Audit Keamanan SIMAK Berdasarkan ISO 27002 (Studi Kasus: FE UNUD)

Yulius C. N. Bless, Gusti Made Arya Sasmita, A. A. Kt. Agung Cahyawan

Jurusan Teknologi Informasi, Fakultas Teknik, Universitas Udayana

E-mail: neill.bless29@gmail.com, aryasasmita@yahoo.com, agungcahyawan@gmail.com

Abstrak

Keamanan sistem informasi merupakan sebuah bagian vital yang menjadi perhatian khusus bagi setiap orang yang aktif menggunakan teknologi internet sebagai alat komunikasi dan informasi. Institusi pendidikan seperti universitas, yang menggunakan sistem informasi sebagai salah satu cara dalam manajemen informasi terkait administrasi pegawai dan mahasiswa, maupun informasi lainnya guna menunjang proses pengambilan keputusan. Sistem Informasi Manajemen Akademik (SIMAK) di Fakultas Ekonomi Universitas Udayana berfungsi untuk manajemen data akademik mahasiswa. Informasi yang diolah dalam SIMAK haruslah memenuhi CIA (Confidentiality, Integrity, dan Availability). Audit dilakukan agar dapat diketahui tingkat kematangan sistem informasi saat ini. Standar dalam proses audit SIMAK menggunakan ISO/IEC 27002:2005 dan COBIT 4.1 untuk proses pemetaan dan penyusunan rekomendasi. Tingkat kematangan SIMAK saat ini adalah 3 atau Well Defined. Secara umum, tingkat kematangan ini dimaksudkan bahwa sudah terdapat prosedur yang standar dan telah didefinisikan secara baik, namun pelaksanaannya masih belum dilakukan secara rutin dan terstruktur.

Kata kunci: audit, COBIT 4.1, ISO/IEC 27002:2005, tingkat kematangan.

Abstract

Information system's security is one of an important part that being considered by people who actively use Internet technology as a main tool of communication and information. Especially for educational institutes such as universities, that has been using information system as a way for managing information related to administrative information for employees and students, as well as other information which is useful as a benchmark in making decision. Academic Management Information System in Faculty of Economy in Udayana University used to managing the students' academic stuff. The processes information in the system must meet with the CIA (Confidentiality, Integrity, and Availability). Audit is used to measuring the maturity level of the information system. Standard that has been used for the audit process is ISO/IEC 27002:2005 with COBIT 4.1 on mapping process and making recommendation. The maturity level of Academic Management Information System as-is 3 that means Well Defined. In commonly, the maturity level means that the standard procedure has been defined pretty well.

Keywords: audit, COBIT 4.1, ISO/IEC 27002:2005, Maturity Level

1. Pendahuluan

Universitas Udayana yang terletak di pulau Bali merupakan salah satu universitas negeri unggulan di Indonesia yang mengandalkan aplikasi web sebagai salah satu penunjang kebutuhan informasi. Aplikasi web yang menjadi penunjang kinerja ini adalah Sistem Informasi Manajemen Akademik atau disingkat SIMAK, yang merupakan sebuah sistem informasi yang

digunakan untuk manajemen administrasi data mahasiswa, perkuliahan, nilai mahasiswa dan lainnya.

SIMAK sebagai manajemen akademik mahasiswa perlu untuk menjamin keamanan serta privasi dan integritas data yang diolah, selain itu kinerja sistem informasi juga menjadi bagian penting yang harus diperhatikan sehingga sistem informasi dapat digunakan secara maksimal.

