA INSTANSI X

Daniel Alexander Octavianus Turang[1], Merry Christy Turang[2]
Program Studi Teknik Informatika[1], Program Studi Sistem Informasi[2]
Sekolah Tinggi Teknologi Bontang[1], Universitas Teknologi Yogyakarta[2]
daniel.alexanderot@gmail.com[1], merryturang12@gmail.com[2]

Abstract

Information technology governance has an important role in regulating the use and utilization of information technology at the X Institusions. Problems in the X Institusions, especially in the management of information technology security. In this research, the process design on COBIT 5 is the DSS05 and APO13 domains that focuses on ensuring the management of information technology security. Based on the capability level assessment for the DSS05 and APO13 domains, the results are still at level 1. Level 1 means that the IT security governance process has been implemented but the documentation process is incomplete. Therefore, IT security audits are needed in managing, directing and evaluating IT resources to create optimization of IT utilization. The target set is level 2, where management carries out processes that have been planned, monitored, and adjusted, as well as the exact products set, controlled and maintained.

Keywords*: COBIT 5, IT Governance, Security, Capability*

Abstrak

Tata kelola teknologi informasi memiliki peranan penting dalam mengatur penggunaan dan pemanfaatan teknologi informasi di Instansi X. Permasalahan yang muncul pada Instansi X, terutama pada bagian pengelolaan keamanan teknolgi informasi. Pada penelitian dilakukan perancangan proses pada COBIT 5 yaitu domain DSS05 dan APO13 yang berfokus dalam memastikan pengelolaan keamanan teknologi informasi. Berdasarkan penilaian tingkat kapabilitas untuk domain DSS05 dan APO13, hasilnya masih berada di level 1. Level 1 memiliki arti bahwa proses tata kelola keamanan TI telah dilaksanakan namun proses dokumentasi belum lengkap. Oleh karena itu, perlu adanya audit tata kelola keamanan TI dalam mengelola mengarahkan, dan mengevaluasi sumber daya TI untuk menciptakan optimalisasi pemanfaatan TI. Target yang ditetapkan adalah level 2, dimana manajemen melaksanakan proses yang telah direncanakan, dimonitor, dan disesuaikan, serta produk yang tepat ditetapkan, dikontrol dan dipelihara.

Kata kunci*: COBIT 5, Tata Kelola TI, Keamanan, Kapabilitas*

1. PENDAHULUAN

Instansi X memiliki tujuan yaitu mengelola arsip-arsip penting daerah yang didukung dengan pengelolaan aktivitas bisnis dan teknologi informasi. Instansi X memiliki 4 bidang yaitu departemen instansi daerah, departemen pengelolaan arsip, departemen pengembangan teknologi informasi, dan departemen pemberdayaan layanan Instansi Daerah. Rencana kerja Instansi X ini membahas mengenai pelaksanaan teknologi informasi. Penerapan rencana kerja tersebut dapat dibuktikan dari hasil wawancara dan diskusi dalam implementasi TI di Instansi X.

Terdapat beberapa permasalahan berkaitan dengan tata kelola teknologi informasi diantaranya teknologi informasi yang ada di organsasi belum berjalan secara optimal untuk mengelola proses dan tujuan bisnis. Hal ini disebabkan karena kemampuan sistem untuk pertukaran data dan informasi belum terintegrasi, jaringan komunikasi yang belum tercukupi di berbagai wilayah dengan skala kecil, informasi publik yang belum tersedia secara optimal, jaringan internet yang selalu eror, masih lambatnya penyelesaian resiko bisnis, keamanan sistem yang belum sesuai prosedur dan jumlah individu atau sumber daya pengelola teknlogi informasi komunikasi yang kurang. Akibatnya dukungan layanan teknologi yang digunakan ini belum mampu mendukung operasional secara optimal, dan diperlukan evaluasi terhadap teknolgi informasi yang telah dijalankan. Evaluasi direncanakan untuk menentukan keadaan objek dan hasil yang dicapai, serta digunakan sebagai pengambilan keputusan untuk mencapai tujuan. Instansi yang baik adalah instansi yang mementingkan aset publik terkait tata kelola yang baik pada TI [1]. Tata kelola TI tidak hanya dapat digunakan pada sektor industri maupun perusahan, tetapi juga digunakan dalam sektor publik untuk mengevaluasi proses yang telah dilaksanakan [2].

