INTENSIF, Vol.2 No.1 February 2018
ISSN: 2580-409X (Print) / 2549-6824 (Online)
http://ojs.unpkediri.ac.id/index.php/intensif

Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standar ISO 27002: 2013 Menggunakan SSE-CMM

[1]Endang Kurniawan, [2]Imam Riadi
[1,2]Teknik Informatika, Universitas Islam Indonesia
[1,2]Jogyakarta, Indonesia
E-mail: [1]kurniawan1911@gmail.com, [2]imam.riadi@is.uad.ac.id

Abstrak— **Penelitian ini dilakukan untuk mengetahui tingkat keamanan informasi dalam sistem informasi akademik dan memberikan rekomendasi perbaikan dalam manajemen keamanan informasi. Berdasarkan hasil analisis, 13 kontrol obyektif dan 43 kontrol keamanan tersebar dalam 3 klausul, disimpulkan bahwa tingkat kematangan tata kelola sistem informasi keamanan pada sistem infromasi akademik adalah 2,51, yang berarti tingkat kematangan masih pada tingkat 2 namun mendekati level 3 atau well define.**

Kata Kunci— Academic Information Security, Security System, Maturity Level, SSE-CMM

Abstract— **The objective of this research is to find out the level of information security in the academic information system to give recommendations improvements in information security management. The method used is qualitative research method, which data obtained based on the results of questionnaires distributed to respondents with the Guttmann scale. Based on the analysis results, 13 objective controls and 43 security controls were scattered in 3 clauses. From the analysis, it was concluded that the maturity level of information system security governance was 2.51, which means the level of maturity is still at level 2 but is approaching level 3 well defined.**

Keyword— Academic Information Security, Security System, Maturity Level, SSE-CMM

I. PENDAHULUAN

Sistem Informasi Akademik telah banyak digunakan oleh hampir semua perguruan tinggi di Indonesia, hal ini dimaksudkan untuk memudahkan penyampaian informasi kepada peserta didik, dan staf pengajar serta tenaga administrasi dalam manajemen. Semakin banyak interaksi antara sistem dan pengguna, sistem yang lebih baik akan rentan disusupi atau dirusak oleh pihak-pihak yang tidak bertanggung jawab. Ini akan menjadi isu baru dalam hal keamanan.Sistem informasi akademik sebagai manajemen akademik mahasiswa perlu memastikan keamanan dan privasi dan integritas data yang diolah, disamping kinerja sistem

informasi juga menjadi bagian penting yang harus diperhatikan agar sistem informasi dapat dimanfaatkan secara optimal.

Masalah keamanan memicu mekanisme untuk mengendalikan akses ke jaringan untuk melindunginya dari penyusup [1]. Pada pengembangan perangkat lunak yang mendukung jaringan forensik adalah bagaimana menentukan metode yang tepat untuk memudahkan pengolahan data log [2]. Sistemnya bisa terus berjalan sesuai dengan kebutuhan dan kegunaannya. Hal ini diperlukan untuk mengolah pengukuran kinerja yang dilakukan melalui pemeriksaan. Agar pemeriksaan keamanan sistem informasi berhasil, diperlukan standar untuk melakukannya. Secara formal tidak ada acuan standar mengenai standar apa yang akan digunakan atau dipilih oleh organisasi untuk melakukan pemeriksaan keamanan sistem informasi sehingga dapat menggunakan standar sesuai kebutuhan.

