Audit Keamanan TI Menggunakan Standar ISO/IEC 27002 dengan COBIT 5

Altry David Purba, I Ketut Adi Purnawan, I Putu Agus Eka Pratama
Program Studi Teknologi Informasi, Fakultas Teknik, Universitas Udayana
Bukit Jimbaran, Bali, Indonesia-803611
e-mail: altrysiboro@gmail.com, adipurnawan@unud.ac.id, eka.pratama@unud.ac.id

Abstrak

Keamanan teknologi informasi merupakan kebutuhan vital bagi organisasi untuk menjamin kerahasiaan, integritas dan ketersediaan informasi. Salah satu organisasi yang membutuhkan keamanan TI adalah Lembaga X. Lembaga X yang memiliki tugas dan fungsi sebagai penyelenggara sistem informasi, pusat data dan informasi kebencanaan harus mampu menjamin keamanan, kerahasiaan, dan integritas data, juga kinerja sistem harus dikendalikan sehingga dapat berjalan dengan optimal. Audit keamaman TI dilakukan untuk memastikan bahwa keamanan informasi dan pengelolaan data yang diterapkan di Lembaga X sesuai dengan prosedur serta mengetahui tingkat kematangan teknologi informasi yang diterapkan. Standar yang digunakan dalam proses audit adalah ISO/IEC 27002 sebagai kontrol keamanan dan COBIT 5 untuk mengidentifikasi proses bisnis serta tingkat kematangan. Hasil tingkat kematangan TI di lembaga X adalah 2.48 yang masuk ke dalam kategori level 2: *Managed Process.* Level 2: *Managed Process* menunjukkan bahwa proses penerapan teknologi informasi telah dijalankan dan diimplementasikan dengan cara yang lebih teratur dan sudah mulai dikendalikan.

.

Kata Kunci: Audit Keamanan, ISO 27002, COBIT 5, Tingkat Kematangan

Abstract

Information technology security is an important for organizations to ensure the confidentiality, integrity and availability of information. One of the organization that requires IT security is Lembaga X. Lembaga X has duties and functions as the implementation of information systems, the disaster data and information centers must be able to ensure the security, confidentiality and data integrity, also the system performance must be controlled so that it can run optimally. IT security audit is needed to ensure the information security management are implemented in accordance with procedures and to determine the level of information technology maturity applied. The standards used in this audit are ISO / IEC 27002 as a security controls and COBIT 5 to identify business processes and maturity levels. The result of the IT maturity level in Lembaga X is 2.48 which is included in the level 2: Managed Process. Level 2 indicates that the process of applying information technology has been implemented regularly and has begun to be controlled.

Keywords: *Security Audit,* ISO 27002, COBIT 5, *Maturity Level*

1. Pendahuluan

Kemajuan TI atau SI di era globalisasi berkembang sangat pesat. Teknologi informasi menjadi kebutuhan bagi organisasi sebagai alat komunikasi, pengolahan data dan informasi serta sebagai upaya meningkatkan efektivitas kinerja organisasi. Kontrol keamanan aset informasi yang lemah adalah masalah yang harus dicegah dan diatasi untuk menghindari pihak yang tidak bertanggungjawab dapat mencuri dan menggangu jalannya aktivitas yang berkaitan dengan pengelolaan data dan informasi. Salah satu instansi yang membutuhkan keamanan terhadap perlindungan aset informasi adalah Lembaga X. Lembaga X merupakan unit pelaksana yang bertugas menyiapkan dukungan fasilitas penyelenggaraan sistem informasi dan berfungsi sebagai pusat data dan informasi kebencanaan yaitu penerima, pengolah, dan pendistribusi Informasi [1].

Lembaga X sebagai pusat data dan informasi tentunya harus mampu menjamin keamanan TI sehingga kerahasiaan, integritas data yang diolah serta kinerja sistem dapat dikendalikan untuk memastikan bahwa sistem TI yang diterapkan berjalan dengan optimal.

Audit keamanan TI di Lembaga X dilakukan untuk memastikan bahwa keamanan informasi dan pengelolaan data yang diterapkan telah sesuai prosedur dan memiliki performa yang maksimal. Audit juga dilakukan untuk mengetahui *maturity level* yang diterapkan.

Standar yang digunakan dalam audit ini adalah ISO/IEC 27002 dan COBIT 5. ISO 27002 digunakan sebagai kontrol keamanan TI [2] serta COBIT 5 digunakan untuk mengidentifikasi proses bisnis dan tujuan organisasi serta peniliaian *maturity level* [3].