Dibutuhkan keamanan yang tinggi untuk menjaga kerahasiaan dan penyalahgunaan informasi dalam suatu organisasi [3]. Dalam upaya meningkatkan keamanan aktivitas operasional bisnis dan kualitas sumber daya teknologi informasi, Instansi X memerlukan evaluasi dan panduan agar terciptanya optimalisasi keamanan aset teknologi informasi yang ada. Tata kelola TI telah banyak diterapkan dalam sektor publik [4]. Penggunaan COBIT 5 ini mampu membantu dalam mengungkapkan ide-ide konseptual baru dibandingkan versi sebelumnya. COBIT 5 mendefinisikan panduan proses tata kelola teknologi informasi kedalam 5 domain, yaitu *Deliver, Service and Support* (DSS), *Evaluate, Direct and Monitor* (EDM), *Build, Acquire and Implement* (BAI), *Align, Plan and Organise* (APO), dan *Monitor, Evaluate and Assess* (MEA) [5]. Fungsi dari kelima domain ini ialah menentukan keselarasan antara tujuan bisnis, nilai antar *stakeholder* yang berbeda, dan nilai teknologi informasi yang digunakan. COBIT 5 tidak membatasi untuk setiap unit teknologi informasi saja tetapi mencakup seluruh organisasi. COBIT 5 mencakup panduan untuk integrasi dengan tata kelola TI di organisasi untuk penciptaan nilai dengan menentukan peran, kegiatan dan hubungan serta menunjukkan bahwa COBIT 5 bertujuan untuk menjadi *framework* panduan [6]. Berdasarkan masalah yang terjadi di Instansi X, maka dilakukan penelitian terkait perancangan tata kelola TI menggunakan COBIT 5 berfokus pada keamanan dengan domain DSS05 dan APO13.

2. METODOLOGI PENELITIAN

2.1. Audit Teknologi Informasi

Audit teknologi informasi secara umum adalah suatu proses dikumpulkannya data dan dievaluasinya bukti untuk menetapkan apakah suatu sistem aplikasi komputerisasi sudah diterapkan dan menerapkan sistem pengendalian, internal yang sudah sepadan, seluruh aktivas dilindungi dengan baik atau disalahgunakan dan juga terjamin integritas data, keandalan dan juga efektifitas dan efisiensi penyelenggaraan informasi berbasis komputer. Pelaksanaan audit mampu memberikan informasi terkait tingkat keamanan asset, pemeliharaan integritas data, mendorong pencapaian tujuan organisasi secara efektif, penggunaan sumberdaya secara effisien, dan mengetahui tingkat kematangan teknologi informasi, serta menghasilkan rekomendasi untuk mencapai tingkat kematangan yang optimal [7].

Aspek utama dalam audit teknologi informasi terdiri dari aspek conformance dan aspek performance. Aspek *conformance* (kesesuaian), tujuan audit teknologi informasi digunakan untuk Kerahasiaan (*Confidentiality*), Integritas (*Integrity*), Ketersediaan (*Availability*) dan Kepatuhan (*Compliance*). Sedangkan berdasarkan aspek *performance* (kinerja) digunakan untuk Efektifitas (*Effectiveness*), Efisiensi (*Efficiency*), dan Kehandalah (*Realibility*).

2.2. COBIT 5

COBIT 5 (*Control Objective for Information and Related Technology*) adalah serangkaian *best practice* yang terdiri dari ringkasan eksekutif, kerangka kerja, tujuan pengendalian, pedoman audit, alat implementasi dan pedoman manajemen yang sangat berguna untuk mengelola bisnis dan teknologi informasi (IT *management*) yang strategis. COBIT 5 juga memiliki peranan sebagai penggerak yang terkandung dalam 7 *enabler*, yaitu [8]:

a. *Principles, Policies and Framework*
b. *Organisational Structures*
c. *Process*
d. *Organization Structure*
e. *Culture, ethnics, and Behaviour*
f. *Information*
g. *Service, Infrastructure, and Applications*

2.3. Domain DSS05

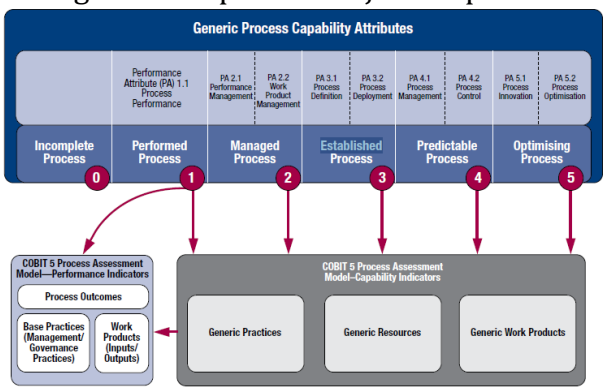
DSS05 berfokus pada pengelolaan layanan keamanan. Proses dari domain DSS05 adalah untuk melindungi informasi perusahaan untuk menjaga tingkat keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan, serta membangun dan memelihara peran keamanan informasi dan hak akses dan pemantauan keamanan [9][10].

2.4. Domain APO13

APO13 berfokus pada pengelolaan keamanan. Proses dari domain APO13 adalah menentukan, mengoperasikan, dan memantau sistem untuk manajemen keamanan informasi [9][10]. Tujuan dari proses domain APO13 adalah menjaga agar dampak dan kejadian dari insiden keamanan informasi masih berada pada level risiko yang dapat diterima perusahaan.

