CAPABILITY MATURITY MODEL INTEGRATION (CMMI) UNTUK ANALISIS KEAMANAN INFORMASI MENGGUNAKAN DOMAIN APO13 COBIT 5 PADA PUSTIPAD INSTANSI X

Hariani[1)], Darmatasia[2)] , Wahyuddin Saputra[3)]

[1,2,3] Jurusan Teknik Informatika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Alauddin Makassar
[1,2,3]Jl. H.M. Yasin Limpo No. 36 Samata, Kab Gowa, Sulawesi Selatan, Indonesia
E-mail: hariani.kasim@uin-alauddin.ac.id[1)], darmatasia@uin-alauddin.ac.id[2)], wahyuddin.saputra@uin-alauddin.ac.id[3)]

Abstrak – Keamanan Informasi fokus terhadap perlindungan kerahasiaan, integritas, dan ketersediaan informasi. Namun, hal yang menjadi tak kalah penting terkait dengan keamanan informasi adalah kesadaran terhadap keamanan informasi. Instansi X sebagai salah satu Perguruan Tinggi yang memiliki UPT yang bertanggung jawab terhadap pengelolaan dan penyediaan layanan Teknologi Informasi dan Komunikasi (TIK). Layanan TIK tersebut berada di bawah UPT Pusat Teknologi Informasi dan Pangkalan Data (PUSTIPAD). PUSTIPAD memiliki peranan penting dalam mengumpulkan, mengolah, menyimpan, dan menyajikan informasi yang dibutuhkan oleh lembaga. Penelitian ini mengacu kepada framework COBIT 5 domain APO13 membahas tentang tata kelola keamanan informasi yang mencakup pemeliharaan sistem, mengelola resiko keamanan,dan memonitor keamanan sistem informasi. Penelitian ini menggunakan metode CMMI untuk proses analisis, CMMI merupakan Capability Level yang memiliki tingkat kemampuan dan berlaku untuk memberikan capaian kinerja pada institusi dan memberikan peningkatan proses praktik individual. Hasil penelitian dan penilaian menggunakan standar COBIT 5 APO13 terhadap proses Manajemen keamanan Sistem pada PUSTIPAD Instansi X yaitu untuk proses area APO13.01 mempunyai nilai kondisi saat ini yaitu 4.12 atau berada pada Capability Level *Managed and Measurable,* sedangkan untuk APO13.02 mempunyai nilai 3.77 juga berada pada level *Managed and Measurable* dan untuk APO13.03 mempunyai nilai 3.42 dan berada pada level *defined.* secara keseluruhan ISMS pada domain APO13 untuk PUSTIPAD sudah cukup terstruktur dan berjalan sesuai dengan tujuan yang telah di definisikan sebelumnya.

Kata Kunci: Audit, COBIT 5, CMMI, Keamanan Sistem Informasi.

PENDAHULUAN

Penerapan dan pemanfaatan Teknologi Informasi pada Institusi Pendidikan sudah menjadi hal yang biasa. Peranan Teknologi Informasi tersebut menjadi sangat penting dalam menunjang dan mendukung operasional Institusi agar lebih efektif dan efisien dalam pengelolaannya, sebagai contoh mahasiswa akan mudah memperoleh Informasi yang di butuhkan untuk keperluan administrasi. Penerapan TIK pada institusi setidaknya harus disesuikan dengan kebutuhan agar dapat mencapai tujuan Institusi yang sudah di tetapkan.

Instansi X sebagai salah satu Perguruan Tinggi yang memiliki UPT yang bertanggung jawab terhadap pengelolaan dan penyediaan layanan Teknologi Informasi dan Komunikasi (TIK). Layanan TIK tersebut berada di bawah UPT Pusat Teknologi Informasi dan Pangkalan Data (PUSTIPAD). PUSTIPAD memiliki peranan penting dalam mengumpulkan, mengolah, menyimpan, dan menyajikan informasi yang dibutuhkan oleh lembaga. Sebagai unit utama yang bertanggung jawab terhadap ketersediaan informasi, PUSTIPAD tidak hanya bertanggung jawab terhadap kebutuhan teknis tetapi juga harus mampu menjamin keamanan informasi lembaga. Untuk menjamin kualitas layanan, pihak PUSTIPAD tentunya harus melakukan tahap perencanaan, implementasi, dan evaluasi sistem secara berkala. Salah satu hal yang menjadi keharusan bagi setiap unit penyedian layanan Teknologi Informasi (TIK) adalah menjamin keamaanan informasi lembaga. Seiring dengan perkembangan teknologi, kerentanan Information Exchange Environment (IEE) juga semakin meningkat yang menyebabkan ancaman keamanan menjadi kompleks dan komprehensif bagi lembaga. Hal tersebut merupakan permasalahan dasar yang harus diantisipasi baik oleh organisasi, lembaga, maupun pemerintah.