Penelitian sebelumnya yang membahas mengenai audit keamanan TI diantaranya adalah "Audit Keamanan SIMAK Berdasarkan ISO 27002 (Studi Kasus: FE UNUD)" oleh Yulius C. N. Bless dan kawan-kawan dengan topik bahasan audit mencakup kebijakan keamanan, organisasi keamanan informasi, manajemen komunikasi dan operasi, kontrol akses, akuisisi sistem informasi, pembangunan dan pemeliharaan serta manajemen kejadian keamanan informasi. Model pengujian tingkat kematangan menggunakan perhitungan *Maturity Level* [2]. *"Audit of Application Procurement using Cobit Framework"* oleh Gusti Ayu Theresia yang melakukan audit untuk mengukur *maturity level* pengadaan aplikasi di sebuah universitas dengan menggunakan kerangka kerja COBIT 4.1. COBIT digunakan sebagai alat untuk mengidentifikasi proses bisnis dan tujuan perusahaan. Fokus domain yang dipilih adalah PO2, PO3 AI2, AI5, AI7 and DS7 [3]. "*Measuring the Performance of IT Management in Financial Enterprise by Using COBIT*" oleh Gusti Ayu Dian dan kawan-kawan yang melakukan pengukuran tinkat kematangan kinerja manajemen TI di perusahaan keuangan. Kerangka kerja yang digunakan adalah COBIT 5 dengan fokus domain adalah PO1, PO2, AI4, DS7, ME1, and ME4 [4]. "Pedoman Tata Kelola Teknologi Informasi Menggunakan *IT Governance Design Frame Work* (Cobit) Pada PT. X." oleh I Ketut Adi Purnawan yang menggunakan COBIT sebagai *framework* dalam penyusunan pedoman tata kelola teknologi informasi secara khusus pada DS11 yaitu pengelolaan data mengenai tingkat kepedulian manajemen (*management awareness*) dan tingkat kematangan (*maturity level*) [5]. "Audit TI Kinerja Manajemen PT. X Dengan Frame Work Cobit 4.1 oleh I Putu Ade Ambara dan kawan-kawan merupakan penelitian yang menggunakan COBIT sebagai panduan implementasi tata kelola manajemen TI. Audit dilakukan untuk mengukur tingkat kematangan TI dan menganalisis kesenjangan sehingga dapat diberikan rekomendasi untuk meningkatkan kinerja manajemen TI [6].

Pengembangan penelitian audit keamanan TI yang dilakukan adalah dengan menggunakan kombinasi 2 standar yaitu COBIT 5 dan ISO 27002. Melalui kombinasi standar tersebut maka tujuan bisnis organisasi dapat didefinisikan dan di identifikasi lebih rinci berdasarkan kontrol yang telah disediakan COBIT 5 serta dengan ISO 27002 penilaian tingkat keamanan TI yang diterapkan di lingkungan organisasi dapat dilakukan dengan tepat sasaran karena standar ISO 27002 sangat fleksibel untuk dikembangkan tergantung kepada kebutuhan, tujuan bisnis, proses bisnis organisasi serta di khususkan untuk audit di bidang keamanan teknologi informasi.

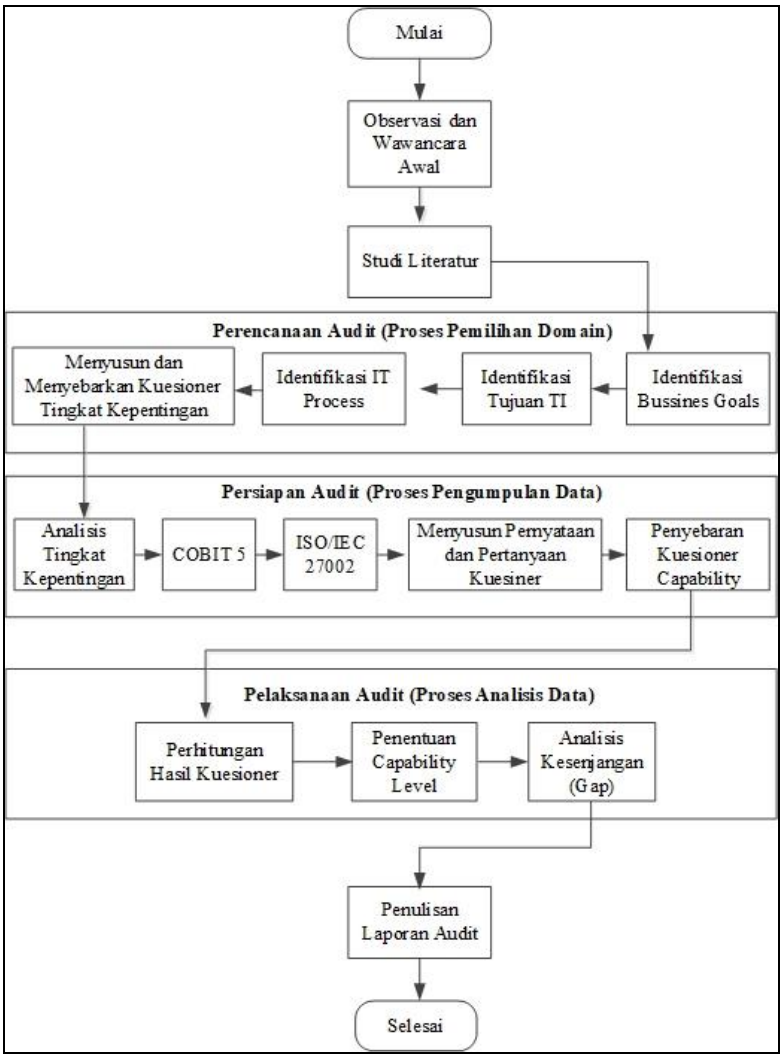
Audit ini dilakukan untuk mengetahui *maturity level* keamanan sistem TI yang diterapkan di Lembaga X.