2.5. COBIT 5 *Processes Capability Model*

Processes Capability Model COBIT 5 berdasarkan standar penilaian yang telah diakui secara internasional. Model ini akan membantu dalam mencapai tujuan yang sama secara keseluruhan dari proses penilaian tersebut. *Processes Capability Model* memiliki enam tingkatan seperti ditunjukkan pada Gambar 1.



Gambar 1. *Processes Capability Model* [9]

Dalam *Processes Capability Model*, proses TI harus mencapai atribut yang terkait sesuai dengan indikator masing-masing tingkatan yang bertujuan mengevaluasi kemampuan proses untuk mencapai tujuan [11]. Berikut penjelasan tingkatan yang ada pada *Processes Capability Model* [9]*:*

a. Level 0 – *Incomplete Process*
   Proses ini gagal atau tidak dilaksanakan dalam mencapai tujuan prosesnya. Pada tingkat ini ada sedikit bukti atau tidak ada sama sekali pada pencapaian proses.
b. Level 1 – *Performed Process*
   Proses ini diterapkan untuk mencapai tujuan prosesnya. Terdapat satu atribut pada proses ini, yaitu *process performance.*
c. Level 2 – *Managed Process*
   Proses yang diterapkan berhasil dilaksanakan (direncanakan, dimonitor, dan disesuaikan) dan produk yang tepat ditetapkan, dikontrol dan dipelihara. Terdapat dua atribut pada proses ini, yaitu *performance management* dan *work product.*
d. Level 3 – *Established Process*
   Pada proses yang sebelumnya dikelola dan diterapkan dengan mendefinisikan proses yang mampu mencapai tujuan proses. Terdapat dua atribut pada proses ini, yaitu *process definition* dan *process deployment*.
e. Level 4 – *Predictable Process*
   Proses dioperasikan dengan penetapan batasan untuk mencapai tujuan proses. Terdapat dua atribut pada proses ini, yaitu *process management* dan *process*

control.

f. Level 5 – *Optimising Process*
Proses diprediksi dan terus ditingkatkan untuk memenuhi tujuan bisnis yang relevan. Terdapat dua atribut pada proses ini, yaitu *process innovation* dan *process optimisation*.

Menilai proses mencapai kemampuan pada tingkat 1 dapat dilakukan dengan meninjau hasil dalam deskripsi proses secara rinci dan hasilnya akan diklasifikasikan menjadi empat kategori [12], yaitu:

a. N (*Not achieved*)
Dalam kategori ini tidak ada atau hanya sedikit bukti atas pencapaian atribut proses tersebut. Rentang nilai yang diraih pada kategori ini berkisar 0-15%.
b. P (*Partially achieved*)
Dalam kategori ini terdapat beberapa bukti mengenai pendekatan dan beberapa pencapaian atribut atas proses tersebut. Rentang nilai yang diraih pada kategori ini berkisar 15-50%.
c. L (*Large achieved*)
Dalam kategori ini terdapat bukti atas pendekatan sistematis dan pencapaian signifikan atas proses tersebut, meskipun mungkin masih ada kelemahan yang tidak signifikan. Rentang nilai yang diraih pada kategori ini berkisar 50-85%.
d. F (*Fully achieved*)
Dalam kategori ini terdapat bukti atas pendekatan sistematis dan lengkap dan pencapaian penuh atas atribut proses tersebut. Tidak ada kelemahan terkait atribut proses tersebut. Rentang nilai yang diraih pada kategori ini berkisar 85-100%.

2.6. *Balanced Scorecard*

Balanced scorecard merupakan suatu sistem manajemen yang memperlihatkan sistem manajemen yang menjabarkan visi dan strategi suatu perusahaan kedalam tujuan operasional dan memiliki tolak ukur. *Balanced scorecard* memiliki 4 sudut pandang, diantaranya [8]:

a. Keuangan (*Financial*), yaitu memberikan petunjuk mengenai strategi perusahaan, implementasi dan pelaksanaannya dalam memberikan konstribusi terhadap peningkatan keuntungan perusahaan.
b. Pelanggan (*Customer*), yaitu mengidentifikasi pelanggan dan segmen pasar. Mengidentifikasi pelanggan dibutuhkan beberapa hal yang harus diperhatikan sebagai ukuran yaitu kepuasan pelanggan, akuisisi pelanggan baru, profitabilitas pelanggan dan pangsa pasar sehingga dapat mempengaruhi keputusan pelanggan untuk tetap loyal kepada perusahaan.
c. Internal bisnis *(Internal Business)*, yang memungkinkan unit bisnis untuk :
    1) Memberikan nilai yang akan menarik perhatian dan mempertahankan pelanggan dalam segmen pasar sasaran.
    2) Memenuhi keuntungan finansial yang tinggi dari pemegang saham.
    3) Proses *internal* yang akan berdampak besar kepada pelanggan dan pencapaian tujuan finansial perusahaan.

d. Pembelajaran dan pertumbuhan *(Learning and Growth)* yaitu mengindentifikasi infrastruktur yang harus dibangun dalam menciptakan pertumbuhan dan peningkatan kinerja jangka panjang. Untuk mencapai tujuan aspek keuangan, pelanggan dan proses *internal* bisnis perusahaan.