Umumnya keamanan informasi fokus terhadap perlindungan kerahasiaan, integritas, dan ketersediaan informasi. Namun, hal yang menjadi tak kalah penting terkait dengan keamanan informasi adalah kesadaran

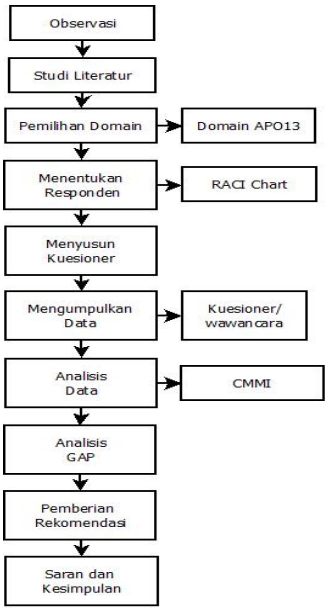
terhadap keamanan informasi. Kesadaran yang dimaksud berkaitan dengan penerapan program kesadaran keamanan yang bertujuan menciptakan perilaku positif sebagai salah satu elemen penting untuk mendukung efektivitas lingkungan keamanan informasi.

Keamanan informasi yang tidak disertai dengan manajemen keamanan informasi tentunya tidak dapat berjalan secara maksimal. Manajemen keamanan informasi berkaitan dengan penanganan keamanan dari sisi manajerial. Manajemen tersebut biasanya dilakukan oleh lembaga yang bertujuan untuk meminimalisir dampak dari insiden terkait keamanan informasi yang tidak diharapkan. Manajemen keamanan informasi memiliki peranan yang sangat penting untuk menjamin keamanan aset informasi yang dimiliki lembaga atau organisasi agar tetap aman dari berbagai kemungkinan ancaman yang ada.

Penelitian ini mengacu kepada framework COBIT 5 domain APO13 membahas tentang tata kelola keamanan informasi yang mencakup pemeliharaan sistem, mengelola resiko keamanan,dan memonitor keamanan sistem informasi. Temuan yang dipeoleh dalam penelitian diharapkan mampu memberi rekomendasi bagi PUSTIPAD Instansi X. Rekomendasi tersebut diharapkan menjadi pedoman dalam meningkatkan kualitas pengelolaan TIK khususnya terakit dengan layanan keamanan informasi. Hal tersebut diharapkan dapat mendukung cita-cita organisasi sehingga tercipta organisasi yang kredibel dan berkualitas.

METODOLOGI PENELITIAN

Penelitian ini meliputi beberapa tahapan dimulai dengan melakukan Observasi pada objek penelitian yaitu PUSTIPAD, kami melakukan interview pada bagian tertinggi organisasi yang mengatur jalannya manajemen teknologi informasi untuk mengetahui pemasalahan yang dihadapi. Wawancara juga bertujuan untuk mengetahui lebih jelas objek yang diaudit sehingga penelitian lebih terarah pada saat dilakukan proses audit, jadi melakukan observasi sebelum turun ke lapangan akan membantu untuk mendapatkan informasi yang akan dipersiapkan pada saat audit. untuk lebih jelasnya dapat dilihat pada gambar dibawah:



Gambar 1 Tahapan Penelitian

Setelah dilakukan observasi maka tahap selanjutnya yaitu melakukan studi literatur dengan mencari referensi dan mempelajari metode-metode sebelumnya yang telah di lakukan oleh peneliti lainnya. Berikutnya adalah pemilihan domain, dalam hal ini peneliti memilih domain APO13 cobit 5 sebagai acuan standar untuk mengetahui apakah sudah sesuai dengan tujuan yang ingin dicapai. Selanjutnya menentukan responden berdasarkan RACI Chart artinya pemilihan responden sesuai dengan peran dan yang bertanggung jawab mengenai domain yang dipilih sebelumnya, setidaknya ada 4 peran dalam pemilihan responden sesuai RACI Chart yaitu Responsible yaitu orang yang melaksanakan kegiatan atau melaksanakan pekerjaan tersebut. Accountable orang yang mempunyai peran yang bertanggung jawab dan memiliki otoritas dalam mengambil keputusan. Consulted orang yang dibutuhkan saran dan konstribusinya pada suatu kegiatan dan Informed orang yang perlu tahu hasil dari keputusan atau tindakan yang diambil. Setelah menentukan responden, tahap selanjutnya menyusun kuesioner untuk diisi oleh responden yang dipilih sesuai RACI chart diatas. Selanjutnya adalah pengumpulan data, baik yang kuesioner maupun wawancara. Setelah data terkumpul maka dilakukan analisis data dengan metode CMMI, dari hasil analisis nanti akan diketahui GAP dari proses ini untuk selanjutnya diberikan solusi dan rekomendasi untuk memperbaiki kondisi, terakhir adalah pengambilan kesimpulan dan saran.