2. Metodologi Penelitian

Metodologi penelitian merupakan langkah yang sudah ditetapkan dalam melakukan penelitian. Tujuan dari metodologi penelitian ini adalah agar proses penelitian yang dilakukan menjadi lebih teratur, sistematis, terkontrol dan terarah.

2.1 Desain Proses Audit

Desain proses audit merupakan tahapan-tahapan yang ditetapkan dalam melakukan audit keamanan teknologi informasi agar proses audit yang dilakukan secara sistematis dan tepat sasaran. Tahapan-tahapan desain proses audit dapat dilihat dalam Gambar.1



Gambar 1**.** Desain Proses Audit

Gambar 1. menunjukkan bahwa terdapat 6 tahapan utama proses audit, yang dimulai dari proses melakukan observasi dan wawancara dengan bagian tertinggi 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. Tahap kedua yaitu melakukan studi literatur yang berhubungan dengan keamanan teknologi informasi, panduan pengimplementasian ISO/IEC 27002 dan COBIT 5. Tahap ketiga yaitu proses pemilihan domain yang terdiri dari 4 proses yang saling berhubungan yaitu mengidentifikasi *business goals*, mengidentifikasi IT *goals*, mengidentifikasi IT *process* serta *Mapping* domain COBIT 5 kedalam Objektif Kontrol ISO 27002. Identifikasi *business goals* bertujuan untuk memadankan tujuan bisnis dan visi misi organisasi dengan *business goals* yang ada pada COBIT 5. Identifikasi IT *goals* bertujuan untuk melihat keterkaitan antara tujuan bisnis organisasi dari hasil padanan tujuan bisnis dengan IT *goals* pada COBIT 5. Identifikasi IT *process* adalah proses untuk menemukan proses-proses domain yang ada pada COBIT 5 yang dikaitkan dengan IT *goals* yang telah dipetakan. Proses TI yang telah terpilih kemudian dijadikan sebagai dasar penyusunan kuesioner tingkat kepentingan. Fungsi dari kuesioner kepentingan ini adalah untuk mengetahui opini dari petinggi organisasi mengenai nilai kepentingan setiap proses TI. Tahap keempat yaitu proses pengumpulan data yang terdiri dari proses menganalisis hasil dari kuesioner tingkat kepentingan, melakukan *mapping* proses TI COBIT 5 hasil kuesioner tingkat kepentingan dengan ke dalam Objektif Kontrol ISO 27002 serta penyusunan daftar pernyataan dan pertanyaan dalam bentuk kuesioner yang didasarkan pada panduan implementasi yang ada pada ISO/IEC 27002, kemudian disebarkan ke pada responden yang dipilih.

Tahap kelima yaitu proses analis data. Tahap analisis data merupak proses perhitungan hasil kuesioner yang telah di isi oleh para responden. Hasil jawaban dari pertanyaan kuesioner kemudian dianalisis dan di hitung tingkat kematangannya dengan metode penilaian *Capability level* untuk setiap kontrol keamanan. Hasil *nilai capability* level yang telah diperoleh kemudian dilakukan analisis kesenjangan (GAP) yaitu dengan cara membandingkan *maturity level* yang diharapkan dengan *maturity level* sistem saat ini. Tahap keenam yaitu melakukan penulisan laporan hasil audit keamanan TI yang dilakukan.

2.2 Metode Pengumpulan Data

Metode pengumpulan data dilakukan menggunakan 3 teknik pengumpulan data yaitu sebagai berikut.

a. Wawancara. Wawancara dilakukan secara terbuka (*opened interview*) dengan tujuan . untuk dapat mengumpulkan informasi yang tidak diperoleh melalui kegiatan observasi.
b. Kuesioner/Angket. Kuesioner/Angket yang dibuat berisi seperangkat pertanyaan yang disusun sesuai dengan standar COBIT 5 untuk kuesioner tingkat kepentingan dan ISO/IEC 27002:2005 untuk kuesioner tingkat kematangan.
c. Observasi. Observasi dilakukan untuk mengetahui kondisi *axisting* objek yang diaudit serta untuk menyesuaikan hasil kuesioner dengan keadaan sistem TI saat ini.

Data audit yang telah diperoleh melalui wawancara dan observasi dilanjutkan dengan melakukan penyusunan kuesioner tingkat kepentingan. Tingkat kepentingan dibagi dalam lima tingkat, yaitu Sangat tidak penting (STP), tidak penting (TP), cukup penting (CP), penting (P) dan sangat penting (SP). Contoh kuesioner tingkat kepentingan terdapat dalam Tabel 1.

Tabel 1. Contoh Kuesioner Tingkat Kepentingan

Domain	Pernyataan	Tingkat Kepentingan				
		STP	TP	CP	P	SP
DSS03	Mengidentifikasi masalah, mengklarifikasi masalah dan akar penyebab serta dapat memberikan rekomendasi perbaikan untuk mencegah resiko yang mungkin kembali muncul.					