2.7. Metode Pendekatan Audit

Metode pendekataan yang digunakan adalah *Top-Down*. Hal ini disebabkan karena tingkat keberhasilan atau kegagalan implementasi kebijakan dipengaruhi oleh kerangka berfikir secara umum ke pemetaan yang spesifik. Tahapan metode *Top-Down*, sebagai berikut [13]:

a. Pemilihan kebijakan yang akan dianalisis
b. Identifikasi tujuan dan sasaran yang akan dicapai dalam dokumen kebijakan.
c. Identifikasi instrumen guna mencapai tujuan dan sasaran kebijakan
d. Identifikasi hasil kebijakan berdasarkan persetujuan pihak-pihak yang terkait sesuai SOP.
e. Identifikasi manfaat bagi stakeholder dari hasil kebijakan.
f. Identifikasi resiko dan dampak hasil pemanfaatan kebijakan

3. HASIL DAN PEMBAHASAN

3.1. Pengumpulan Data

Pengumpulan data dikategorikan menjadi dua kategori, yaitu data primer dan data sekunder sesuai dengan kebutuhan datanya. Kebutuhan data primer berasal dari sumber data aslinya, baik dari individu atau institusi. Kebutuhan data primer dapat dipenuhi melalui hasil wawancara atau kuisioner yang dilakukan dengan pihak responden maupun dengan cara observasi langsung di Instansi terkait. Data primer terdiri dari struktur organisasi, profil, renstra, dan kondisi eksisting.

Data sekunder dapat diperoleh dari dokumen-dokumen yang sesuai dengan kajian penelitian. Umumnya data sekunder berasal dari organisasi atau objek dilakukannya penelitian. Dokumen-dokumen data sekunder dapat diperoleh dari bagian Instansi yang terkait dengan domain DSS dan APO. Data sekunder terdiri dari Standar Operasi Prosedur (SOP), visi dan misi, kebijakan yang dimiliki, buku pedoman dari objek penelitian dan hasil penelitian terkait keamanan dan manajemen risiko TI.

3.2. Analisis Data

Pada analisis data menggunakan aktivitas proses penilaian COBIT yang merupakan tahapan dalam proses penilaian kemampuan tingkat aktivitas untuk perusahaan meliputi.

3.3. Pemetaan *Enterprise Goals COBIT 5 – Enterprise Goals* Instansi X

Pada pemetaan *enterprise goals* COBIT 5 dan *enterprise goals* Instansi X dilakukan pemetaan tujuan strategis di Instansi X terhadap *enterprise goals* yang ada pada COBIT 5 *Enabling Process* yang disusun berdasarkan IT *Balance Scorecard* (BSC). *Enterprise goals* COBIT 5 dijelaskan dalam dimensi BSC, yaitu:

a. *Financial*
   1) Nilai bagi *stakeholder* terhadap investasi bisnis
   2) Portofolio produk dan layanan yang kompetitif
   3) Mengelola risiko bisnis (pemeliharaan aset)
   4) Kesesuaian dengan hukum dan regulasi eksternal
   5) Transparansi keuangan
b. *Customer*
   1) Budaya layanan berbasis pelanggan
   2) Kontinuitas dan ketersediaan layanan bisnis
   3) Tanggapan cepat terhadap perubahan lingkungan bisnis
   4) Pengambilan keputusan strategis berdasarkan informasi
   5) Optimisasi biaya pelayanan
c. *Internal Business*
   1) Optimisasi fungsionalitas proses bisnis
   2) Optimisasi biaya proses bisnis
   3) Mengelola program perubahan bisnis
   4) Produktifitas operasional dan staf
   5) Kesesuaian dengan kebijakan internal
d. *Learning & Growth*
   1) Individu yang termotivasi dan berkemampuan
   2) Budaya inovasi produk dan bisnis.

Pemetaan *Enterprise Goals* Instansi X bedasarkan *Enterprise Goals* COBIT 5 dapat dilihat pada Tabel 1.

