PENERAPAN *FRAMEWORK COBIT* 5 UNTUK AUDIT TATA KELOLA KEAMANAN INFORMASI PADA KANTOR WILAYAH KEMENTERIAN AGAMA PROVINSI LAMPUNG

Dedi Darwis[1)], Nur Yulianti Solehah[1)] , Dartono[2)]

[1]Fakultas Teknik dan Ilmu Komputer, Universitas Teknokrat Indonesia
[2] Sistem Informasi, Institut Teknologi dan Bisnis Swadharma
[1]Jl. ZA Pagar Alam No 9-11 Labuhan Ratu, Bandarlampung
[2] Jl. Pd. Cabe Raya No.36, Pd. Cabe Udik Pamulang, Tangerang Selatan
Email: [1]darwisdedi@teknokrat.ac.id, [2]nuryuliantisolehah@gmail.com

Abstrak

Kementerian Agama Provinsi Lampung merupakan salah satu instansi pemerintahan di bawah naungan Kementerian Agama Republik Indonesia untuk perwakilan pemerintah pusat dalam menangani urusan agama Provinsi Lampung. Audit tata kelola keamanan informasi menggunakan framework COBIT 5 pada Kementerian Agama Provinsi Lampung dilakukan untuk mengetahui sejauh mana Kementerian Agama Provinsi Lampung telah menerapkan tata kelola keamanan informasi dengan baik. Pengumpulan data dilakukan dengan cara wawancara, dokumentasi, tinjauan pustaka, menyebarkan kuesioner, dan pengamatan secara langsung. Hasil pengolahan data kuisioner digunakan untuk mengetahui kinerja TI yang telah berjalan selama ini sehingga membantu dalam memecahkan masalah melalui pengusulan suatu solusi atau rekomendasi yang mengarah pada pencapaian target yang diharapkan. Pengolahan kuisoner menghasilkan nilai rata-rata yaitu 3,3 dari nilai rentang nilai 0 sampai 5 pada domain EDM03 (Memastikan Optimasi Risiko), APO01(Mengelola Kerangka Kerja Manajemen TI), APO07 (Mengelola Sumber Daya Manusia), APO12 (Mengelola Risiko), BAI06 (Mengelola Perubahan), DSS01 (Mengelola Operasi), DSS02 (Mengelola Permintaan Layanan dan Insiden), DSS03 (Mengelola Masalah), DSS05 (Mengelola Layanan Keamanan), MEA01 (Memantau, Melakukan Evaluasi dan Menilai Kinerja dan Kesesuaian), dan MEA02 (Memantau, Melakukan Evaluasi dan Menilai Sistem dari Kendali Internal). Artinya kementerian agama provinsi lampung sudah melakukan proses keamanan data dan informasi dengan baku dan formal akan tetapi belum mencapai titik optimized dalam meningkatkan tata kelola keamanan informasi.

Kata Kunci: *Audit, COBIT 5, Keamanan, Sistem Informasi, Tata Kelola*

1. Pendahuluan

1.1 Latar Belakang Masalah

Kementerian Agama Provinsi Lampung merupakan salah satu instansi pemerintahan di bawah naungan Kemementerian Agama Republik Indonesia untuk perwakilan pemerintah pusat dalam menangani urusan agama Provinsi Lampung. Kementerian Agama Provinsi Lampung memiliki beberapa divisi yaitu Bagian Tata Usaha, Bidang Pendidikan Madrasah, Bidang Pendidikan Agama dan Keagamaan Islam, Bidang Penyelenggaraan Haji dan Umrah, Bidang Urusan Agama Islam dan Pembinaan Syariah, Bidang Penerangan Agama Islam, Zakat, dan Wakaf, Pembimbing Masyarakat Kristen, Pembimbing Masyarakat Katolik, Pembimbing Masyarakat Hindu, Pembimbing Masyarakat Budha. Kementerian Agama Provinsi Lampung merupakan salah satu instansi pemerintahan yang menggunakan teknologi informasi (TI) dengan menerapkan sistem EMIS. Saatini, teknologi informasi tidak hanya digunakan sebagai faktor pendukung dalam perusahaan, tetapi juga sebagai bagian dari strategi bisnis perusahaan. Agar teknologi informasi dapat digunakan secara optimal, diperlukan suatu tata kelola yang biasa disebut tata kelola teknologi informasi [1], [2]. Tata kelola teknologi informasi adalah bagian dari tata kelola perusahaan yang menitik beratkan pada sistem dan teknologi informasi serta manajemen kinerja dan risikonya.