TINJAUAN PUSTAKA

1. *Keamanan Sistem Informasi*

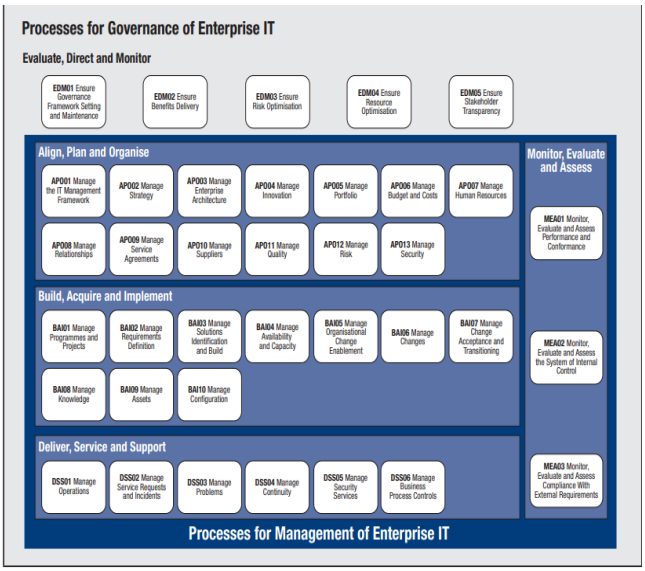
Fungsi dari keamanan informasi yaitu melindungi kerahasiaan, integritas, dan ketersediaan asset baik dalam segi penyimpanan, pengolahan, atau transmisi informasi. Hal tersebut dapat diwujudkan dengan menerapkan kebijakan, pendidikan, pelatihan dan kesadaran serta penguasaan teknologi. Saat ini terdapat tiga konsep utama yang menjadi standar dalam *industry* keamanan yang dikenal dengan sebutan CIA Triangel yang dijelaskan sebagai berikut:.

1. Confidentiality, yaitu usaha dalam menjaga informasi dari pihak yang tidak memiliki akses informasi. Misalnya informasi yang diberikan kepada pihak lain.
2. Integrity, memastikan keaslian pesan yang dikirim melalui jaringan *computer* dan tidak dimodifikasi oleh pihak yang tidak berhak dalam proses pengiriman melalui jaringan.
3. Availability, terdapat ketersediaan hubungan dengan ketersediaan inforamsisaat dibutuhkan. Saat sistem informasi mengalami serangan atau dijebol terdapat mekanisme pada sistem untuk menutup akses informasi.

2. *COBIT 5*

Referensi model proses COBIT 5 merupakan penerus dari model COBIT 4.1 dengan model resiko TI dan IT yang saling terintegritasi. Terdapat 32 proses manajemen dan 5 proses tata kelola yang tergabung dalam 5 domain sebagai berikut:

1. Evaluate, Direct and Monitor (EDM)
   Tata kelola memastikan bahwa tujuan perusahaan dicapai dengan cara melakukan evaluasi kebutuhan, kondisi dan pemilihan pemangku kepentingan; penentuan arah berdasarakan prioritas dan proses pengambilan keputusan; serta pemantauan kinerja, kepatuhan dan kemajuan terhadap arah dan tujuan yang disepakati..
2. Align, Plan and Organize (APO)
   Domain meliputi penggunaan informasi & teknologi dan penentuan cara terbaik yang digunakan dalam perusahaan untuk mencapai tujuan dan sasaran perusahaa. Selain itu Domain juga mengamati bentuk organisasi dan infrastruktur yang harus diambil dalam mencapai hasil yang optimal untuk menghasilkan manfaat sebanyaknya dari penggunaan TI. Tabel berikut mencantumkan proses TI tingkat tinggi.
3. Build, Acquire and Implement (BAI)
   Domain Build, Acquire and Implement (BAI) meliputi identifikasi persyaratan TI, mendapatkan teknologinya, dan mengimplementasikannya dalam proses bisnis perusahaan.
4. Deliver, Service and Support (DSS)
   Berperan pentinga dalam pengiriman teknologi informasi. Yang meliputi bidang pelaksanaan aplikasi dalam sistem sampai hasilnya, dan proses pendukung yang memungkinkan pelaksanaan sistem lebih efektif dan efisien.
5. Monitor, Evaluate and Assess (MEA)
   Domain Monitor, Evaluate and Assess (MEA) berhubungan dengan strategi perusahaan dalam menilai kebutuhan dan melakukan audit terhadap sistem TI apakah masih sesuai dengan tujuan perancangannya dan pengendalian untuk mematuhi persyaratan peraturan. Selain itu meliputi masalah penilaian independen terhadap efektivitas sistem TI dalam kemampuannya untuk memenuhi tujuan bisnis dan proses pengendalian perusahaan oleh auditor internal dan eksternal.