Tabel 1. Pemetaan *Enterprise Goals* COBIT 5 dengan *Enterprise Goals* Instansi X

	***Enterprise Goals* COBIT 5**	***Enterprise Goals* Instansi X**
FINANCE	EG1 (Nilai bagi *stakeholder* terhadap investasi bisnis)	Penyebaran informasi yang tercipta karena adanya kerjasama dengan pihak pemangku kepentingan.
	EG2 (Portofolio produk dan layanan yang kompetitif)	Penyebaran dan pendistribusian informasi nasional dan daerah.
	EG3 (Risiko bisnis dikelola (pengamanan aset)	Optimalisasi jaringan intranet untuk mendukung fungsi pemerintahan
	EG4 (Kepatuhan terhadap hukum dan peraturan eksternal)	Adanya payung hukum untuk tertib administrasi kearsipan.
CUSTOMER	EG6 (Budaya pelayanan berorientasi pelanggan)	Pembaerdayaan Kelompok Informasi Masyarakat (KIM) untuk mengembangkan di wilayah yang kecil.
	EG7 (Layanan bisnis kontinuitas dan ketersediaan)	Optimalisasi pemanfaatan SIMARDA (Sistem Informasi Manajemen Arsip Daerah), *Website* Arsip, dan SOP pelayanan.

	Enterprise Goals COBIT 5	*Enterprise Goals* Instansi X
	EG9 (Pengambilan keputusan strategis berbasis informasi)	Optimalisasi aplikasi yang mendukung fungsi pemerintahan.
	EG10 (Optimalisasi biaya pelayanan)	Optimalisasi *Community Access Point* (CAP).
INTERNAL BUSINESS	*EG11 (Optimalisasi fungsi proses bisnis)*	Meningkatnya kualitas dan kuantitas pelayanan.
	EG13 (Program perubahan bisnis dikelola)	Meningkatnya kualitas sarana dan prasarana penyebaran informasi.
	EG15 (Kepatuhan terhadap kebijakan internal)	Penerapan Keterbukaan Informasi Publik (KIP)
LEARNING & GROWTH	EG16 (Orang-orang terampil dan termotivasi)	Penyelenggaraaan pemberdayaan SDM pengelola Instansi Daerah X dengan masyarakat seperti TBM, Rumah Pintar, dan sejenisnya.
	EG17 (Budaya inovasi produk dan bisnis)	Penggunaan *Mobile Community Access Point* (MCAP) untuk menyebarka informasi yang tidak dibatasi ruang dan waktu (*borderless*)

3.4. Pemetaan *IT-Related Goals COBIT 5 – Enterprise IT-Related* Instansi X

Pada pemetaan *IT-Related Goals* COBIT 5 dan Instansi X bertujuan untuk mengetahui keterkaitan sasaran dari *IT-Related Goals* Instansi X dengan *IT Related Goals* COBIT 5. *IT-Related Goals* COBIT 5 terbagi atas 17 bagian dan selanjutnya dipetakan ke dalam 4 dimensi BSC. Berikut ini diuraikan IT-Related Goals COBIT 5 dalam dimensi BSC, antara lain:

a. *Financial*
   1) Keselarasan strategi TI dan bisnis
   2) Kesesuaian dan dukungan TI untuk kesesuaian bisnis terhadap hukum dan regulasi eksternal
   3) Komitmen manajemen eksekutif dalam pembuatan keputusan terkait TI
   4) Mengelola risiko bisnis terkait TI
   5) Realisasi manfaat dari investasi TI dan portofolio layanan
   6) Transparansi biaya, keuntungan dan risiko TI
b. *Customer*
   1) Penyampaian layanan TI sejalan dengan kebutuhan bisnis
   2) Penggunaan aplikasi, informasi dan solusi teknologi yang memadai
c. *Internal Business*
   1) Kelincahan TI
   2) Keamanan informasi, proses infrastruktur dan aplikasi
   3) Optimisasi aset TI, sumber daya dan kapabilitas
   4) Pemberdayaan dan dukungan proses bisnis dengan mengintegrasi aplikasi dan teknologi ke dalam proses bisnis

5) Penyampaian program yang memberikan manfaat, tepat waktu, dan sesuai kebutuhan dan standar kualitas
6) Ketersediaan informasi yang dapat dipercaya dan bermanfaat dalam pengambilan keputusan
7) Kesesuaian TI terhadap kebijakan internal

d. *Learning & Growth*
1) Personel TI dan bisnis yang kompeten dan termotivasi
2) Pengetahuan, keahlian dan insiatif dalam inovasi bisnis

Pemetaan *IT-Related Goals* Instansi X bedasarkan *IT-Related Goals* COBIT 5 dapat dilihat pada Tabel 2.

Tabel 2. Pemetaan *IT Related Goals* COBIT 5 dengan *IT Related Goals* Instansi X