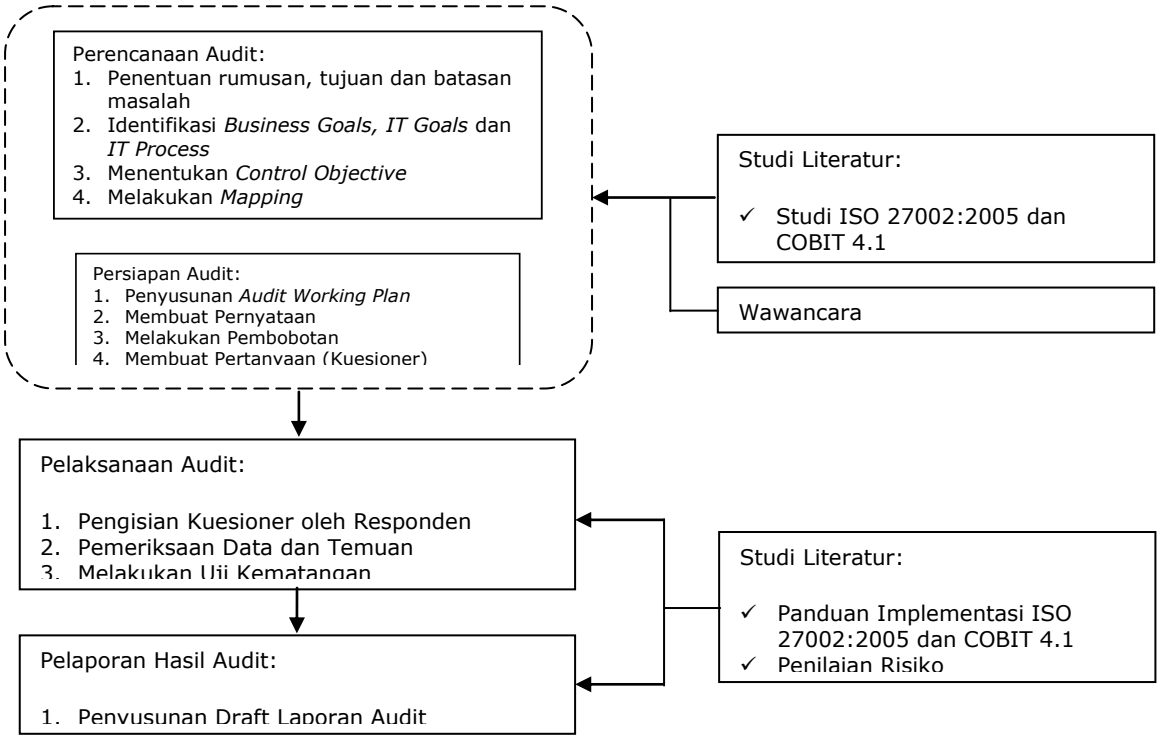
Agar SIMAK dapat terus berjalan sesuai dengan kebutuhan dan kegunaannya maka diperlukan proses pengukuran kinerja yang ditempuh melalui audit. “Agar audit keamanan sistem informasi dapat berjalan dengan baik diperlukan suatu standar untuk melakukan audit tersebut” [1]. Secara formal tidak ada acuan baku mengenai standar apa yang akan digunakan atau dipilih oleh perusahaan untuk melaksanakan audit keamanan sistem informasi sehingga dapat menggunakan standar sesuai dengan kebutuhan [2].

Audit pada SIMAK Fakultas Ekonomi Universitas Udayana (FE UNUD) menggunakan Standar ISO/IEC 27002:2005. Standar ISO/IEC 27002:2005 dipilih dengan pertimbangan bahwa standar ini sangat fleksibel dikembangkan tergantung pada kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis, jumlah pegawai dan ukuran struktur organisasi.

COBIT 4.1 juga digunakan dalam audit ini dalam penentuan proses bisnis, sehingga tujuan dan proses bisnis teknologi informasi pada SIMAK untuk selanjutnya dipetakan dengan ISO/IEC 27002:2005. Kerangka kerja COBIT 4.1 dipilih karena pemetaan dengan ISO/IEC 27002:2005 lebih luas dan dalam dibandingkan dengan kerangka kerja lain.

2. Metodologi Penelitian

Penelitian yang akan dilakukan merupakan proses audit terhadap Sistem Informasi Akademik (SIMAK) Fakultas Ekonomi Universitas Udayana. Secara garis besar, pelaksanaan audit ini akan terlihat seperti pada Gambar 1 mengenai desain tahapan proses audit.



Gambar 1. Desain Tahapan Proses Audit

Pelaksanaan audit dibagi menjadi empat bagian besar yaitu, perencanaan, persiapan, pelaksanaan dan pelaporan, dimana proses perencanaan dan persiapan dikerjakan pada waktu yang hampir bersamaan.