Gambar 2 Model Referensi Proses COBIT 5

3. APO13 (Manage Security)

Meliputi pendefinisian, pengoperasiaan dan pengawasan terhadap sistem dalam proses manajemen keamanan informasi. Yang bertujuan untuk menjaga dampak dan kejadian dari insiden masih berada dalam batas resiko yang dapat diterima

perusahaan. Adapun sub proses pada APO13 sebagai berikut:

1. APO13.1, Membangun dan Memelihara Sistem Manajemen Keamanan Informasi
2. APO13.2, Mendefinisikan dan Mengelola rencana Penanganan Keamanan Informasi.
3. APO13.3, Mengawasi dan Mengkaji Sistem Manajemen Keamanan Informasi.

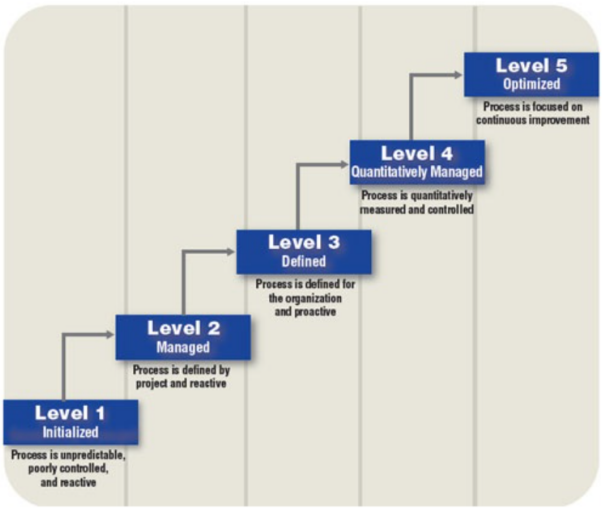
4. Metode CMMI

CMMI merupakan Capability Level yang memiliki tingkat kemampuan dan berlaku untuk memberikan capaian kinerja pada institusi dan memberikan peningkatan proses praktik individual. Pada praktiknya CMMI dikonvensikan ke dalam beberapa level yaitu Level 0 sampai Level 5 (terdiri 6 level) dimana setiap level dikembangkan dari level sebelumnya dengan menambahkan fungsi baru sehingga kemampuan level berikutnya bisa jadi meningkat. Berikut tingkatan Capability Level terlihat seperti gambar di bawah:

Gambar 3. *Capability Level*

- Level 0: Tidak lengkap (Incomplete): proses ini tidak lengkap dikarenakan ada beberapa proses yang belum dilaksanakan oleh instansi.
- Level 1: Dilakukan (Performed): pada proses ini menandakan semua *specific practices* sudah dilaksanakan pada setiap proses area oleh instansi dan memenuhi tujuan dari area praktik.
- Level 2: Dikelola (Managed): terdapat aktivitas yang perlu dilaksanakan untuk mencapai level ini dan merujuk pada praktik level 1, pada praktik ini sederhana, namun cukup lengkap membahas tujuan area praktik.
- Level 3: Ditetapkan (Defined): proses ini sudah dikelolah dengan baik dan dibangun pada praktik level 2. proses ini sudah mengacu menggunakan standar instansi/organisasi yang dapat disesuaikan untuk mengatasi proyek dan pekerjaan untuk mencapai tujuan kinerja di dalam organisasi.
- Level 4: proses ini dikelola secara kuantitatif (Quantitatively Managed): pada proses ini menggunakan kuantitatif statistik dan dibangun di level 3 untuk memahami beberapa type kinerja lalu mendeteksi, memperbaiki dan memprediksi proses kerja selanjutnya agar diperoleh hasil lebih baik sesuai dengan tujuan organisasi.
- Level 5: Mengoptimalkan (Optimizing): proses ini dilakukan pengoktimalan pada kinerja dan terjadi peningkatan, proses ini dibangun di level 4 dengan menggunakan kuantitaif statistik dan mencapai tujuan kinerja yang diharapkan.