	***Enterprise Goals* COBIT 5**	***Enterprise Goals* Instansi X**
FINANCE	ITRG1 (*Alignment of IT and business strategy*)	Sarana dan prasarana disesuaikan sebagai penunjang TI
	ITRG2 (IT *compliance and support for busniess compliance with external laws and regulations*)	Adanya dokumen kebijakan mengenai Informasi dan Teknologi yang sesuai kuantitas.
	ITRG3 (Commitment of executive management for making IT-related decisions)	Kebutuhan aplikasi yang dibuat sesuai besaran.
FINANCE	*ITRG4 (Managed IT-related business risk)*	Total jaringan komunikasi data dan paket pemeliharaan yang optimal.
	ITRG5 (*Realised benefits from ITenabled investments and service portofolio*)	Total pembangunan dan penambahan pemasangan fiber optik
CUSTOMER	ITRG7 (*Delivery of IT services in line with business requirements*)	Total layanan aplikasi diseluruh SKPD yang dapat diakses.
	ITRG8 (*Adequate use of applications,information and technology solutions)*	Total pemanfaatan layanan internet, baik dari invidu maupun kelompok.
INTERNAL BUSIINESS	ITRG9 (*IT agility)*	Total layanan aplikasi diseluruh SKPD yang dapat diakses.
	ITRG11 (*Optimisation of IT assets, resources and capabilities)*	Total jaringan komunikasi data dan paket pemeliharaan yang optimal.
	ITRG12 (*Enablement and support of business processes by integrating applications and technology into business processes*)	Total jaringan komunikasi yang dihubungkan ke masing-masing departemen terkait.
	ITRG13 (*Delivery of programmes delivering benefits, on time, on budget, and meeting requirements and quality standards*)	Website Instansi Daerah X dimanfaatkan untuk memperbarui informasi

	Enterprise Goals COBIT 5	*Enterprise Goals* Instansi X
	ITRG14 (*Availability of reliable and useful information for decision making*)	Sarana dan prasarana disesuaikan sebagai penunjang TI
	ITRG15 (*IT compliance with internal policies)*	Adanya dokumen kebijakan mengenai Informasi dan Teknologi yang sesuai kuantitas.
LEARNING& GROWTH	ITRG16 (*Competent and motivated business and IT personel)*	Total penyelenggaraan pelatihan teknologi dan informasi secara teknis.
	ITRG17 (*Knowledge, expertise and initiatives for business innovation)*	Total penyelenggaraan Diskusi/ Forum/ Seminar Komunikasi Masyarakat Telematika.

3.5. Analisis Data Eksisting dan Hasil *Assesment*

Analisis data eksisting merupakan analisis yang diperoleh dengan cara mengumpulkan data terlebih dahulu yang selanjutnya diolah sesuai dengan kondisi organisasi saat ini. Hasil analisis kondisi saat ini akan dilakukan analisis kondisi *IT Governance* yang ideal di Instansi X. Hasil *capability Level* DSS05 dapat dilihat pada Tabel 3 dan dokumentasi proses DSS05 dapat dilihat pada Tabel 4.

Tabel 3. *Capability Level* DSS05 Pengelolaan Layanan Keamanan

Tujuan	Memastikan bahwa informasi perusahaan terlindungi untuk menjaga tingkat risiko keamanan informasi yang dapat diterima perusahaan sesuai dengan kebijakan keamanan, menetapkan dan memelihara peran keamanan informasi dan akses hak istimewa dan melakukan pemantauan keamanan.

Proses *Ensure Resource Optimization*		**Rating (Persentase)**
Level 0		100 %
Level 1	*Process Attribute 1.1*	69 %
Level 2	*Process Attribute 2.1*	
	Process Attribute 2.2	
Level 3	*Process Attribute 3.1*	
	Process Attribute 3.2	
Level 4	*Process Attribute 4.1*	
	Process Attribute 4.2	
Level 5	*Process Attribute 5.1*	
	Process Attribute 5.2	

Tabel 4. Dokumentasi Proses DSS05

Sub Proses	Deskripsi	Ada/ Tidak ada	Ket.	Skor
DSS05.01 Perlidungan terhadap malware	Adanya dokumen mengenai kebijakan pencegahan perangkat lunak berbahaya	Ada	100%	50%
	Adanya dokumen atau laporan mengenai evaluasi potensi ancaman	Tidak Ada	0%	
DSS05.02 Pengelolan jaringan dan keamanan konektivitas	Adanya dokumen mengenai kebijakan keamanan konektivitas	Ada	100%	100 %
	Adanya dokumen atau laporan mengenai hasil tes penetrasi	Ada	100%	
DSS05.03 Pengelolan keamanan *endpoint*	Adanya dokumen mengenai kebijakan keamanan untuk perangkat *endpoint*	Ada	100%	100 %
DSS05.04 Pengelolaan identitas pengguna dan akses *logical*	Adanya dokumen mengenai hak akses pengguna yang disetujui	Ada	100%	100 %
	Adanya dokumen hasil ulasan akun pengguna	Ada	100%	
DSS05.05 Pengelolaan akses fisik ke aset TI	Adanya dokumen mengenai permintaan akses yang disetujui	Ada	100%	50 %
	Adanya dokumen terkait akses log	Tidak ada	0%	
DSS05.06 Pengelolaan dokumen penting dan perangkat keluaran	Adanya dokumen mengenai inventaris dokumen penting dan perangkat	Tidak Ada	0%	50 %
	Adanya dokumen mengenai hak akses khusus	Ada	100&	
DSS05.07 Memonitor infrastruktur untuk kegiatan yang berhubungan dengan keamanan	Adanya dokumen mengenai keamanan *event logs*	Ada	50%	33 %
	Adanya dokumen mengenai keamanan *incident characteristics*	Tidak Ada	0%	
	Adanya dokumen mengenai keamanan *incident tickets*	Tidak Ada	0%	