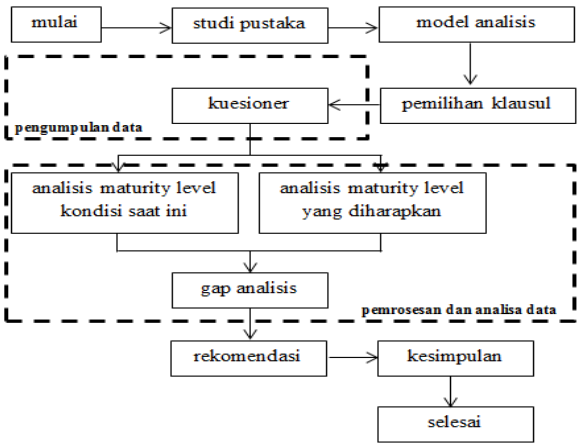
Keamanan informasi adalah suatu keharusan. Persoalannya penting karena jika informasinya bisa diakses oleh orang yang tidak bertanggung jawab maka ketepatan informasi akan diragukan bahkan bisa menyesatkan informasinya. Berikut ini adalah beberapa rumusan masalah yang ada dalam penelitian apakah sistem keamanan pada sistem informasi akademik yang digunakan sesuai dengan standar dan tingkat kesiapan sistem informasi akademik dalam penerapan standar keamanan informasi[3]. Selain itu peran apa yang membakukan keamanan sistem informasi dalam menjaga informasi tersimpan dari berbagai ancaman yang ada.

Tujuan dari penelitian ini adalah untuk mendapatkan hasil pengukuran yang akurat dalam hal keamanan informasi pada sistem informasi akademik dan peningkatan kualitas keamanan informasi sesuai dengan standar ISO 27002. Selain mengetahui tingkat kematangan sistem keamanan yang digunakan dalam sistem informasi akademik. Diharapkan hasil tersebut bisa dijadikan bahan pertimbangan untuk mempersiapkan langkah-langkah untuk memperbaiki sistem manajemen keamanan informasi

II. METODE PENELITIAN

Bab ini menjelaskan bagaimana melakukan penelitian, dimana ada rincian tentang materi atau bahan, peralatan, urutan langkah yang harus dilakukan secara sistematis, logis sehingga bisa dijadikan pedoman, jelas dan mudah untuk menyelesaikan permasalahan, analisis hasil dan kesulitan yang dihadapi. Dalam penelitian ini, metode yang digunakan adalah metode penelitian kualitatif, dimana data yang diperoleh berdasarkan hasil kuesioner yang disebarkan kepada responden. Dalam menyebarkan kuesioner penulis membuat daftar pertanyaan berdasarkan standar yang termuat dalam ISO 27002 tentang instruksi pelaksanaan manajemen keamanan

informasi yang terdiri dari 3 kriteria atau klausul. Lingkup pemeriksaan keamanan sistem informasi dilakukan dengan menentukan tujuan pengendalian yang akan digunakan. Dan sudah ada kesepakatan yang telah dibuat sebelumnya. Organisasi perlu melakukan pemilihan terhadap kontrol yang ada dengan memperhatikan kebutuhan organisasinya, bagaimana menerapkan dan menentukan risiko jika kontrol tersebut tidak terpenuhi. Urutan langkah penelitian pemecahan masalah dapat dilihat pada Gambar 1 dibawah ini :



Gambar 1. LANGKAH-LANGKAH PENELITIAN

Kontrol dirancang untuk memberikan kepastian bahwa tindakan manajerial dapat memastikan tujuan organisasi akan tercapai dan kejadian yang tidak diinginkan akan dicegah, dideteksi dan diperbaiki. Tabel 3 adalah pemetaan yang telah disepakati untuk dilakukan penelitian yang merujuk pada standar ISO 27002.

Tabel 1. KLAUSUL ISO 27002: 2013

Klausul	Keterangan
9	Akses Kontrol
11	Keamanan Fisik dan Lingkungan
14	Akuisisi Sistem Informasi, Pengembangan, dan Pemeliharaan

Data sekunder yang penulis gunakan dalam penelitian ini diperoleh melalui literatur atau studi literatur seperti buku, jurnal, dan prosiding. Dari hasil kuesioner yang telah disebarkan kemudian diolah untuk mengetahui tingkat kematangan dari keamanan sistem informasi sistem informasi akademik. Skala yang digunakan dalam kuesioner ini menggunakan skala Guttmann. Skala pengukuran dengan jenis ini, akan mendapatkan jawaban yang tegas, yaitu ya-tidak, benar-salah, tidak pernah-tidak pernah, positif-negatif dan lain-lain. Dalam penelitian ini menjawab kuesioner yang diberikan dua pilihan yaitu pilihan Ya dan jawaban Tidak. Dalam

perhitungan, jawaban Y (Ya) diubah menjadi nilai 1, dan jawaban T (Tidak) diubah menjadi nilai 0[4].