Model perhitungan yang digunakan untuk mengukur tingkat kematangan menggunakan SSE-CMM. SSE-CMM adalah *Capability Maturity Model* (CMM) untuk *System Security Engineering* (SSE). CMM adalah kerangka untuk mengembangkan proses, seperti proses teknis baik formal maupun informal.

Tahap perencanaan dilakukan penentuan proses bisnis, tujuan teknologi informasi dan proses teknologi informasi ditentukan melalui wawancara kepada bagian tertinggi yang mengatur jalannya SIMAK dengan tujuan agar penentuan proses bisnis sesuai dengan keadaan dan tujuan dari SIMAK. Wawancara ini juga bertujuan untuk mengetahui lebih jelas dan pasti mengenai visi dan misi dari SIMAK sehingga didapatkan objektif yang lebih terarah pada saat dilakukan audit.

Tahap persiapan audit, setiap pernyataan akan disesuaikan dengan proses bisnis yang telah dipetakan secara objektif yang telah dilakukan pada tahap perencanaan. Pembobotan setiap pernyataan disesuaikan dengan analisis risiko yang ditentukan pada saat wawancara dan pembuatan pertanyaan sesuai dengan panduan implementasi yang ada pada ISO/IEC 27002:2005 yang disesuaikan dengan keadaan pada SIMAK.

Pada tahap pelaksanaan audit, digunakan 3 (tiga) teknik pengumpulan data seperti berikut.

a) Wawancara
   Wawancara yang digunakan oleh peneliti dalam penelitian ini adalah wawancara tak terstruktur atau wawancara terbuka (*opened interview*). Wawancara ini dapat digunakan untuk mengumpulkan informasi yang tidak mungkin diperoleh melalui observasi.
b) Kuesioner/Angket
   Kuesioner/Angket yang digunakan berisi seperangkat pertanyaan yang disusun sesuai dengan standar ISO/IEC 27002:2005 dimana terdiri dari beberapa domain atau klausul. Setiap klausul terdiri dari beberapa pertanyaan dan setiap pertanyaan dijawab dengan cara memilih rentang angka 0 sampai 5 sesuai dengan jawaban yang dirasa sesuai dan benar oleh responden. Melalui hasil kuesioner ini, peneliti akan menggunakannya sebagai data dalam melakukan perhitungan tingkat kematangan/*maturity level* pada SIMAK untuk selanjutnya dihasilkan temuan dan rekomendasi guna pengembangan atau perbaikan.
c) Observasi
   Observasi dalam penelitian ini dilakukan untuk menyesuaikan hasil kuesioner terhadap keadaan pada sistem sehingga temuan dan rekomendasi yang dihasilkan menjadi lebih maksimal.

Tahap akhir audit yaitu pelaporan hasil audit dibuat dan disusun berdasarkan temuan di lapangan dan berisi rekomendasi perbaikan. Audit pada SIMAK akan berfokus hanya pada sistem informasi saja, sehingga narasumber untuk wawancara dan responden kuesioner merupakan pihak yang mengetahui dan mengerti secara menyeluruh kinerja dan kemampuan dari SIMAK.

3. Kajian Pustaka

3.1 Audit Sistem Informasi

Audit ialah proses atau aktivitas yang sistematik, independen dan terdokumentasi untuk menemukan suatu bukti (audit *evidence*) dan dievaluasi secara obyektif untuk menentukan apakah telah memenuhi kriteria pemeriksaan (audit) yang ditetapkan. Tujuan dari audit adalah untuk memberikan gambaran kondisi tertentu yang berlangsung di perusahaan dan pelaporan mengenai pemenuhan terhadap sekumpulan standar yang terdefinisi [3].

Tujuan utama dari audit sistem informasi adalah memberikan panduan pengelolaan, menyediakan manajemen, dan khususnya bagi petugas keamanan teknologi informasi sebagai pihak yang mendukung implementasi dan optimasi keamanan informasi.

3.2 ISO/IEC 27002:2005

ISO 27000 merupakan serangkaian standar yang disediakan oleh *International Standards Organization* (ISO) dan *International Electrotechnical Commission* (IEC) dalam penanganan keamanan informasi. Standard ISO 27000 Series secara spesifik telah ditetapkan oleh ISO untuk urusan yang terkait dengan *information security*.