Salah satustandar yang digunakan dalam tata kelola teknologi informasi adalah *COBIT (Control Objectives for information and Related Technology)*. Standar *COBIT* mengukur kinerja tata kelola teknologi informasi yang sesuai dengan tujuan bisnis perusahaan. Layanan teknologi informasi yang tepat waktu, akurat dan relevan dengan kebutuhan user merupakan hal yang sangat penting diperhatikan dalam mendukung kelancaran pelaksanaan aktivitas suatu organisasi termasuk institusi pendidikan, tujuan institusi pendidikan akan tercapai jika perencanaan dan strategi bisnis organisasi, penerapan teknologi informasi yang selaras dengan

tujuan kementerian agama hanya dapat dihasilkan apabila didukung dengan tujuan institusi tersebut. Tujuan dapat dihasilkan apabila didukung dengan sistem tata kelola teknologi informasi yang baik sejak tahap perencanaan, implementasi, dan evaluasi [3], [4]. Framework *COBIT* memiliki dua versi yaitu *COBIT* 4.1 dan *COBIT* 5.

Kementerian Agama Provinsi Lampung dalam pasal 5 memiliki beberapa fungsi salah satunya yaitu perumusan kebijakan teknis di bidang pengelolaan administrasi dan informasi. Berdasarkan fungsi tersebut sebagai perumusan kebijakan teknis dan informasi, kementerian agama menerapkan sistem EMIS, yang digunakan untuk pengelolaan seluruh data pendidikan se-provinsi lampung. Saat ini kegiatan tata kelola keamanan informasi belum dilakukan. Untuk mengantisipasi terjadinya kendala seperti sumber daya manusia yang kurang memahami penerapan teknologi informasi sehingga sering terjadinya eror pada aplikasi, kemudian pengaksesan data oleh orang yang tidak memiliki hak akses dapat melakukan tindakan negative seperti penyalahgunaan data, maka dari itu di perlukan adanya audit tata kelola keamanan informasi untuk peningkatan keamanan informasi pada Kementerian Agama Provinsi Lampung. Keamanan informasi akan meningkatkan kualitas, integritas pemerintahan serta meningkatkan investasi dalam pengelolaan dan pengembangan sistem informasi yang akan terus meningkat di masa mendatang [5], [6].

Salah satu metode pengelolaan teknologi informasi menggunakan kerangkakerja *COBIT* yang pertama kali diterbitkan pada april 1966, adalah *framework* pertama yang diakui secara internasional untuk bidang *ITGI (IT Governance)* yang bekerjasama dengan ahli dari berbagai bidang seperti industri, akademisi, pemerintah, dan IT *Security and Control* [7], [8]. *COBIT* berfungsi untuk mempertemukan semua kebutuhan control dan isu-isu teknik, selain itu *COBIT* juga dirancang menjadi alat bantu untuk memecahkan permasalahan pada IT *Governance* dalam memahami dan mengelola resiko serta keuntungan yang berhubungan dengan sumber daya informasi. *COBIT* 5 menyediakan kerangka kerja yang komprehensif sertadasar yang kuat untuk kemanan informasi yang membantu perusahaan untuk mencapai tujuan dan memberikan nilai melalui tata kelola dan manajemen perusahaan IT yang efektif [9].

Untuk mencapai tujuan dan memberikan nilai tata kelola dan manajemenp erusahaan TI yang efektif diperlukan standarisasi tata kelola keamanan informasi dengan menggunakan *framework COBIT* 5. Salah satu metode pengelolaan teknologi informasi yang digunakan secara luas adalah *IT Governance* yang terdapat pada *COBIT* [10]. Tata kelola teknologi informasi adalah bagian dari tata kelola perusahaan yang menitik beratkan pada sistem dan teknologi informasi serta manajemen kinerja dan risikonya. Kerangka *COBIT* 5 merupakan sebuah kerangka yang dapat membantu organisasi atau perusahaan dalam Tata Pengelolaan dan Manajemen TI [11].

Kerangka *COBIT* 5 membagi proses teknologi informasi menjadi 5 domain, yaitu EDM *(Evaluate, Direct and Monitor)*, APO *(Align, Plan and Organise)*, BAI(*Build, Acquire and Implement*), DSS (*Deliver, Service, and Support*), MEA (*Monitor, Evaluate and Assess*) dengan keseluruhan 37 proses yang ada didalamnya [9]. *COBIT* 5 dipilih karena memilik icakupan yang luas untuk proses pengelolaan teknologi informasi, kedetilan proses dan aktivitasnya. Audit tata kelola keamanan infromasi menggunakan *framework COBIT* 5 akan memberikan informasi kepada kementerian agama mengenai hasil analisis yang akan digunakan untuk melakukan peningkatan terhadap sistem EMIS *(Education Mangement Information System).*

1.2 Landasan Teori

A. Audit

"Audit pada dasarnya adalah proses sistematis dan obyektif dalam memperoleh dan mengevaluasi bukti-bukti tindakan ekonomi, guna memberikan asersi / pernyataan dan mmenilai seberapa jauh tindakan ekonomi sudah sesuai dengan kriteria yang berlaku dan mengkomunikasikan hasilnya kepada pihak terkait" [12].