Kuesioner tingkat kepentingan bertujuan untuk mengetahui opini dari petinggi organisasi mengenai nilai kepentingan setiap proses TI. Hasil kuesioner tingkat kepentingan, selanjutnya dipetakan kedalam kontrol keamanan ISO 27002. Hasil pemetaan tersebut dijadikan sebagai acuan penyusunan pernyataan berdasarkan kontrol keamanan yang telah dipilih. Contoh pernyataan audit untuk kontrol Keamanan Organisasi Keamanan Informasi terdapat dalam Tabel 2.

Tabel 2. Contoh Pernyataan Kontrol Keamanan Organisasi Keamanan Informasi

Klausul 6 Organisasi Keamanan Informasi		
6.1.3 Pembagian Tanggung Jawab Keamanan Informasi		
No.	**Pernyataan**	**Bobot**
1	Adanya pembagian tugas dan tanggung jawab keamanan informasi yang ditetapkan secara rinci dan jelas..	
2	Telah tersedia panduan dan prosedur dalam alokasi peranan keamanan di lingkungan organisasi yang dituangkan dalam dokumen kebijakan keamanan	

Setiap pernyataan akan dilakukan pembobotan karena penerapan masing-masing pernyataan memiliki resiko yang berbeda-beda. Pembobotan nilai resiko dapat dilihat dalam Tabel 3.

Tabel 3. Bobot Penilaian Resiko

Bobot	Risiko
0.1 – 0.3	*Low*
0.4 – 0.6	*Medium*
0.5 – 1.0	*High*

Pernyataan yang telah memiliki nilai pembobotan, dilanjutkan dengan membuat pertanyaan berdasarkan pernyataan yang ada. Setiap pernyataan belum tentu memiliki satu pertanyaan namun dapat memiliki lebih dari satu perntanyaan asalkan pertanyaan tersebut memiliki kaitan dengan setiap pertanyaan**.** Contoh pertanyaan untuk kontrol keamanan Organisasi Keamanan Informasi berdasarkan pernyataan yang telah dibuat adalah seperti Tabel 4.

Tabel 4. Contoh Pertanyaan pada Kontrol Keamanan Organisasi Keamanan Informasi

Klausul 6 Organisasi Keamanan Informasi	
Kontrol Keamanan: 6.1.3 Pembagian Tanggung Jawab Keamanan Informasi	
No Pernyataan	**Pertanyaan**
1	• Apakah telah ditetapkannya pembagian tanggung jawab keamanan informasi secara jelas? • Apakah pembagian tanggung jawab tersebut telah dibuat secara detail dan terdokumentasi secara jelas?

Kuesioner yang telah dibuat kemudian disebarkan ke pada responden yang telah di pilih dan hasil kuesioner yang di isi responden kemudian dihitung untuk mengukur tingkat kematangan. Cara perhitungan kuesioner tingkat kematangan dijelaskan dalam Tabel 5 [7].

Tabel 5. Cara Perhitungan *Maturity level*.

Langkah	**Proses**
01	Menghitung rata-rata bobot setiap pernyataan (bila pernyataan lebih dari satu)
02	Merekapitulasi skor nilai setiap pertanyaan
03	Menghitung rata-rata skor nilai setiap pertanyaan
04	Mengalikan bobot setiap pernyataan dengan nilai rata-rata skor nilai pertanyaan

Contoh kerangka kerja perhitungan untuk mengetahui *maturity level* dapat dilihat dalam Tabel 6.

Tabel 6. Contoh Kerangka Kerja Perhitungan *Maturity level*.

Klausul 6 Organisasi Keamanan Informasi				
Kontrol Keamanan: 6.1.3 Pembagian Tanggung Jawab Keamanan Informasi				
No.	**Pernyataan**	**Bobot**	**Skor nilai**	**Nilai**
1	Pengalokasian tugas dan tanggung jawab keamanan informasi telah ditetapkan secara rinci dan jelas..			
2	Tersedia panduan dan prosedur dalam alokasi peranan keamanan di lingkungan organisasi yang dituangkan dalam dokumen kebijakan keamanan			

3. Kajian Pustaka

3.1 Audit Keamanan Informasi

Audit Keamanan Sistem Informasi merupakan kegiatan yang dilkukan untuk mengetahui, menentukan dan memverifikasi apakah semua proses perlindungan kemanan yang ada sudah berjalan dengan baik dan sesuai kebijakan yang mangacu kepada standar kemanan yang telah ditetapkan (Ahmad, 2012)[8]. Hal-hal yang harus dipahamai dalam perencanaan kebijaksanaan (*policy*) keamanan jaringan komputer adalah *confidentiality* (kerahasiaan), *integrity* (integritas), *availability* (ketersediaan) dan *non-repudiation* (tindakan telah diawasi). Tujuan audit keamanan menurut Waber (Ron Waber, 1999) adalah sebagai berikut ini [9].

a. Meningkatkan keamanan aset perusahaan, informasi perusahaan seperti *hardware*, *software*, sumber daya manusia dan file data lainnya yang bersifat *sensitive* untuk mengidari penyalagunaan aset perusahaan.
b. Meningkatkan integritas data.
c. Meningkatkan efektivitas sistem.
d. Meningkatkan efisiensi sistem.