ISO 27000 Series memberikan rekomendasi tentang *information security management, risks dan controls* di dalam konteks *Information Security Management System* (ISMS) secara keseluruhan [4]. ISO 27002 merupakan *Code of practice for ISMS.* Terkait dengan dokumen ISO 27001, yang mana berisi panduan praktis (*code of practice*) teknik keamanan informasi.

ISMS bukanlah produk melainkan suatu proses yang dilakukan untuk penentuan bagaimana *(how-to)* mengelola (merencanakan, mengimplementasikan, menggunakan, memonitor, memperbaiki dan mengembangkan) informasi agar menjadi aman.

Struktur organisasi ISO/IEC 27002:2005 dibagi 2 bagian yaitu:

1. Klausul: Mandatory Process
   Klausul (pasal) adalah persyaratan yang harus dipenuhi jika organisasi menerapkan ISMS dengan menggunakan standar ISO/IEC 27001.
2. Annex A: Security Control
   Security control adalah dokumen referensi yang disediakan dan dapat dijadikan rujukan untuk menentukan kontrol apa saja yang perlu diimplementasikan dalam ISMS. Terdiri dari 11 klausul kontrol keamanan, 39 objektif kontrol dan 133 kontrol.

3.3 COBIT 4.1

COBIT *(Control Objective for Information and Related Technology)* merupakan *a set of best practices (framework)* bagi pengelolaan teknologi informasi (TI). COBIT 4.1 menekankan kepatuhan pada peraturan, membantu organisasi untuk meningkatkan nilai yang diperoleh dari TI, memungkinkan penyelarasan dan menyederhanakan pelaksanaan kerangka kerja COBIT 4.1. Kerangka kerja atau *framework* COBIT 4.1 mendefinisikan kegiatan TI dalam 34 model proses dan mengelompokannya kedalam 4 domain, yaitu *Plan and Organise, Acquire and Implement, Deliver and Support,* dan *Monitor and Evaluate* [5].

3.4 SSE-CMM

SSE-CMM adalah *Capability Maturity Model* (CMM) untuk *System Security Engineering* (SSE). CMM adalah kerangka untuk mengembangkan proses, seperti proses teknis baik formal maupun informal. SSE-CMM terdiri dari dua bagian, yaitu:

1. Model untuk teknik keamanan proses, proyek dan organisasi, dan
2. Metode penilaian untuk mengetahui kematangan proses.

SSE-CMM mempunyai lima tingkat kemampuan untuk menunjukkan tingkat kematangan proses. Tingkat 0 menandakan tidak semua praktek dasar dilakukan. Tingkat 1 menandakan semua praktek dasar dilakukan namun secara informal, yang artinya tidak ada dokumentasi, tidak ada standar dan dilakukan secara terpisah. Tingkat 2 *planned & tracked* yang menandakan komitmen merencanakan proses standar. Tingkat 3 *well defined* yang berarti proses standar telah berjalan sesuai dengan definisi. Tingkat 4 dikendalikan secara kuantitatif, yang berarti peningkatan kualitas melalui *monitoring* setiap proses. Tingkat 5 ditingkatkan terus-menerus yang menandakan standar telah sempurna dan fokus untuk beradaptasi terhadap perubahan. Metode SSE-CMM digunakan dengan memberikan skor penilaian pada setiap area proses yang dipilih antara 0 sampai 5 untuk setiap area proses.

3.5 Pengumpulan Data

Data audit dihasilkan melalui wawancara, kuesioner dan observasi. Persiapan kuesioner dilakukan dengan membuat pernyataan berdasarkan kontrol keamanan yang telah ditentukan pada tahap perencanaan audit. Berikut contoh pernyataan audit dari kontrol keamanan Aturan dan Tanggung Jawab yang ada dalam klausul 8 Manajemen Sumber Daya Manusia.