B. Jenis-Jenis Audit

Berikut ini merupakan jenis-jenis audit [12] :

1) Financial Audit, memeriksa keterdalaman dan integritas dari transaksi-transaksi keuangan, catatan akuntansi dan laporan keuangan.
2) Internal Kontrol Audit, memeriksa kebijakan prosedur pengendalian internal serta efektifitas dalam pengamanan asset, audit tersebut biasanya mengevaluasi input dan output sistem, pengendalian pemrosesan, rencana *backup* dan pemulihan keamanan sistem serta fasilitas sistem.
3) Operational Audit, berkaitan dengan penggunaan secara ekonomis dan efisien atas sumber daya pencapaian tujuan serta sasaran yang diterapkan.
4) *Compiance* Audit, menentukan apakah entitas mematuhi hokum, peraturan, kebijakan, dan prosedur yang berlaku. Audit ini sering menghasilkan rekomendasi untuk meningkatkan proses dan pengendalian yang digunakan untuk memastikan kepatuhan terhadap regulasi.
5) *Investigative* Audit, menguji kejadian-kejadian dari penipuan yang mungkin terjadi, penggunaan asset yang tidak tepat, pemborosan dan penyalahgunaan atau aktivitas tata kelola yang buruk.

C. Tata Kelola Teknologi Informasi

"Tata kelola TI sebagai tanggungjawab eksekutif dan dewan direksi, sebagai bagian dari tata kelola bisnis terdiri atas kepemimpinan, struktur dan

proses-proses organisasi, yang akan memastikan bahwa TI organisasi tersebut bisa mendukung dan menyampaikan tujuan strategis organisasi" [12].

Pentingnya Tata Kelola Teknologi yaitu :

1) Adanya perubahan peran TI, dari peran efisiensi ke peran strategic yang harus ditangani level korporat.
2) Banyak proyek TI *strategic* yang penting namun gagal dalam pelaksanaanya karena hanya ditangani oleh teknisi TI.
3) Keputusan TI di dewan direksi sering bersifat ad hoc atau tidak terencana dengan baik.
4) TI merupakan pendorong utama proses transformasi bisnis yang member imbas penting bagi organisasi dalam pencapaian misi, visi, dan tujuan strategic.

D. Keamanan Informasi

"Aset informasi : *hardware, software*, sistem, informasi dan manusia, merupakan asset yang penting bagi suatu organisasi yang perlu dilindungi dari risiko keamanannya baik dari pihak luar dan dalam organisasi. Keamanan informasi tidak bisa hanya disandarkan pada alat / *tools* atau teknologi keamanan informasi, melainkan perlu adanya pemahaman dari organisasi tentang apa yang harus dilindungi dan menetukan secara tepat solusi yang dapat menangani permasalahan kebutuhan keamanan informasi" [13].

"Keamanan Informasi terdiri dari 3 prinsip yaitu Confidentiality, Integrity dan Availability. Pada awalnya prinsip keamanan informasi hanya CIA, seiring pertambahan waktu prinsip keamanan informasi diperlukan menjadi CIA+ [12].

1. *Confidentiality* (Kerahasiaan)
2. *Integrity* (Integritas)
3. *Availability* (Ketersediaan)
4. *Privacy* (Privasi)
5. *Identification* (Identifikasi)
6. *Authentification* (Otentifikasi)
7. *Authorization* (Otorisasi)
8. *Accountability* (Akuntabiliti)

2. Metode Penelitian

2.1 *Domain COBIT 5*

Penelitian ini berfokus pada Domain EDM (*Evaluate, Direct and Monitor*), APO (*Align, Plan and Organise*), BAI (*Build, Acquire and Implement*), DSS (*Deliver, Service, and Support*), MEA (*Monitor, Evaluate and Assess*) dengan jumlah 11 proses yang ada di dalamnya.

A. EDM (Evaluate, Direct and Monitor) Mengevaluasi, Mengarahkan dan Memantau.

Proses tata kelola ini berkaitan dengan tujuan tata kelola pemangku kepentingan dalam melakukan penilaian, optimasi risiko dan sumber daya, mencakup praktek dan kegiatan yang bertujuan untuk mengevaluasi pilihan strategis, memberikan arahan kepada TI dan pemantasan hasilnya [12]. *Evaluate, Direct* and Monitor (EDM) terdapat 5 *hight level control objectives*, yaitu :

1) EDM01:Memastikan Penetapan Kerangka Kerja Tata Kelola dan Pemeliharaan
2) EDM02 :Memastikan Pnyampaian Keuntungan
3) EDM03 : Memastikan Optimasi Risiko
4) EDM04 :Memastikan Optimasi Sumber Daya
5) EDM05 : Memastikan Transparasi Pemangku Kepentingan