Model CMMI selanjutnya menempatkan instansi/insitusi ke dalam tingkat kematangan yang disebut 5 Maturity Level seperti Gambar dibawah:



Gambar 4. *Maturity Level*

- Level 1: *Initial*. Pada level ini institusi belum menjalankan proses CMMI dan umumnya institusi pada level ini tidak bergantung pada sistem tapi bergantung kepada orang.
- Level 2: *Managed*. Dilevel ini Institusi sudah mencapai beberapa proses, setiap orang dapat terlibat aktif dan saling menyesuaikan akan tetapi belum seragam secara keseluruhan.
- Level 3: *Defined*. Dilevel ini Instansi/ Institusi sudah melaksanakan semua proses yang sudah

ditetapkan dan semua tim mengerti bagaimana proses itu berjalan.

- Level 4: *Quantitatively Managed.* Dilevel ini Instansi atau Institusi dikelola semakin terstruktur dan terbuka, pada setiap proses sudah diterapkan konsepp kuantitatif dimana semuanya sudah dikontrol dan dimonitoring.
- Level 5: *Optimizing.* Dilevel ini berada pada level puncak dalam CMMI, suatu Institusi telah fokus pada peningkatan secara berkesinambungan dan melalui semua proses yang ada pada level 2, 3, dan 4 sehingga sistem dapat berjalan secara optimal.

PENELITIAN TERKAIT

Penelitian ini ditinjau dari penelitian sebelumnya, berikut beberapa penelitian terkait mengenai tata kelola dan manajemen kemanan informasi.

Penelitian terkait pengelolaan keamanan informasi telah banyak dilakukan. Turang dan Turang (2020) melakukan penelitian pada salah satu instansi terkait audit tata kelola keamanan Teknologi Informasi. Auidt tata kelola tersebut dilakukan dengan menggunakan Framework COBIT 5. Audit tata kelola yang dilakukan berfokus pada keamanan Teknologi Informasi DSS05 untuk mengetahui tingkat ketercapaian kapabilitas pada domain tersebut. Hasil penelitian menunjukkan bahwa tata kelola layanan keamanan informasi pada instansi X masih berada pada level 1. Adapun tingkat pencapaian kapabilitas yang diperoleh adalah sekitar 69%. Untuk mencapai mencapai level selanjutnya, intansi perlu melakukan perancangan tata kelola keamanan Teknologi Informasi yang meliputi evaluasi secara berkala terhadap berbagai kemungkinan ancaman keamanan, menyediakan dokumen terkait hak akses pengguna berdasarkan kebutuhan pada setiap unit, serta menyediakan dokumen SOP yang lengkap terkait keamanan Teknologi Informasi. Selain domains DSS05, dalam penelitian tersebut juga dilakukan audit menggunakan domain APO13. Hasil penelitian menunjukkan bahwa instansi X masih berada pada level 1 dengan tingkat pencapaian kapabiitas sebesar 33%. Pencapaian level selanjutnya, instansi perlu melakukan perancangan terkait ketersediaan unit khusus yang bartanggung jawab terhadap manajemen keamanan sistem informasi. Selain itu, instansi juga harus memiliki dokumentasi yang lengkap terkait setiap aktivitas yang dilakukan.

Penelitian selanjutnya yaitu Budiyono dan Ramdani (2020) menggunakan COBIT 4.0 untuk audit keamanan Sistem Informasi Jaringan di Diskominfo Kota Tangerang. Hasil penelitian menunjukkan bahwa instansi tersebut telah menerapkan Teknologi Informasi terkini namun masih perlu dilakukan perencanaan lebih lanjut untuk menjamin keamanan informasi khususnya yang berkaitan dengan transaksi data. Untuk mencapai hal tersebut, diperlukan peranan sumber daya manusia dalam melaksanakan dan mengawasi penerapan teknologi informasi yang aman. Selain itu, instansi juga perlu melakukan evaluasi secara berkala yang meliputi pengecekan, pengawasan, dan juga pengelolaan agar penggunaan teknologi informasi disertai dengan keamanan informasi. Pihak instansi perlu melakukan sosialisasi, pendidikan dan pelatihan kepada Sumber Daya Manusia sebagai pelaksana dan pengawas penerapan Teknolgi Informasi.