Sub Proses	Deskripsi	Ada/ Tidak ada	Ket.	Skor
	Rata-rata			69 %

Proses DSS05 pada tabel 3 menjelaskan bahwa nilai tingkat kapabilitas pengelolaan layanan keamanan berada pada level 1 yaitu tercapai hanya sebagian dengan persentase 69 %. Sedangkan hasil *capability Level* APO13 dapat dilihat pada Tabel 5 dan dokumentasi proses APO13 dapat dilihat pada Tabel 6.

Tabel 5. APO13 Pengelolaan Keamanan

Tujuan	Menentukan, mengoperasikan, dan memantau sistem untuk manajemen keamanan informasi.	
Proses *Ensure Resource Optimization*		Rating (Persentase)
Level 0		100 %
Level 1	*Process Attribute 1.1*	33 %
Level 2	*Process Attribute 2.1*	
	Process Attribute 2.2	
Level 3	*Process Attribute 3.1*	
	Process Attribute 3.2	
Level 4	*Process Attribute 4.1*	
	Process Attribute 4.2	
Level 5	*Process Attribute 5.1*	
	Process Attribute 5.2	

Tabel 6. Dokumentasi Proses APO13

Sub Proses	Deskripsi	Ada/ Tidak ada	Ket.	Skor
APO13.01 menetapkan dan memelihara manajemen keamanan sistem informasi	Adanya dokumen mengenai kebijakan manajemen keamanan sistem informasi	Ada	100%	50%
	Adanya dokumen mengenai *scope statement* manajemen keamanan sistem informasi	Tidak Ada	0%	
APO13.02 Menentukan dan mengelola rencana	Adanya dokumen mengenai rencana penanganan risiko keamanan informasi	Ada	100%	50%

Sub Proses	Deskripsi	Ada/ Tidak ada	Ket.	Skor
perawatan risiko keamanan informasi	Adanya dokumen mengenai *business cases* keamanan informasi	Tidak Ada	0%	
APO13.03 Monitor dan peninjauan manajemen keamanan sistem informasi	Adanya dokumen mengenai laporan audit manajemen keamanan sistem informasi	Tidak Ada	0%	0 %
	Adanya dokumen mengenai rekomendasi untuk meningkatkan manajemen keamanan sistem informasi	Tidak Ada	0%	
Rata-rata				33 %

Dari hasil penilaian tingkat kapabilitas pada proses APO13 yaitu pengelolaan keamanan berada pada level 1 yaitu tercapai sebagian dengan presentase 33%. Dari hasil perhitungan tingkat kapabilitas pada domain DSS05 dan APO13 menghasilkan rangkuman nilai rata-rata tingkat kapabilitas dari masing-masing domain. Adapun rangkuman nilai rata-rata tingkat kapabilitas dijelaskan pada Tabel 7.

Tabel 7. Ringkasan Penilaian Domain DSS05 dan APO13

Domain		Rata-Rata
DSS05	Pengelolaan Layanan Keamanan	69%
APO13	Pengelolaan Keamanan	33%

Berdasarkan proses analisis data eksisting yang dilakukan terhadap proses-proses yang ada, didapatkan hasil *assessment* yang dapat dilihat pada Tabel 8.

Tabel 8. Hasil *Assessment*

Proses	Level	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
DSS05 Pengelolaan Layanan Keamanan	1	L	N	N	N	N	N	N	N	N
APO13	1	P	N	N	N	N	N	N	N	N

Pengelolaan Keamanan

Berdasarkan hasil penilaian dapat diketahui tingkat *capability level* yang dicapai untuk proses DSS05 pengelolaan layanan keamanan hasil pada level *performed process* dengan kategori *lagerly* atribut PA 1.1 sebesar 69% dan dapat disimpulkan bahwa bukti pencapaian terhadap atribut ini memiliki pendekatan yang sistematis walaupun masih terdapat kelemahan. Selanjutnya proses APO13 pengelolaan keamanan didapatkan hasil penilaian dengan tingkat *capability level* pada level *performed process* sebesar 33% pada PA 1.1 yang termasuk dalam kategori *partially* dapat disimpulkan bahwa bukti terhadap pencapaian atribut yang dinilai ada walaupun dengan kondisi yang tidak terduga.

3.6. Target *Capability Level*

DSS05 dan APO13 telah melalui proses penilaian dan masing-masing proses ini berada pada level satu yaitu *perfomed process* yang mengimplemetasikan setiap proses menjadi objek penilaian untuk mencapai tujuan masing-masing proses tersebut. Berdasarkan hasil yang didapat Instansi X menetapkan target *capability level* berada pada level dua dengan menyempurnakan level satu terlebih dahulu agar level dua bisa tercapai.