B. APO (Align, Plan and Organise) Menyelaraskan, Rencana dan Mengorganisir.

Memberikan arah untuk pengiriman solusi (BAI) dan penyediaan layanan dan dukungan (DSS). Domain ini mencakup strategi dan taktik, serta mengidentifikasi kekhawatiran cara terbaik TI agar dapat berkontribusipada penncapaian tujuan bisnis. Realisasi visi strategis perlu direncanakan, dikomunikasikan dan dikelolauntuk perpektif yang berbeda. Sebuah organisasi yang tepat, serta infrastruktur teknologi, harus dimasukkan kedalam tempatnya [12]. *Align, Plan and Organise* (APO) terdapat 13 *hight level control objectives*, yaitu :

1) APO01 : Mengelola Kerangka Kerja Manajemen TI
2) APO02 : Mengelola Strategi
3) APO03 : Mengelola Arsitektur Perusahaan
4) APO04: Mengelola Inovasi
5) APO05: Mengelola Portofolio
6) APO06: Mengelola Anggaran dan Biaya
7) APO07: Mengelola Sumber Daya Manusia
8) APO08: Mengelola Hubungan
9) APO09: Mengelola Perjanjian Layanan
10) APO10: Mengelola Penyedia
11) APO11: Mengelola Kualitas
12) APO12: Mengelola Risiko
13) APO13: Mengelola Pelayanan

C. BAI(Built, Acquire and Implement)

Memberikan solusi dan melewatinya sehingga akan berubah menjadi layanan. Untuk mewujudkan strategi TI, solusi TI perlu diidentifikasi, dikembangkan atau diperoleh, serta diimplementasikan dan terintegrasi ke dalam proses bisnis. Perubahan dan pemeliharaan sistem yang ada juga dicakup oleh domain ini, untuk memastikan bahwa solusi terus memenuhi tujuan bisnis [12]. *Built, Acquire and Implement* (BAI) terdapat 10 *hight level control objectives*, yaitu :

1) BAI01 : Mengelola Program dan Proyek
2) BAI02 : Mengelola Penetapan Persyaratan
3) BAI03 : Mengelola Identifikasi Solusi dan Membangun
4) BAI04 : Mengelola Ketersediaan dan Kapasitas
5) BAI05 : Mengelola Pemberdayaan Perubahan Organisasi

6) BAI06 : Mengelola Perubahan
7) BAI07 : Mengelola Penerimaan terhadap Perubahan dan Masa Transisi
8) BAI08 : Mengelola Pengetahuan
9) BAI09 : Mengelola Aset
10) BAI10 : Mengelola Konfigurasi

D. *DSS* (*Deliver, Service, and Support*)

Meliputi layanan, dan dukungan atau member pelayanan yang aktual bagi bisnis, termasuk manajemen data dan proteksi informasi yang berhubungan dengan proses bisnis [12]. *Deliver, Service, and Support* (DSS) terdapat 5 hight level control objectives, yaitu :

1) DSS01: Mengelola Operasi
2) DSS02: Mengelola Permintaan Layanan dan Insiden
3) DSS03: Mengelola Masalah
4) DSS04: Mengelola Kelangsungan
5) DSS05: Mengelola Kendali Proses Bisnis

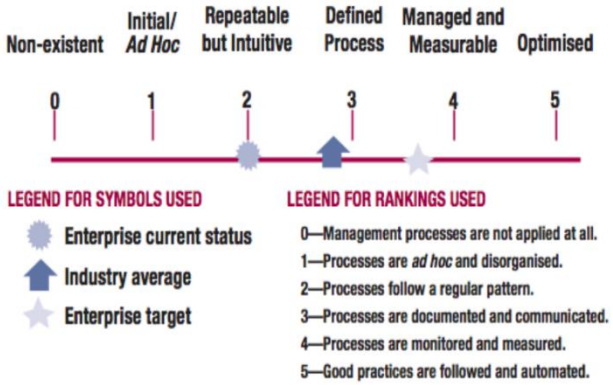
E. MEA (Monitor, Evaluate and Assess)

Menerima solusi dan dapat digunakan bagi pengguna akhir. Domain ini berkaitan dengan pengiriman actual dan dukungn layanan yang dibutuhkn, yang meliputi pelayanan, pengelolaan keamanan dan kelangsungan, dukungan layanan bagi pengguna, dan manajemen data serta fasilitas operasional [12]. *Monitor, Evaluate and Assess* (MEA) terdapat 3 *hight level control objectives*, yaitu :

1) MEA01:Memantau, Melakukan Evaluasi, Menilai Kinerja, dan Kesesuaian
2) MEA02 : Memantau, Melakukan Evaluasi dan Menilai Sistem dari Kendali Internal
3) MEA03:Memantau, Melakukan Evaluasi dan Menilai Kepatuhan dengan Persyaratan Internal

2.2 *Maturity Level*

Salah satu alat pengukur dari kinerja suati sistem teknologi informasi adalah model kematangan (*maturity level*), model kematangan digunakan untuk mengontrol proses-proses teknologi informasi menggunakan framework *COBIT* dengan informasi menggunakan metode penilaian / scoring tujuannya adalah organisasi dapat mengetahui posisi kematangan teknologi informasi saat ini dan organisasi dapat terus menurut dan bekesinambungan berusaha meningkatkan levelnya sampai tingkat tertinggi agar aspek governance terhadap teknologi informasi dapat berjalan dengan lancar. Tingkat kemampuan pengelola TI pada skala *Maturity level* dibagi menjadi 6 level seperti pada Gambar 1.