3.2 ISO/IEC 27002:2005

ISO 27000 merupakan sebuah standar dalam bidang keamanan informasi yang disediakan oleh *International Standards Organization* (ISO) dan *International Electrotechnical Commission* (IEC). ISO 27000 *Series* memberikan prosedur, panduan dan rekomendasi mengenai proses pengelolaan manajemen keamanan informasi, resiko dan kontrol dalam konteks SMKI (Sistem Manajemen Keamanan Informasi). ISO 27002 merupakan panduan praktitis dalam pengelolaan ISMS. SMKI adalah proses menetukan bagaimana cara mengelola informasi agar dapat dilindungi dan menjadi aman [10]. Struktur organisasi ISO/IEC 27002:2005 dibagi 2 bagian yaitu:

1. Klausul: *Mandatory Process Klausul* (pasal) syarat-syarat yang harus diterapkan dan dilaksanakan oleh organisasi yang menerapkan SMKI dengan menggunakan standar ISO 27001..
2. Annex A: *Security Control. Security control* adalah Dokumen panduan yang dijadikan sebagai sebagai acuan dalam menentukan *security contol* yang perlu diimplementasikan dalam SMKI.

Standar ISO/IEC 27002:2005 memiliki kontrol yang di implementasikan sebagai bagian dari ISMS organisasi yang terdiri dari 11 klausul dan 133 kontrol.

3.3 COBIT *5*

COBIT adalah kumpulan langkah praktis yang membantu para auditor atau pengguna untuk menjembatani kesenjangan antara resiko bisnis, *control* dan permasalahan teknis lainnya [10]. COBIT dikembangkan oleh IT Governance Institute, yang merupakan bagian dari *Information System Audit and Control Association* (ISACA). COBIT 5 terdiri dari area *Governance of Enterprise* IT yaitu Domain EDM (*Evaluate, Direct and Monitor*) sebanyak 5 proses dan *Management of Enterprise* IT yang terdiri dari APO (*Align, Plan and Organise*) 13 proses, BAI (*Build, Acquire and Implement*) 10 proses, DSS (*Deliver, Service and Support*) 6 proses, MEA (*Monitor, Evaluate and Assess*) 3 proses.

3.4 Pengukuran Tingkat Kematangan (*Maturity Level*)

Maturity model adalah metode untuk mengukur level pengembangan manajemen proses, yang berarti adalah mengukur sejauh mana kapabilitas manajemen tersebut. Seberapa bagus pengembangan atau kapabilitas manajemen tergantung pada tercapainya tujuan-tujuan COBIT yang telah diterapkan. Tingkat kemampuan pengelolaan TI pada skala *maturity* dibagi menjadi 6 level yaitu [11]:

a. *Incomplete Process*. Proses tidak diterapkan atau gagal mencapai keluaran yang ditetapkan..
b. *Level 1 Performed Process*. Proses telaH dijalankan dan berhasil mencapai tujuan.
c. *Level 2 Managed Process*. Telah dijalankan dan diimplementasikan dengan cara yang lebih teratur dan *outcome* yang dihasilkan telah ditetapkan, dikendalikan serta dijaga dengan baik.
d. *Level 3 Established Process.* Proses telah dijalankan sesuai aturan/proses yang ditetapkan dan mampu mencapai keluaran yang diharapkan.
e. *Level 4 Predictable Process*. Proses telah implementasikan sesuai dengan aturan yang telah ditetapkan untuk untuk mencapai *outcome* diharapkan.
f. *Level 5 Optimising* Proses yang ada secara teratur dan berkesinambungan ditingkatkan untuk mencapai tujuan yang diharapkan baik pada saat ini maupun masa depan.

4. Hasil dan Pembahasan

4.1 Identifikasi Tujuan *Bisnis (Bussiness Goals)*

Identifikasi tujuan bisnis merupakan proses memetakan antara tujuan bisnis organisasi dengan tujuan bisnis COBIT 5. Hasil identifikasi tujuan bisnis organisasi diperoleh 5 tujuan bisnis COBIT 5 yang sepadan dan melingkupi 4 perspektif. *Mapping* tujuan organisasi dengan tujuan bisnis COBIT 5 dapat dilihat pada Tabel 7.

Tabel 7. *Mapping* Tujuan Organisasi dengan Bussines *Goals* COBIT 5

Tujuan Organisasi	No.	Tujuan Bisnis	Perspektif Kinerja
1. Memperkuat kapasitas dan ketahanan seluruh pemangku kepentingan dalam pengurangan risiko bencana. 2. Memanfaatkan teknologi secara efektif dalam penanggulangan bencana. 3. Pusat data dan informasi kebencanaan sebagai penerima, pengolah, dan pendistribusi informasi. 4. Melindungi masyarakat dari bencana melalui diskriminasi peringatan dini dan pelayanan kegawatdaruratan. 5. Menyelenggarakan kerja sama dengan berbagai pihak dalam bidang TI dalam penanggulangan bencana secara terencana, terpadu, terkoordinir dan menyeluruh.	3	Pengelolaan resiko bisnis terutama pengamanan aset	Perspektif Keuangan
	4	Kepatuhan terhadap hukum dan peraturan eksternal	Perspektif Keuangan
	9	Strategi pengambilan keputusan berdasarkan informasi yang ada	Perspektif Pelanggan
	15	Kepatuhan terhadap kebijakan internal	Perspektif Internal
	17	Produk dan inovasi bisnis berdasarkan budaya	Perspektif Pembelajaran dan Pertumbuhan