Tabel 1. Contoh Pernyataan Pada Kontrol Keamanan Aturan dan Tanggung Jawab

Klausul: 8 Manajemen Sumber Daya Manusia	
Kategori Keamanan Utama: 8.1 Sebelum Menjadi Pegawai	
Kontrol Keamanan 8.1.1 Aturan dan Tanggung Jawab	
No.	**Pernyataan**
1	Terdapat aturan mengenai tanggung jawab informasi pada kontrak kerja pegawai.
2	Terdapat penandatanganan perjanjian kerahasiaan oleh seluruh pegawai yang menggunakan fasilitas pemrosesan informasi.

Pembobotan dilakukan terhadap setiap pernyataan, karena setiap pernyataan pada prosesnya memiliki resiko yang berbeda satu dengan lainnya jika tidak dilakukan. Pembobotan ditentukan dari panduan implementasi dan tingkat kepentingan setiap pernyataan yang ada menurut organisasi.

Tabel 2. Pembobotan Penilaian Resiko

Resiko	**Bobot**
Low	0,1 – 0,3
Medium	0,4 – 0,6
High	0,7 – 1,0

Setiap pernyataan yang telah diberikan bobot selanjutnya akan dibuat pertanyaan berdasarkan setiap pernyataan yang ada.

Tabel 3. Contoh Pertanyaan Pada Kontrol Keamanan Aturan dan Tanggung Jawab

Klausul: 8 Manajemen Sumber Daya Manusia	
Kategori Keamanan Utama: 8.1 Sebelum Menjadi Pegawai	
Kontrol Keamanan 8.1.1 Aturan dan Tanggung Jawab	
No. Pernyataan	**Pertanyaan**
1	▪ Sejauh mana isi kontrak kerja pegawai yang menyangkut tanggung jawab terhadap keamanan informasi?
2	▪ Sejauh mana penerapan penandatangan perjanjian kerahasiaan dengan calon pegawai telah dilaksanakan? ▪ Sejauh mana perjanjian kerahasiaan telah mempertimbangkan risiko keamanan informasi?

Kuesioner kemudian akan disebarkan dan hasil kuesioner akan dihitung untuk mengukur tingkat kematangan dengan cara:

1. Merekapitulasi skor nilai setiap pertanyaan
2. Menghitung rata-rata skor nilai setiap pernyataan
3. Menjumlahkan bobot setiap pernyataan dengan skor nilai rata-rata hasil rekapitulasi

Tabel 4. Contoh Kerangka Kerja Perhitungan Tingkat Kematangan

Kontrol Keamanan 8.1.1 Aturan dan Tanggung Jawab				
No.	Pernyataan	Bobot	Skor Nilai	Nilai
1	Terdapat aturan mengenai tanggung jawab informasi pada kontrak kerja pegawai.			
2	Terdapat penandatanganan perjanjian kerahasiaan oleh seluruh pegawai yang menggunakan fasilitas pemrosesan informasi.			

4. Hasil dan Pembahasan

4.1 Identifikasi *Business Goals* (Tujuan Bisnis)

Identifikasi tujuan bisnis dengan COBIT digunakan agar tujuan bisnis dari perusahaan dapat dipetakan dengan tujuan bisnis dari COBIT. Melalui hasil identifikasi berdasarkan tujuan bisnis perusahaan (misi perusahaan) dalam kasus ini adalah Divinkom Universitas Udayana, didapatkan 8 tujuan bisnis COBIT 4.1 yang sepadan dan melingkupi 4 perspektif.

Tabel 5. Padanan Misi Divinkom dengan Tujuan Bisnis COBIT 4.1

Misi Perusahaan	**No.**	**Tujuan Bisnis (*Business Goals*)**	**Perspektif Kinerja**
Misi dari Divinkom Universitas Udayana antara lain sebagai berikut: 1. Menyelaraskan implementasi TIK (Teknologi Informasi dan Komunikasi) dengan perencanaan strategi organisasi, 2. Menyesuaikan implementasi TIK (Teknologi Informasi dan Komunikasi) dengan kebutuhan *stakeholder*, 3. Membangun integrasi antar unit, 4. Penggunaan sumber daya secara efektif dan	2	Pengelolaan resiko bisnis yang terkait dengan teknologi informasi.	Perspektif Keuangan
	4	Peningkatan layanan dan orientasi terhadap pelanggan.	Perspektif Pelanggan
	5	Penawaran produk dan jasa yang kompetitif.	Perspektif Pelanggan
	6	Penentuan ketersediaan dan kelancaran layanan.	Perspektif Pelanggan
	9	Perolehan informasi yang bermanfaat dan handal untuk pembuatan keputusan strategis.	Perspektif Pelanggan
	11	Penurunan biaya proses.	Perspektif Proses