Gambar 1. *Maturity Level*[12]

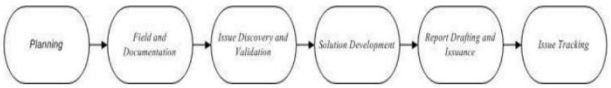
Keterangan masing-masing level sebagai berikut:

1. Level 0 *(Non existent)*
   Pada level ini, perusahaan sama sekali tidak perduli terhadap pentingnya teknologi informasi untuk dikelola secara baik oleh manajemen.
2. Level 1 (*Initial*)
   Pada level ini, perusahaan secara aktif melakukan penerapan dan implementasi teknologi informasi sesuai dengan kebutuhan-kebutuhan mendadak yang ada, tanpa didahului dengan perencanaan sebelum nya.
3. Level 2 (*Repeatable)*
   Pada level ini, perusahaan telah memiliki pola yang berulangkali dilakukan dalam manajemen aktivitas terkait dengan tata kelola teknologi, namun keberadaannya belum terdefinisi secara baik dan formal sehingga masih terjadi ketidak konsistenan.
4. Level 3 (*Defined Process*)
   Pada level ini, perusahaan telah memiliki prosedur baku formal dan tertulis yang telah di sosialisasikan ke segenap jajaran dan karyawan untuk dipatuhi dan dikerjakan dalam aktivitas sehari-hari.
5. Level 4 (*Manage and Measurable)*
   Pada level ini, perusahaan telah memiliki sejumlah indikator atau ukuran kuantitatif yang dijadikan sebagai sasaran maupun obyektif kinerja setiap penerapan aplikasi teknologi informasi yang ada.
6. Level 5 (*Optimised)*
   Pada level yang terakhir, perusahaan telah mengimplementasikan tata kelola teknologi informasi yang mengacu pada "*best practice*".
   Tabel 1 merupakan *Maturity Level* tata kelola keamanan informasi pada perusahaan.

Tabel 1. *Maturity Level*

Indek Kematangan	Level Kematangan
0 - 0.49	*0 - Non-Existent*
0.50 - 1.49	*1- Initial/Ad Hoc*
1.50 - 2.49	*2 - Repeatable But Intutitive*
2.50 - 3.49	*3 - Defined Process*
3.50 - 4.49	*4 - Manage And Measurable*
4.50-5.0	*5- Optimized*

2.3 *Tahapan Penelitian*



Gambar 2. Tahapan Penelitian [12]

1) Perencanaan Audit
   Tujuan dari proses perencanaan adalah menetukan tujuan dan ruang lingkup audit dan menentukan apa yang akan dicapai dari hasil pengauditan. Perencanaan yang dilakukan penulis yaitu akan dilakukannya evaluasi terhadap sistem EMIS dengan menggunakan *framework COBIT* 5 berdasarkan 5 Domain 37 proses, kemudian dari domain dan proses tersebut di pilih kembali oleh peneliti yang akan digunakan untuk penelitian dengan menyesuaikankondisi lapangan pada kementerian agama provinsi lampung.
2) Dokumentasi dan Peninjauan Lapangan (*Filedwork and Documentation)*
   Dokumentasi merupakan bagian penting dari sebuah penelitian audit. Pada tahap ini penulis mendokumentasikan setiap pekerjaan penulis seperti Data wawancara, Data Pendidikan, Data Pengamatan, Data Kuisioner, dan Data Tinjauan Pustaka.
3) Penemuan Masalah dan Validasi (*Issue Discovery and Validation)*
   Pada Tahap ini penulis menemukan permasalahan berdasarkan hasil wawancara, pengamatan yang ditinjau secara langsung di kementerian agama provinsi lampung. Permasalahan yang terjadi yaitu sering terjadinya eror pada aplikasi EMIS, kemudian oleh pihak yang tidak bertanggungjawab dapat melakukan tindakan negatif seperti manipulasi dan kehilangan data, maka dari itu diperlukan adanya audit tata kelola keamanan informasi untuk peningkatan keamanan informasi pada Kementerian Agama Provinsi Lampung.
4) Pengembangan Solusi (*Solution Development*)
   Setelah penulis melakukan identifikasi masalah dan telah divalidasi fakta dan risikonya, penulis dapat bekerja sama dengan pengguna sistem untuk mengembangkan rencana selanjutnya untuk mengatasi permasalahan yang ada dengan menerapkan temuan-temuan dan rekomendasi yang dihasilkan dari penyebaran kuisioner yang berkaitan dengan teknologi informasi pada kementerian agama provinsi lampung.
5) Penyusunan dan Pembuatan Laporan (*Report Drafting and Issuance)*
   Penting bagi penulis untuk membuat laporan agar menghindari kesalah pahaman.Meringkas masalah secara rinci, sehingga seseorang dapat membaca dan memahami dengan mudah mengenai kondisi keseluruhan hasil audit. Laporan harus mencerminkan informasi relevan mengenai audit.
6) Pemantauan Masalah (*Issue Tracking*)
   Penulis mengembangkan proses audit dimasa yang akan datang serta dapat dilacak dan diikuti oleh peneliti setelahnya. Hal ini dapat dilakukan dengan cara menjaga database yang berisi semua poin audit. Penulis melakukan kontak secara teratur dengan pengguna sistem dan memastikan permasalahan dapat terselesaikan sesuai dengan rekomendasi dari hasil pengauditan.