Instansi X untuk mencapai level dua pada *capability level* perlu terpenuhinya tujuan pada level satu tesebut untuk dapat masuk ke level selanjutnya, yaitu level dua. Target pencapaian pada *capability level* yang ingin dicapai dapat dilihat pada Tabel 9. Instansi X pada level satu perlu mengimplementasikan proses untuk mencapai tujuannya. Pada level dua, proses diimplementasikan dengan baik dan terdapat perencanaan, pengawasan dan penyesuaian terhadap produk kerja yang dihasilkan.

Tabel 9. Target *Capability Level*

Proses	Level	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
DSS05 Pengelolaan Layanan Keamanan	1	F	F	F	N	N	N	N	N	N
APO13 Pengelolaan Keamanan	1	F	F	F	N	N	N	N	N	N

4. SIMPULAN

Kesimpulan dari analisis tata kelola TI di Instansi X yang berfokus pada keamanan teknologi informasi khususnya pada DSS05 adalah perhitungan pencapaian tingkat kapabilitas pada domain DSS05 yaitu pengelolaan layanan keamanan di Instansi X berada pada level 1 dengan rata-rata nilai pencapaian 69%. Instansi X dalam mencapai tingkat kapabilitas pada level dua perlu melakukan perancangan tata kelola keamanan TI yaitu melakukan evaluasi rutin terhadap

potensi ancaman keamanan, memiliki dokumen terkait hak akses pengguna sesuai dengan kebutuhan masing-masing unit, dan memiliki dokumen SOP terkait keamanan teknologi informasi. Sedangkan berdasarkan hasil perhitungan pencapaian tingkat kapabilitas pada domain APO13 yaitu pengelolaan keamanan di Instansi X berada pada level 1 dengan rata-rata nilai pencapaian 33%. Dalam mencapai tingkat kapabilitas pada level dua perlu dilakukan perancangan tata kelola keamanan TI yaitu memliki unit khusus yang menangani hal terkait manajemen keamanan sistem informasi dan setiap aktivitas yang dilakukan terdokmentasi dengan baik.

DAFTAR PUSTAKA

[1] C. Juiz, C. Guerrero, and I. Lera, "Implementing Good Governance Principles for the Public Sector in Information Technology Governance Frameworks," *Open Journal of Accounting*, vol. 3, no. 1, pp. 9–27, 2014, doi: 10.4236/ojacct.2014.31003.

[2] L. Al Omari, P. H. Barnes, and G. Pitman, "Optimising COBIT 5 for IT Governance : Examples from the Public Sector," in *International Conference on Applied and Theoretical Information Systems Research*, 2012, pp. 1–13.

[3] R. Jumardi, "Kajian Kebijakan Keamanan Sistem Informasi Sebagai Bentuk Perlindungan Kerahasiaan Pribadi Karyawan Perusahaan XYZ," *Journal Scientific and Applied Informatics*, vol. 1, no. 1, pp. 13–17, 2018, doi: 10.36085/jsai.v1i1.8.

[4] L. N. Amali, "Tata Kelola TI Yang Efektif di Organisasi Pemerintahan Daerah," in *Seminar Nasional Sistem Informasi Indonesia*, 2013, pp. 37–43.

[5] ISACA, *COBIT 5 Framework*. United States of America: ISACA, 2012.

[6] K. Youssfi, J. Boutahar, and S. Elghazi, "A Tool Design of Cobit Roadmap Implementation," *International Journal of Advanced Computer Science and Applications*, vol. 5, no. 7, pp. 86–94, 2014, doi: 10.14569/ijacsa.2014.050714.

[7] D. A. O. Turang, D. Y. Ratnasari, and I. Y. Pasa, "Audit Teknologi Informasi Bandung Techno Park Menggunakan Framework COBIT 5 Pada Domain EDM (Evaluate, Direct, And Monitor)," *INTEK: Jurnal Informatika dan Teknologi Informasi*, vol. 1, no. 2, pp. 11–19, 2018.

[8] ISACA, *Enabling Processes*. United States of America: ISACA, 2012.

[9] ISACA, *COBIT 5: A business framework for Governance and Management of Enterprise IT*. United States of America: ISACA, 2012.

[10] ISACA, *COBIT 5 for Assurance*. United States of America: ISACA, 2012.

[11] A. Pasquini and E. Galiè, "COBIT 5 and the Process Capability Model. Improvements Provided for IT Governance Process," in *Proceedings of FIKUSZ '13 Symposium for Young Researchers*, 2013, pp. 67–76.

[12] ISO/IEC, *Software Engineering-Process Assessment-Part 2: Performing an Assessment*. Switzerland: ISO, 2003.

[13] ISACA, *COBIT 5 for Risk*. United States of America: ISACA, 2013.