4.2 *Identifikasi Tujuan TI (IT Goals)*

Proses identifikasi tujuan TI merupakan tahap memetakan *bussines goals* COBIT 5 yang telah diperoleh proses sebelumnya dengan IT *goals* COBIT 5. Hasil pemetaan *bussines goal* dengan *IT goal* dapat dilihat pada Tabel 8.

Tabel 8. Pemetaan *Business Goal* dengan IT *Goals*

No.	Tujuan Bisnis (*Business Goals*)	Tujuan TI (IT *Goals*)					
3	Pengelolaan risiko bisnis terutama pengamanan *aset*	04	10	16			
4	Kepatuhan terhadap kebijakan dan peraturan eksternal	02	10				
9	Strategi pengambilan keputusan berdasarkan informasi yang ada	01	14				
15	Kepatuhan terhadap kebijakan internal	02	10	15			
17	Produk dan inovasi bisnis berdasarkan budaya	09	17				

4.3 Identifikasi Proses TI *(IT Process)*

Tahap identifikasi proses TI merupakan proses pemetaan tujuan TI yang telah diperoleh sebelumnya dengan proses TI pada COBIT 5. Tujuan tahap Identifikasi proses TI dilakukan agar didapatkan proses apa yang ada atau dijalankan di dalam organisasi. Hasil pemetaan Tujuan TI dan Proses TI dapat dilihat dalam Tabel 9.

Tabel 9. Pemetaan Tujuan TI dengan Proses TI

Tujuan TI		Proses TI				
		EDM	APO	BAI	DSS	MEA
1	Penyelarasan TI dengan strategi bisnis	01, 02	01, 02, 03, 05 07, 08	01, 02		
2	Kepatuhan TI serta dukungan untuk kepatuhan peraturan serta hukum eksternal		01, 12 13	10	05	02
4	Menangani masalah TI yang terkait risiko bisnis		10, 12,13	01 06	01, 02, 03, 04, 05, 06	01 02, 03
9	Ketangkasan TI	04	01, 03, 04, 10	08		
10	Keamanan informasi, pemrosesan infrastruktur dan aplikasi		12, 13	06	05	

14	Ketersediaan informasi yang dapat dipercaya dan bermanfaat bagi pengambilan keputusan.		09, 13	04, 10	03, 04	
15	Kepatuhan TI serta terhadap kebijakan internal		01			01, 02
17	Pengetahuan, keahlian, dan inisiatif untuk inovasi bisnis.		01, 02, 04, 07,08	05, 08		

Tabel 9 merupakan hasil pemetaan antara proses TI dan tujuan TI yang memperoleh 31 proses TI. Hasil pemetaan yang terdapat dalam Tabel 9 kemudian dipadankan dengan proses pendukung TI yang ada pada COBIT 5 berdasarkan area tata kelola TI yang paling sesuai dengan proses yang diterapkan di lingkungan organisasi dan topik penelitian. Fokus audit yang dipilih dari 5 area tata kelola TI yaitu pada area *risk management*. Area *risk management* dipilih karena memiliki keterkaitan yang paling sesuai dengan fokus audit yang dilakukan yaitu mengenai audit dibidang keamanan TI. Proses TI yang bekaitan dengan *risk management* dapat dilihat pada Tabel 10.

Tabel 10. Area Tata Kelola *Risk Management*

Area Tata Kelola TI	**Proses Pendukung**	
	Primer	**Sekunder**
Risk Management	EDM01, EDM03, APO01, APO08, APO10, APO012, APO13, DSS01, DSS02, DSS03, DSS04, DSS05, MEA02, MEA03	APO02, APO03, APO07, BAI01, BAI02, BAI04, BAI08, BAI10, MEA01

Proses TI yang terdapat dalam Tabel 10 area tata kelola *risk management* dijadikan sebagai dasar dalam penyusunan kuesioner tingkat kepentingan. Fungsi dari kuesiner tingkat kepentingan adalah mengetahui persepsi pimpinan organisasi mengenai nilai kepentingan setiap proses TI yang ada dalam COBIT 5.

4.4 Hasil Kuesioner Tingkat Kepentingan

Penentuan tingkat kepentingan mengacu kepada tujuan penelitian, tujuan organisasi serta tingkat kekritisan bisnis proses yang diperoleh melalui kuesioner tingkat kepentingan. Proses TI yang terpilih dari hasil kuesioner tingkat kepentingan dapat dilihat dalam Tabel 11.

Tabel 11. Hasil Kuesiner Tingkat Kepentingan

Domain	**Proses TI**
DSS05	Mengelola servis keamanan.
APO13	Mengelola Keamanan.
EDM03	Memastikan Optimalisasi Risiko.