3. Hasil dan Pembahasan

3.1 *Identifikasi Enterprise Goals*

Pada tahap ini penulis mengelompokkan enterprise goals dari Kementerian Agama Provinsi Lampung, dengan enterprise goals yang ada pada *COBIT* 5 dengan cara melihat tujuan penelitian yaitu meningkatkan keamanan data dan informasi maka penulis mengkategorikan tujuan tersebut kedalam tujuan perusahaan (enterprise goals) yang terdapat pada *COBIT* 5 pada bagian Managed Bussiness *Risk* (*Safeguarding of Assets*). Enterprise goals dari Kementerian Agama Provinsi Lampung termasuk dalam kategori *Managed Business Risk (Safeguarding of Assets*) karena Kementerian Agama Provinsi Lampung mengharapkan peningkatan keamanan data dan informasi EMIS.

3.2 *Identifikasi IT Related Goals*

Related Goals, berdasarkan perbandingan matrik dari *enterprise goals*. Ada tiga *IT Related Goals* yang memiliki hubungan yang bersifat "Primer" dengan *Managed Business Risk (Safeguarding of Assets*) yaitu *Manage IT-related business risk, Security of information, processing infrastructure and applications, Enablement and support of business process by integrating applications and technology into business process.*

3.3 *Identifikasi Domain COBIT 5*

Pada Tabel merupakan pembagian dan identifikasi IT Domain dan IT Proses.

Tabel 2. Identifikasi Domain *COBIT* 5

IT Domain	**IT *Process***
Evaluate, Direct and Monitor	*EDM01*
Align, Plan and Organise	APO01, APO10, APO12, APO04, APO07
Build, Acquire and Implement	BAI11, BAI06
Deliver, Service, and Support	DSS01, DSS02, DSS03, DSS04, DSS05, DSS06
Monitor, Evaluate and Assess	*MEA01, MEA0,* MEA03

3.4 *Identifikasi Proses COBIT 5*

Tabel 3. Identifikasi Proses *COBIT* 5

Domain	***Descript (Evaluate, Direct and Monitor)***
EDM03	Memastikan Optimasi Risiko
Domain	**APO*(Align, Plan and Organise)***
APO01	Mengelola Kerangka Kerja Manajemen TI
APO07	Mengelola Sumber Daya Manusia
APO12	Mengelola Risiko
Domain	**BAI (*Build, Acquire and Implement*)**
BAI06	Mengelola Perubahan
Domain	**DSS (*Deliver, Service, and Support*)**
DSS01	Mengelola Operasi
DSS02	Mengelola Permintaan Layanan dan Insiden
DSS03	Mengelola Masalah
DSS05	Mengelola Layanan Keamanan
Domain	**MEA (*Monitor, Evaluate and Assess*)**
MEA01	Memantau, Melakukan Evaluasi dan Menilai Kinerja dan Kesesuaian
MEA02	Memantau, Melakukan Evaluasi dan Menilai Sistem dari Kendali Internal

3.5 *Perhitungan Tingkat Kematangan (Maturity Level)*

Pada perhitungan tingkat kematangan (*maturity level),* menjelaskan hasil perhitungan pada setiap proses untuk mengetahui kesenjangan (gap) yang ada. Dengan pencapaian target tingkat kematangan yang telah disesuaikan dengan kebutuhan sistem pada Kementerian Agama Provinsi Lampung sebesar 3,4 yaitu pada level *Defined Process* yang berarti kementerian agama provinsi lampung sudah melakukan proses keamanan data dan informasi dengan baku dan formal akan tetapi belum mencapai titik *optimized* dalam meningkatkan tata kelola keamanan informasi.

Rata-rata hasil perhitungan dari domain dijabarkan pada Tabel 4.