efisien, 5. Kualitas sistem yang tinggi.			Bisnis/Internal
	15	Peningkatan dan pengelolaan produktivitas operasional dan staf.	Perspektif Proses Bisnis/Internal
	17	Perolehan dan pemeliharaan karyawan yang cakap dan termotivasi.	Perspektif Pembelajaran dan Pertumbuhan

4.2 Identifikasi IT *Goals* (Tujuan TI)

Tujuan TI ditentukan agar didapatkan tujuan yang sesuai dengan kebutuhan menurut COBIT 4.1. Pada tahap ini tujuan bisnis dikaitkan dengan tujuan TI.

Tabel 6. Keterkaitan Tujuan Bisnis dan Tujuan TI SIMAK

No.	Tujuan Bisnis (*Business Goals*)	Tujuan Teknologi Informasi (IT *Goals*)						
2	Pengelolaan resiko bisnis yang terkait dengan teknologi informasi.	2	14	17	18	19	21	22
4	Peningkatan layanan dan orientasi terhadap pelanggan.	3	23					
5	Penawaran produk dan jasa yang kompetitif.	5	24					
6	Penentuan ketersediaan dan kelancaran layanan.	10	16	22	23			
9	Perolehan informasi yang bermanfaat dan handal untuk pembuatan keputusan strategis.	2	4	12	20	26		
11	Penurunan biaya proses.	7	8	13	15	24		
15	Peningkatan dan pengelolaan produktivitas operasional dan staf.	7	8	11	13			
17	Perolehan dan pemeliharaan karyawan yang cakap dan termotivasi.	9						

4.3 Identifikasi IT *Process* (Proses TI)

Pada tahap Identifikasi proses TI dilakukan agar didapatkan proses apa yang ada atau dijalankan di dalam perusahaan. Tujuan TI akan disesuaikan dengan proses TI yang menurut COBIT 4.1. Setelah didapatkan keterkaitan antara proses TI, selanjutnya akan dipilih proses pendukung TI pada COBIT 4.1 berdasarkan area tata kelola TI yang paling sesuai dengan proses dalam SIMAK.

Tabel 7. Proses Pendukung TI pada COBIT 4.1

Area Tata Kelola TI	Proses Pendukung	
	Primer	Sekunder
Risk Management	PO4, PO6, PO9, DS2, DS4, DS5, DS11, DS12, ME2, ME3, ME4	PO1, PO2, PO3, PO7, PO8, PO10, AI1, AI2, AI4, AI7, DS3, DS7, DS9, DS10, ME1
Performance Measurement	DS1, ME1, ME4	PO5, PO7, PO10, AI7, DS2, DS3, DS4, DS6, DS8, DS10

4.4 *Mapping* IT *Process* COBIT 4.1 Pada ISO/IEC 27002:2005

Mapping proses TI COBIT 4.1 ke dalam standar yang dipilih yaitu ISO/IEC 27002:2005. Audit keamanan SI yang dilakukan perlu disesuaikan dengan ruang lingkup audit yang dilaksanakan, sehingga *mapping* berikut sekaligus untuk menentukan daftar klausul dan kontrol keamanan yang akan digunakan dalam audit ini.