Dewi et al (2015) Menggunakan COBIT 5 dalam melakukan audit keamanan Sistem Informasi pada kantor pemerintah di kota Yogyakarta. Untuk mencapai level 1, unit TIT Setda Kota Yogyakarta selaku penanggung jawab terhadap layanan Teknologi Informasi perlu melakukan praktik dasar untuk perbaikan proses serta menghasilkan produk kerja yang berada pada level 1 *performed process.* Untuk menpai level selanjutnya, unit perlu melakukan praktik generik dan menghasilkan produk kerja generik yang berada pada level 2 *managed process.*

Penelitian yang dilakukan oleh David dkk (2018) juga menggunakan COBIT 5 untuk audit keamanan Teknologi Informasi pada lembaga X. Hasil penelitian menunjjukan bahwa instansi X berada pada level 2: *Managed Process* dengan tingkat kematangan Teknologi Informasi adalah 2.48. Hal tersebut menunjukkan bahwa penerapan Teknologi Informas dalam instansi dilakukan secara teratur dan dapat dikendalikan dengan baik oleh instansi.

HASIL DAN PEMBAHASAN

A. Pengumpulan Data

Penelitian ini menggunakan kuesioner yang diberikan kepada narasumber sesuai dengan RACI Chart, dimana posisi narasumber di dalam organisasi sebagai divisi Pengembangan dan Pelatihan Sistem, Divisi Internet dan Jaringan dan Divisi Multimedia

dan WEB. Kuesioner ini kemudian disesuaikan domain APO13 pada framework COBIT 5 dan dianalisis menggunakan metode CMMI. Model sampel mengikuti skala likert meliputi ukuran ordinal dimana angka diberikan pada tiap tingkatan, dan ukuran nominal dimana angka ini digunakan untuk memberi urutan pada tingkatan terendah sampai tertinggi.

Tabel 1 Skala Likert

Jawaban	Nilai
Sangat tidak setuju	1
Tidak Setuju	2
Ragu	3
Setuju	4
Sangat Setuju	5

Seperti terlihat pada tabel diatas angka 1 berada pada urutan terendah dan angka 5 berada pada urutan tertinggi.

B. *Analisis Data Menggunakan CMMI*

Interpretasi kuesioner dan wawancara dapat digunakan sebagai temuan dalam penelitian ini berdasarkan perhitungan maturity level yang di peroleh. Terdapat beberapa kriteria yang harus di penuhi oleh PUSTIPAD untuk proses identifikasi ini seperti terlihat pada tabel 1 dibawah:

Tabel 2 Kriteria Maturity level

Kriteria	Level
0-0.50	*Initial*
0.51-1.50	*Ad Hoc*
1.51-2.50	*Repeatable but Invinitive*
2.51-3.50	*Define Process*
3.51-4.50	*Managed and Measurable*
4.51-5.00	*optimized*

Hasil kuesioner dari responden akan dilakukan perhitungan sesuai dengan jawaban dan jumlah pertanyaan pada tiap sub domain. Terdapat beberapa pertanyaan untuk tiap sub domain seperti yang terlihat pada contoh tabel 2 dibawah, berikut hanya contoh satu sub domain karena keterbatasan tempat:

Tabel 3 Nilai Kuesioner

Sub Domain	Pertanyaan	Responden	Expected
APO13.01 menetapkan dan memelihara Sistem Manajemen Keamanan Informasi (ISMS)	1	5	5
	2	5	5
	3	5	5
	4	5	5
	5	3	5
	6	4	5
	7	3	5
	8	3	5

Selanjutnya untuk menghitung index kematangan dapat menggunakan rumus berikut:

$$Index = \sum \frac{Jawaban\ Kuesioner}{Domain\ Proses}$$

Perhitungan Index yang telah dilakukan akan memperoleh hasil seperti tabel 4. Data indeks adalah maturity level existing atau level nilai saat ini dan nilai ini nanntinya digunakan untuk melihat Gap.

Tabel 4 Hasil Index

Selanjutnya dapat dilakukan analisis pada Gap Maturity Level sehingga Maturity Level setiap subdomain bisa di tetapkan . Seperti pada Tabel 5 dan 6 berikut.