Tabel 4. Rata-rata Tingkat Kematangan

Proses	Keterangan	Nilai	Kondisi
EDM03	Memastikan Optimasi Resiko	3,4	*Defined Process*
APO01	Mengelola Kerangka Manajemen TI	3,5	*Managed and Measureabel*
APO07	Mengelola Sumber Daya Manusia	3,4	*Defined Process*
APO12	Mengelola Risiko	3,3	*Defined Process*
BAI06	Mengelola Perubahan	3,1	*Defined Process*
DSS01	Mengelola Operasi	3,3	*Defined Process*
DSS02	Mengelola Permintaan Layanan dan Insiden	3,3	*Defined Process*
DSS03	Mengelola Masalah	3,5	*Managed and Measureabel*
DSS05	Mengelola Layanan Keamanan	3,4	*Defined Process*
MEA01	Memonitor, Mengevaluasi, Menilai Kinerja dan Kesesuaian	3,6	*Managed and Measureabel*
MEA02	Memonitor, Mengevaluasi, Menilai sistem dari kendali internal	3,2	*Defined Process*
Nilai Rata-rata		3,4	*Defined Process*

Berdasarkan Tabel 4 pada hasil perhitungan nilai kematangan Domain EDM, APO, BAI, DSS, dan MEA, dapat dijabarkan bahwa rata-rata dari proses EDM03, APO01, APO07, APO2, BAO06, DSS01, DSS02, DSS03, DSS05, MEA01, dan MEA02 menghasilkan nilai tingkat kematangan 3,4. Dari nilai kematangan ini dapat disimpulkan bahwa pengelolaan teknologi informasi pada Kementerian Agama Provinsi Lampung berada pada level Defined Process artinya organisasi telah menggunakan teknologi informasi berdasarkan prosedur baku dan formal yang sudah ditetapkan akan tetapi belum secara keseluruhan dan maksimal, karena sisi pengamanan hanya dilakukan pada pengamanan fisik ataupun pemasangan anti virus.

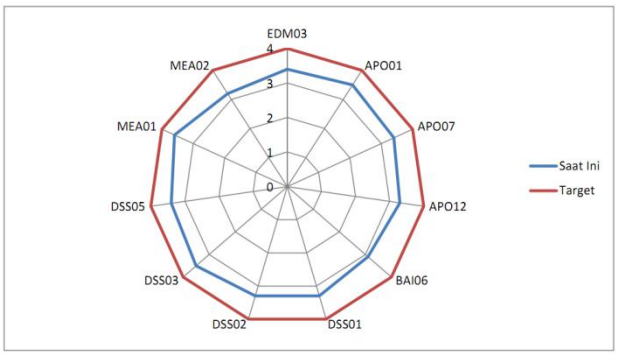
Maka dari itu belum sesuai dengan standar *COBIT*

5 yang seharusnya diterapkan untuk pengamanan asset data dan informasi pada Kementerian Agama Provinsi Lampung. Tabel 5 berikut ini menunjukkan Gap antara tingkat kematangan saat ini dengan tingkat kematangan yang diharapkan :

Tabel 5. Analisis Gab

Proses	Tingkat Kematangan		
	Saat ini	Diharapkan	Gap
EDM03	3,4	4	0,6
APO01	3,5	4	0,5
APO07	3,4	4	0,6
APO12	3,3	4	0,7
BAI06	3,1	4	0,9
DSS01	3,3	4	0,7
DSS02	3,3	4	0,7
DSS03	3,5	4	0,5
DSS05	3,4	4	0,6
MEA01	3,6	4	0,4
MEA02	3,2	4	0,8
Nilai Rata-rata			0,6

Terdapat kesenjangan yaitu 0,6 pada proses domain EDM03, APO01, APO07, APO12, BAI06, DSS01, DSS02, DSS03, DSS05, MEA01, dan MEA02 antara nilai kematangan saat ini dengan nilai tingkat kematangan yang diharapkan. Meskipun GAP terbilang cukup kecil akan tetapi dibutuhkan penyesuaian masing-masing proses karena 0,6 merupakan nilai rata-rata per-proses, makan penulis akan memberikan rekomendasi pada masing-masing proses sehingga perbaikan dapat dilakukan secara menyeluruh peningkatan keamanan data dan informasi pada kementerian agama provinsi lampung. Perbedaan kondisi kesenjangan proses domain EDM, APO, BAI, DSS, dan MEA tata kelola saat ini dengan tata kelola yang diharapkan dapat dilihat pada Gambar 3.



Gambar 3. Kesenjangan Setiap Proses Domain

4. Kesimpulan

Berdasarkan hasil penyebaran kuesioner didapatkan nilai rata-rata yaitu 3,3 dari nilai rentang nilai 0 sampai 5 pada domain EDM03, APO01, APO07, APO12, BAI06, DSS012, DSS02, DSS03, DSS05, MEA01, dan MEA02. Artinya kementerian agama provinsi lampung sudah melakukan proses keamanan data dan informasi dengan baku dan formal akan tetapi belum mencapai titik optimized dalam meningkatkan tata kelola keamanan informasi. Hasil evaluasi menemukan variasi antara kedelapan proses domain yang digunakan untuk menganalisis tata kelola keamanan informasi, diamana pada proses EDM03, APO01, APO07, APO12, BAI06, DSS01, DSS02, DSS05, dan MEA02 dikategorikan kedalam Defined Process kemudian untuk proses domain APO01, DSS03, dan MEA01 dikategorikan kedalam *Managed and Measureabel.*

Daftar Pustaka

[1] U. P. Hakim and D. Darwis, "Audit Tata Kelola Teknologi Informasi (EMIS) Menggunakan Framework *COBIT* 5 PT TDM Bandarlampung," *J. Teknoinfo*, vol. 10, no. 1, p. 14, 2016, doi: 10.33365/jti.v10i1.21.