Tabel 8. Kontrol Keamanan ISO 27002 yang Digunakan

Klausul	Objektif Kontrol	Kontrol Keamanan
5	5.1	5.1.1, 5.1.2
6	6.1	6.1.1, 6.1.2, 6.1.3, 6.1.4, 6.1.5, 6.1.6, 6.1.7, 6.1.8
10	10.1, 10.4, 10.5, 10.6, 10.10	10.1.1, 10.1.3, 10.1.4, 10.4.1, 10.4.2, 10.5.1, 10.6.1, 10.6.2, 10.10.1, 10.10.2, 10.10.3, 10.10.4, 10.10.5, 10.10.6
11	11.1, 11.2, 11.4, 11.5, 11.6, 11.7	11.1.1, 11.2.1, 11.2.2, 11.2.3, 11.2.4, 11.4.1, 11.4.2, 11.4.4, 11.4.5, 11.4.6, 11.4.7, 11.5.1, 11.5.2, 11.5.3, 11.5.4, 11.5.5, 11.5.6, 11.6.1, 11.6.2, 11.7.1, 11.7.2
12	12.1, 12.2, 12.3, 12.4, 12.5, 12.6	12.1.1, 12.2.1, 12.2.2, 12.2.3, 12.2.4, 12.3.1, 12.3.2, 12.4.1, 12.4.2, 12.4.3, 12.5.1, 12.5.2, 12.5.3, 12.5.4, 12.6.1
13	13.1, 13.2	13.1.1, 13.1.2, 13.2.1, 13.2.2, 13.2.3

4.5 *Maturity Level* (Tingkat Kematangan)

Tingkat kematangan dari SIMAK Fakultas Ekonomi Universitas Udayana dihitung dengan menjumlahkan tingkat kematangan setiap klausul yang telah diperoleh.

Tabel 9. Tingkat Kematangan SIMAK FE UNUD

Klausul	***Maturity Level***
5 Kebijakan Keamanan	2,2
6 Organisasi Keamanan Informasi	2,06
10 Manajemen Komunikasi dan Operasi	3,47
11 Kontrol Akses	4,1
12 Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan	3,19
13 ***Manajemen Kejadian Keamanan Informasi***	3,19
Total *Maturity Level* = 3,035	

Total nilai tingkat kematangan diatas kemudian direpresentasikan ke dalam diagram jaring berikut.

Gambar 2. *Maturity Level* SIMAK

4.6 Analisis Kesenjangan (Gap)

Analisis kesenjangan tingkat kematangan dilakukan dengan cara membandingkan secara umum tingkat kematangan sistem informasi yang diharapkan (*to-be*) dengan tingkat kematangan sistem informasi saat ini (*as-is*).

Tabel 10. Perbandingan Tingkat Kematangan Saat Ini dan Yang Diharapkan

Domain	Tingkat Kematangan		
	Saat Ini	Diharapkan	Gap (Kesenjangan)
Klausul 5	2,2	4	4,0 – 2,2 = 1,8
Klausul 6	2,06	4	4,0 – 2,06 = 1,94
Klausul 10	3,47	4	4,0 – 3,47 = 0,53
Klausul 11	4,1	4	4,0 – 4,1 = -0,1
Klausul 12	3,19	4	4,0 – 3,19 = 0,81
Klausul 13	3,19	4	4,0 – 3,19 = 0,81
Rata-rata (1,8 + 1,94 + 0,53 + (-0,1) + 0,81 + 0,81) / 6 = **0,965**			

5. Kesimpulan

Berdasarkan penelitian yang telah dilakukan, maka dapat ditarik kesimpulan bahwa SIMAK Fakultas Ekonomi Universitas Udayana berada pada tingkat kematangan 3 atau *Well Defined*. Secara umum, tingkat kematangan ini dimaksudkan bahwa sudah terdapat prosedur yang standar dan telah didefinisikan secara baik.

Daftar Pustaka

[1] Tanuwijaya, H. dan Sarno, R. 2010. Comparation of CobiT Maturity Model and Structural Equation Model for Measuring the Alignment between University Academic Regulations and Information Technology Goals, International Journal of Computer Science and Network Security, VOL.10 No.6, June 2010.

[2] Rahardjo, Budi. Keamanan Sistem Informasi Berbasis Internet. Bandung: PT. Insan Indonesia. 2005.

[3] ISACA. CISA Review Manual. United States of America: ISACA. 2006.

[4] ISO/IEC 27002:2005, 2007. Information Technology-Security Techniques-Code of Practice for Information Security Management ISO/IEC 17799 (27002):2005 - Final Draft. Switzerland: ISO/IEC JTC 1.

[5] Information Technology Governance Institute (ITGI). COBIT 4.1: Control Objective, Management Guidelines, Maturity Models. United States of America: IT Governance Institute. 2007.