Tabel 5 Maturity Level

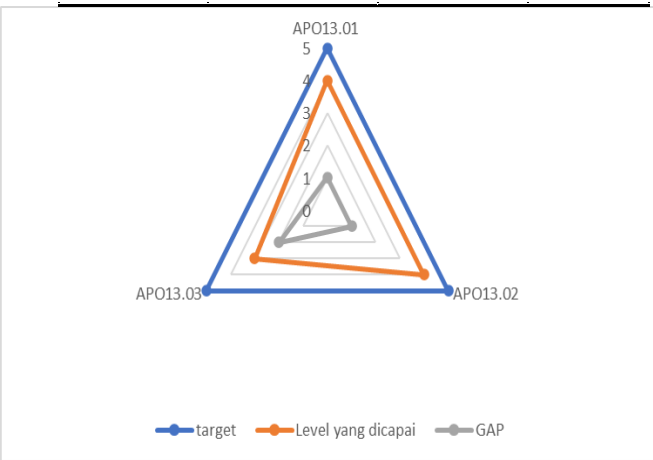
Sub Domain	Deskripsi	level
APO13.01	**menetapkan dan memelihara Sistem Manajemen Keamanan Informasi (ISMS).**	Managed and Measurable
APO13.02	**Menentukan dan mengelola rencana perawatan risiko keamanan informasi (ISMS)**	Managed and Measurable
APO13.03	**Monitor dan peninjauan manajemen keamanan sistem informasi (ISMS).**	Define Process

Gap maturity level telah kita dapatkan dan menjadi acuan untuk memberikan rekomendasi untuk perbaikan.

Tabel 6 GAP Maturity Level

Sub Domain	Deskripsi	Target	Level yang dicapai	GAP
APO13.01	menetapkan dan memelihara Sistem Manajemen Keamanan Informasi (ISMS).	5	4	1
APO13.02	Menentukan dan mengelola rencana perawatan risiko keamanan informasi (ISMS)	5	4	1
APO13.03	Monitor dan peninjauan manajemen keamanan sistem informasi (ISMS).	5	3	2

Sub Domain	Deskripsi	Jumlah Pertanyaan	Index Maturity
APO13.01	menetapkan dan memelihara Sistem Manajemen Keamanan Informasi (ISMS).	8	4.12
APO13.02	Menentukan dan mengelola rencana perawatan risiko keamanan informasi (ISMS)	9	3.77
APO13.03	Monitor dan peninjauan manajemen keamanan sistem informasi (ISMS).	7	3.42



Gambar 5 GAP Maturity Level

Gap Maturity Level selanjutnya bisa dianalisis sehingga dapat di tetapkan Maturity Level untuk tiap subdomain.

C. Pemberian Rekomendasi

Hasil analisis Gap yang telah di dapatkan dari level yang dicapai dan level saat ini pada APO13, maka dapat diberikan rekomendasi sebagai bemrikut:

1. APO13.01 Menetapkan dan memelihara Sistem Manajemen Keamanan Informasi (ISMS). sub-domain ini berada pada level *Managed and Measurable* dimana pada level ini PUSTIPAD semakin terstruktur dalam mengelola ISMS nya, dan pada setiap prosesnya sudah dikontrol dan

dimonitoring. Agar dapat berada pada level puncak PUSTIPAD perlu mengoptimalkan level ini dengan melakukan perkembangan dan peningkatan secara berkesinambungan pada semua proses manajemen.

2. APO13.02 Menentukan dan mengelola rencana perawatan risiko keamanan informasi (ISMS). bagian ini berada pada level *Managed and Measurable* sama dengan sub-domain yang APO13 yang pertama. Dalam menentukan dan mengelolah ISMS PUSTIPAD harus mengoptimalkan setiap prosesnya pada level-level sebelumnya agar dapat mencapai level puncak atau *Optimizing.*
3. APO13.03 Monitor dan peninjauan manajemen keamanan sistem informasi (ISMS). sub-domain ini berada pada level *define*, dilevel ini PUSTIPAD sudah melaksanakan semua proses ISMS yang sudah ditetapkan dan semua tim mengerti bagaimana proses tersebut berjalan. Namun untuk ke level berikutnya perlu dioptimalkan ari level sebelumnya.