4.5 *Mapping* Proses TI COBIT 5 dengan ISO/IEC 27002:2005

Tahap yang dilakukan setelah proses TI COBIT 5 telah ditemukan yaitu melakukan *mapping* ke dalam standar ISO/IEC 27002:2005. Mapping ini dilakukan untuk disesuaikan dengan ruang lingkup audit yang dilaksanakan. Melalui mapping ini juga sekaligus menentukan daftar klausul dan kontrol keamanan yang digunakan dalam proses audit. *Mapping* proses TI COBIT 5 dengan ISO 27002 dapat dilihat dalam Tabel 12.

Tabel 12*. Mapping* ISO 27002 dengan COBIT 5

DOMAIN COBIT 5	ISO 27002:2005
DSS05 *Manage Security Services*. 5.1 Melindungi terhadap malware. 5.2 Mengelola jaringan dan keamanan konektivitas. 5.3 Mengelola keamanan endpoint. 5.4 Mengelola identitas pengguna dan *logical acces*. 5.5 Mengelola akses fisik ke aset TI. 5.6 Mengelola perangkat dan dokumen sensitive. 5.6 Memonitor keamanan infrastruktur	Klausul 11 Kontrol Akses 11.1 Persyaratan bisnis untuk akses kontrol 11.2 Manajemen akses *user* 11.3 Tanggung jawab pengguna (*user*) 11.4 Kontrol Akses jaringan 11.5 Kontrol Akses Sistem Operasi 11.6 Kontrol Akses Informasi dan aplikasi Klausul 9 Kemanan Fisik dan Lingkungan 9.1 Wilayah Aman 9.2 Keamanan Peralatan Klausul 6 Organisasi Kemanan Informasi 6.1 Organisasi Internal Keamanan Informasi 6.2 Organisasi Eksternal Keamanan Informasi Klausul 5 Kebijakan Keamanan Informasi 5.1 Kebijakan Keamanan Informasi
APO13 *Manage Security*. 13.1 Menetapkan dan memelihara ISMS. 13.2 Mendefinisikan dan mengelola rencana perlakuan resiko keamanan informasi. 13.1 Memantau dan meninjau ISMS.	
EDM03 *Ensure Risk Optimisation*. 3.1 Mengevaluasi manajemen risiko. 3.2 Manajemen *direct risk* 3.3 Memonitor manajemen risiko.	

Hasil dari *mapping* antara Proses TI COBIT 5 dengan ISO 27002 diperoleh 4 klausul yang memiliki kesepadanan yang terdiri dari 11 objektif kontrol.

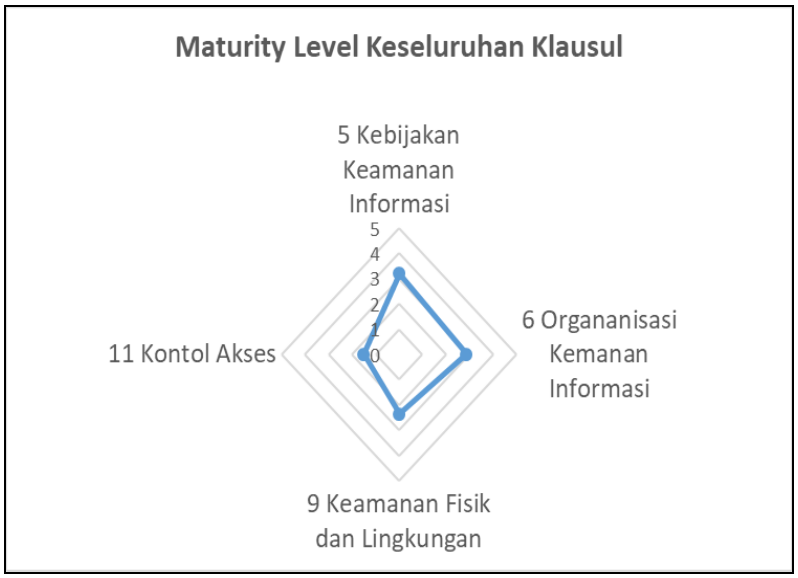
4.7 Hasil Tingkat Kematangan (*Capability Level*)

Hasil nilai *capability level* penerapan teknologi informasi di Lembaga X dari hasil kuesioner tingkat kematangan yang dihitung sesuai dengan model perhitungan yang telah dijelaskan dalam Tabel 5 untuk 4 klausul yang dipilih dapat dilihat dalam Tabel 13.

Tabel 13. Hasil *Capability Level*

Klausul	*Capability level*
5 Kebijakan Keamanan Informasi	3.24
6 Organisasi Keamanan Informasi	2.83
9 Keamanan Fisik dan Lingkungan	2.36
11 Kontol Akses	1.5
Total *Capability level*	**2.48**

Hasil nilai *capability level* yang terdapat pada Tabel 13 dapat direpresentasikan ke dalam diagram jaring yaitu seperti Gambar 2.