[2] D. Darwis and . Yuniarwati, "Audit Tata Kelola Teknologi Informasi Menggunakan Framework *COBIT* 4.1 sebagai Upaya Peningkatan Keamanan Data pada Dinas Pendidikan dan Kebudayaan Kabupaten Pesawaran," *Explor. J. Sist. Inf. dan Telemat.*, vol. 7, no. 1, 2016, doi: 10.36448/jsit.v7i1.770.

[3] R. Nugroho, R. R. Suryono, and D. Darwis, "Audit Tata Kelola Teknologi Informasi Untuk Integritas Data Menggunakan Framework *COBIT* 5 Pada PT Kereta Api Indonesia (Persero) Divre IV TNK," *J. Teknoinfo*, vol. 10, no. 1, p. 20, 2016, doi: 10.33365/jti.v10i1.22.

[4] Y. Fernando, R. Biilmilah, and D. Darwis, "Audit Kinerja Sistem Informasi Penelusuran Perkara Pada Pengadilan Agama Tanjung Karang Kelas I a Bandar Lampung," *J. Tekno Kompak*, vol. 11, no. 1, p. 18, 2017, doi: 10.33365/jtk.v11i1.178.

[5] R. R. Suryono, D. Darwis, and S. I. Gunawan, "Audit Tata Kelola Teknologi Informasi Menggunakan Framework *COBIT* 5 (Studi Kasus: Balai Besar Perikanan Budidaya Laut Lampung)," *J. Teknoinfo*, vol. 12, no. 1, p. 16, 2018, doi: 10.33365/jti.v12i1.38.

[6] D. Darwis, F. D. Apriyanti, and E. R. Susanto, "Perancangan Sistem Informasi Akuntansi Pengeluaran Operasional Perusahaan (Study Kasus: Pt Sari Segar Husada)," *J. TEKNOKOMPAK*, vol. 13, no. 1, pp. 1–6, 2019, [Online]. Available: http://ejurnal.teknokrat.ac.id/index.php/teknokompak/article/download/192/168.

[7] D. Darwis and D. M. Pauristina, "AUDIT SISTEM INFORMASI MENGGUNAKAN FRAMEWORK *COBIT* 4.1 SEBAGAI UPAYA EVALUASI PENGOLAHAN DATA PADA SMKK BPK PENABUR BANDAR LAMPUNG," *J. Ilm. Infrastruktur Teknol. Inf.*, vol. 1, no. 1, pp. 1–6, 2020.

[8] K. Sofa, T. L. M. Suryanto, and R. R. Suryono, "Audit Tata Kelola Teknologi Informasi Menggunakan Kerangka Kerja *COBIT* 5 Pada Dinas Pekerjaan Umum Kabupaten Tanggamus," *J. Teknol. dan Sist. Inf.*, vol. 1, no. 1, pp. 39–46, 2020, [Online]. Available: http://jim.teknokrat.ac.id/index.php/sisteminformasi/article/view/50.

[9] H. Sulistiani and Prita Dellia, "Evaluasi Kelayakan Investasi Teknologi Informasi Menggunakan Metode Cost Benefit Analysis," in *Konferensi Nasional Sistem Informasi*, 2018, pp. 11–13, doi: 10.31227/osf.io/4e9r2.

[10] H. Sulistiani and D. Darwis, "Penerapan Metode Agile untuk Pengembangan Online Analytical Processing (OLAP) pada Data Penjualan (Studi Kasus : CV Adilia Lestari)," *J. CoreIT*, vol. 6, no. 1, pp. 50–56, 2020.

[11] Miswanto, H. Sulistiani, and Damayanti, "PENERAPAN METODE COST AND BENEFIT ANALYSIS DALAM PENGUKURAN INVESTASI TEKNOLOGI INFORMASI (STUDY KASUS : CV LAUT SELATAN JAYA) The Application of Cost and Benefit Analysis Methods in Measuring Information Technology Investment (Case Study : CV Laut Sel," *J. Tekno Kompak*, vol. 14, no. 1, pp. 54–61, 2020.

[12] ISACA, *Kerangka COBIT 5, COBIT 4.1, BMI (Modeling Bussiness Information), Manajemen Tata Kelola, Jaminan Framework, Kerangka IT Risk*. 2012.

[13] D. Darwis, A. Junaidi, and Wamiliana, "A New Approach of Steganography Using Center Sequential Technique," *J. Phys. Conf. Ser.*, vol. 1338, no. 1, 2019, doi: 10.1088/1742-6596/1338/1/012063.