KESIMPULAN

Hasil penelitian dan penilaian menggunakan standar COBIT 5 APO13 terhadap proses Manajemen keamanan Sistem pada PUSTIPAD Instansi X dapat disimpulkan bahwa untuk proses area APO13.01 mempunyai nilai kondisi saat ini yaitu 4.12 atau berada pada Capability Level *Managed and Measurable,* sedangkan untuk APO13.02 mempunyai nilai 3.77 juga berada pada level *Managed and Measurable* dan untuk APO13.03 mempunyai nilai 3.42 dan berada pada level *defined.* secara keseluruhan ISMS pada domain APO13 untuk PUSTIPAD sudah cukup terstruktur dan berjalan sesuai dengan tujuan yang telah di definisikan sebelumnya, meskipun beberapa proses masih belum seragam pelaksanaannya tapi dengan usaha dan sistem yang terbuka serta tim yang memahami proses dapat meningkatkan level secara maksimal atau berada pada level puncak.

DAFTAR PUSTAKA

Andrianti, A., & Astri, L. Y. (2020). Tata Kelola Keamanan Teknologi Informasi Menggunakan Framework COBIT 5 Fokus Proses DSS05 (Studi Pada RS Bhayangkara Jambi). *Indonesian Journal of Computer Science*, *9*(2), 86–95. https://doi.org/10.33022/ijcs.v9i2.297

Budiyono, P., Kom, S., Email, M. K., Ramdani, D., Kom, S., & Email, M. T. (2020). *Audit Keamanan Sistem Informasi Jairngan Komputer Dengan COBIT 4 . 0 di Diskominfo Kota Tangerang Computer Network Information Security Audit Audit with COBIT 4 . 0 at Diskominfo Tangerang City*. *III*(03), 20–22.

Ciptaningrum, D., Nugroho, E., & Adhipta, D. (2015). Cobit 5 Sebagai Metode Alternatif Bagi Audit Keamanan Sistem Informasi. *Seminar Nasional Teknologi Informasi Dan Multimedia*, 6‑8.

Ciptaningrum, D., Nugroho, E., & Adhipta, D. (2015). Audit Keamanan Sistem Informasi pada Kantor Pemerintah Yogyakarta. *Seminar Nasional Teknologi Informasi Dan Komunikasi*, 2089-9815.

David Purba, A., Adi Purnawan, I. K., & Agus Eka Pratama, I. P. (2018). Audit Keamanan TI Menggunakan Standar ISO/IEC 27002 dengan COBIT 5. *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*, *6*(3), 148. https://doi.org/10.24843/jim.2018.v06.i03.p01

Imany, Y. D., Hayuhardhika, W., Putra, N., & Herlambang, A. D. (2019). Evaluasi Tata Kelola Keamanan Informasi menggunakan COBIT 5 pada Domain APO13 dan DSS05 (Studi pada PT Gagas Energi Indonesia). *Jurnal Pengembangan Teknologi Informasi Dan Ilmu Komputer*, *3*(6), 5926–5935.

ISACA. (2012). Enabling Processes. In *Cobit 5*.

Lenawati, M., Winarno, W. W., & Amborowati, A. (2017). Tata Kelola Keamanan Informasi pada PDAM Menggunakan ISO/IEC 27001:2013 Dan COBIT 5. *Sentra Penelitian Engineering Dan Edukasi*, *9*(1), 44–49.

Matin, I. M. M., Arini, A., & Wardhani, L. K. (2018). Analisis Keamanan Informasi Data Center Menggunakan Cobit 5. *Jurnal Teknik Informatika*, *10*(2), 119–128. https://doi.org/10.15408/jti.v10i2.7026

pratama, heru. (2018). *Audit Keamanan Sistem Informasi Pada Kantor Samsat Di Kota Krui Menggunakan Cobit 5*. *2015*(Sentika). https://doi.org/10.31219/osf.io/pkrej

Turang, D. A. O., & Turang, M. C. (2020). Analisis Audit Tata Kelola Keamanan Teknologi Informasi Menggunakan Framework Cobit 5 Pada Instansi X. *Klik - Kumpulan Jurnal Ilmu Komputer*, *7*(2), 130. https://doi.org/10.20527/klik.v7i2.316

Umar, R., Riadi, I., & Handoyo, E. (2019). Analisis Keamanan Sistem Informasi Berdasarkan Framework COBIT 5 Menggunakan Capability Maturity Model Integration (CMMI). *Jurnal Sistem Informasi Bisnis*, *9*(1), 47. https://doi.org/10.21456/vol9iss1pp47-54

Utomo, B. T. (2019). *AUDIT KEAMANAN*

LABORATORIUM 2 FASILKOM UNIVERSITAS SUBANG BERBASIS COBIT 5 Pendahuluan. *VI*(2), 9–13.

CMMI Product Team, 2020
https://resources.sei.cmu.edu/library/author.cfm?authorid=4781