Gambar 2. Diagram Jaring Nilai Capabilty Level

Nilai *capability level* yang diperoleh untuk seluruh klausul yang dipilih adalah 2.48 yang masuk ke dalam kategori level 2: *Managed Process.* Level tersebut menunjukkan bahwa proses penerapan teknologi informasi telah dijalankan dan diimplementasikan dengan cara yang lebih teratur dan sudah mulai dikendalikan dan dijaga dengan baik.

4.8 Analisis Tingkat Kesenjangan

Analisis kesenjangan merupakan proses membandingkan kematangan teknologi informasi yang diterapkan oleh organisasi saat ini (*as-is*) berdasarkan hasil *capability level* yang telah diperoleh dengan kematangan teknologi informasi yang diharapkan (*to-be*). Analisis kesenjangan kematangan TI saat ini (*as-is*) dengan yang diharapkan (*to-be*) dapat dilihat dari dalam Tabel 14.

Tabel 14. Perbandingan Kematangan TI Saat Ini dan yang Diharapkan

Klausul	**Tingkat Kematangan**		
	Saat ini (*as-si*)	**Diharapkan (*to-be*)**	**Kesenjangan (GAP)**
Klausul 5	3.24	4	4 – 3.24 = 0.76
Klausul 6	2.83	4	4 – 2.83 = 1.17
Klausul 9	2.36	4	4 – 2.36 = 1.64
Klausul 11	1.5	4	4 – 1.5 = 2.5
Rata-rata (0.76 + 1.16 + 1.58 + 2.38)/4 = **1.51**			

Tabel 14 menunjukkan bahwa nilai tingkat kesenjangan antara tingkat kematangan saat ini (*as-is*) dengan yang diharapkan (to-*be*) untuk seluruh klausul keamanan yang dipilih adalah sebesar 1.51.

5. Kesimpulan

Tingkat kematangan teknologi informasi yang diterapkan di Lembaga X dari 4 klausul yang dipilih yaitu untuk klausul 5 kebijakan kemanan memperoleh nilai kematangan 3.24, klausul 6 organisasi kemanan informasi memperoleh nilai kematangan 2.83, klausul 9 keamanan fisik dan lingkungan memperoleh nilai kematangan 2.36, dan klausul 11 kontrol akses memperoleh nilai kematangan 1.5. Secara umum rata-rata nilai kematangan TI dari klausul yang dipilih adalah 2.48 yang masuk ke dalam kategori level 2 *Managed Process.* Level tersebut menunjukkan bahwa proses penerapan teknologi informasi DI Lembaga X telah dijalankan dan diimplementasikan dengan cara yang lebih teratur dan sudah mulai dikendalikan serta dijaga dengan baik.

Daftar Pustaka

[1] Peraturan Gubernur Bali Nomor 26 Tahun 2012. http://jdih.baliprov.go.id/produk-hukum/download/9024, Diakses tanggal 18 Agustus 2018.

[2] Y. C. N. Bless, G. M. Arya Sasmita, A. A. Kt. Agung Cahyawan, "Audit Keamanan SIMAK Berdasarkan ISO 27002 (Studi Kasus: FE UNUD)*", MERPATI*, vol. 2, no. 2, hh. 162-166, 2014.

[3] G. A. Theresia Krisanthi, I. M. Sukarsa, I. P. Agung Bayupati, "Governance Audit of Application Procurement Using Cobit Framework", *Journal of Theoretical and Applied Information Technology*, Vol. 50, No. 2, pp. 342-346, 2014.

[4] I. G. A. D. Sasmita Ratih, I. P. Agung Bayupati, I. M. Sukarsa "Measuring the Performance of IT Management in Financial Enterprise by Using COBIT", *International Journal Information Engineering and Electronic Business*, pp. 15-24, 2014.

[5] I. K. Adi Purnawan "Pedoman Tata Kelola Teknologi Informasi Menggunakan IT Governance Design Frame Work (Cobit) Pada PT. X", *Lontar Komputer*, Vol. 6, No. 3, pp. 200-203, 2015.

[6] I. P. A. Ambara Putra, I. M. Sukarsa, I. P. A. Bayupati "Audit TI Kinerja Manajemen PT. X Dengan Frame Work Cobit 4.1", *Lontar Komputer*, Vol. 6, No. 1, pp. 13-18, 2015.

[7] N. P. S. Merta Suryani. G. M. Arya Sasmita, I. K. Adi Purnawan "Audit of Accounting Information System Using COBIT 4.1 Focus on Deliver Support Domain*", Journal of Theoretical and Applied Information Technology*, vol.78, no.3, pp. 458-459, 2015.

[8] Amar Ahmad. Bakuan Audit Keamanan Informasi Kemenpora*.* Indonesia: Kementerian Pemuda dan Olahraga, 2012.

[9] Ron Waber. Information System Control and Audit. New Jersay: Prentice Hall, inc, 2000.

[10] ISO/IEC, Information-Technology-Security Techniques-Code of Practice for Information Security Management ISO/IEC 17799 (27002):2005-Final Draft, Switzerland: ISO/IEC JTC 1, 2014

[11] ISACA. A Business Framework for the Governance and Management of Enterprise IT. United States of America: ISACA, 2012.