Perangkat lunak yang digunakan dalam perhitungan tingkat kematangan keamanan sistem informasi adalah Microsoft Excel. Setelah semua hasil kuesioner dimasukkan dalam tabel, maka dihitung tingkat kematangan setiap proses pada setiap klausul untuk setiap responden berdasarkan kuesioner yang disebarkan kepada responden yang dipilih untuk mengisi kuesioner. Dalam penelitian ini adalah 7 responden, seperti yang ditunjukkan pada Tabel 2.

Tabel 2. RESPONDEN

No	Keterangan	Jumlah
1	Kepala Divisi Teknologi Informasi	1
2	Asisten Kepala Divisi	1
3	Operator Sistem Informasi Akademik	2
4	Programmer	2
5	Senior Analis Pemrosesan Data Sistem Informasi Akademik	1
Jumlah Responden		7

Analisis dan interpretasi data dari hasil pengolahan data dan wawancara dengan pengelola sistem informasi akademik dapat digunakan sebagai temuan penelitian, berdasarkan hasil perhitungan tingkat kematangan atau maturity level[5], dapat dilihat gap dan dapat menentukan nilai yang diharapkan yang akan dibuat. rekomendasi dari masing-masing tujuan pengendalian yang perlu perbaikan. Model perhitungan yang digunakan untuk mengukur tingkat kematangan menggunakan SSE-CMM. SSE-CMM adalah Capability Maturity Model (CMM) untuk System Security Engineering (SSE)[5]. SSE-CMM menjelaskan karakteristik penting dari suatu proses rekayasa keamanan organisasi yang harus ada untuk memastikan teknik keamanan yang baik dengan tidak menganjurkan proses tertentu atau berurutan, namun mengambil praktek secara umum yang diamati dalam industri.

Untuk mengidentifikasi sejauh mana perusahaan atau organisasi telah memenuhi standard keamanan informasi yang baik, dapat menggunakan kerangka identifikasi yang direpresentasikan dalam sebuah tingkat kematangan yang memiliki tingkat pengelompokkan kapabilitas perusahaan, sebagaimana dijelaskan dalam Tabel 3 berikut ini :

Tabel 3. KRITERIA INDEX PENILAIAN PADA TINGKAT KEMATANGAN

Kriteria	Keterangan
0 – 0.50	Non-Existent
0.51 – 1.50	Initial / Ad Hoc
1.51 – 2.50	Repeatable But Invinitve
2.51 – 3.50	Define Process
3.51 – 4.50	Managed and Measurable
4.51 – 5.00	Optimized

Begitu tingkat kematangan proses saat ini ditetapkan dan target kematangan proses sudah ditentukan, maka gap antara kondisi saat ini dan target yang akan dicapai akan dianalisis dan diidentifikasi peluang dari gap yang akan dioptimalkan. Penjelasan dari teknik pengukuran dibuat dengan ukuran nominal untuk mengurutkan nilai dari yang paling rendah sampai yang tertinggi. Untuk SSE-CMM mempunyai lima tingkat kemampuan yang menunjukkan proses tingkat kematangan atau maturity level, berikut penjelasannya sebagaimana Tabel 4 dibawah ini:

Tabel 4. KRITERIA INDEX PENILAIAN PADA TINGKAT KEMATANGAN

	Kriteria	**Keterangan**
0	Existent	Perusahaan tidak mengetahui sama sekali proses teknologi informasi diperusahaannya
1	Initial / Ad Hoc	Terdapat bukti bahwa perusahaan mengetahui adanya hal-hal yangperlu diperhatikan. Namun demikian belum ada standarisasi proses, pendekatan dilakukan secara individual atau berdasarkan kasus. Pendekatan secara keseluruhan belum diorganisasikan dengan baik.
2	Repeatable but Intuitive	Proses telah dikembangkan dengan adanya prosedur yang sama dan digunakan oleh banyak orang dalam menyelesaikan tugas. Belum ada standarisasi prosedur untuk pelatihan secara formal ataupun komunikasi dan tangung jawab bergantung pada individu. Tingkat kepercayaan pada kemampuan individu sangat tinggi, sehingga kesalahan yang sama sering kali terjadi.
3	Define	Terdapat standarisasi prosedur dan telah didokumentasikan serta dikomunikasikan melalui pelatihan. Proses wajib ditaati sesuai standar. Penyimpangan sulit dideteksi. Prosedur yang digunakan belum canggih tetapi diformulasikan pada praktek.
4	Manage	Manajemen memonitor dan mengukur kepatuhan dengan prosedur dan mengambil tindakan terhadap proses yang tampaknya tidak dapat bekerja secara efektif. Proses berada di bawah peningkatan konstan dan memberikan latihan yang baik. Otomatisasi dan peralatan digunakan secara terbatas atau terfragmentasi
5	Optimized	Proses telah disempurnakan ke tingkat praktek yang baik, berdasarkan hasil dari perbaikan berkelanjutan dan model maturity dari perusahaan lain. TI digunakan secara terintegrasi untuk mengotomatisasi alur kerja, menyediakan alat-alat untuk meningkatkan kualitas dan efektivitas, membuat organisasi cepat beradaptasi

III. HASIL DAN PEMBAHASAN

Pada bagian ini akan dijelaskan hasil analisis terhadap implementasi dan pengukuran kinerja tingkat kematangan sistem informasi akademik yang diperoleh dari hasil kuesioner dan wawancara sesuai dengan kerangka kerja ISO / IEC 27002.

A. Hasil Maturity Level Masing-Masing Klausul

Berdasarkan hasil rekapitulasi kuesioner yang telah disebarkan kemudian dibuat rata-rata jawaban terhadap kuesioner yang dihitung berdasarkan klausul dan responden untuk mendapatkan tingkat kematangan, hasilnya adalah sebagai berikut:

1. Hasil Maturity level Klausul 9: Akses Kontrol

Berdasarkan perhitungan maturity level atau tingkat kematangan, nilai yang diperoleh pada klausul 9 tentang akses kontrol berada pada tingkat Initial / Ad Hoc dengan hasil 1,44 yang berarti tidak ada manajemen proyek, tidak adanya quality assurance, tidak adanya mekanisme manajemen perubahan, tidak ada dokumentasi, tidak adanya seorang ahli yang tahu segalanya tentang perangkat lunak yang dikembangkan, dan sangat bergantung pada kemampuan perseorangan. Tugas dan tanggung jawab keamanan informasi harus dilaksanakan oleh semua staf yang menjalankan sistem informasi akademik. Pihak ketiga tidak diizinkan untuk mengakses informasi non-resmi; pihak ketiga hanya dapat mengakses data umum, seperti ditunjukkan pada Tabel 5.

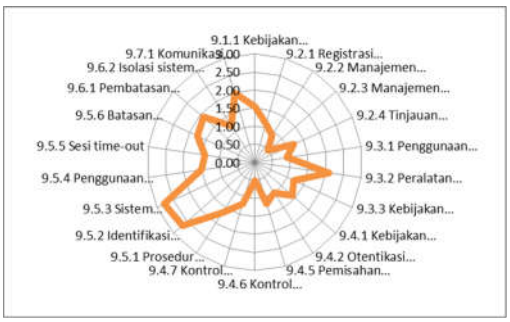
Tabel 5. HASIL PERHITUNGAN MATURITY LEVEL KLAUSUL 9: AKSES KONTROL

Kontrol Keamanan	Keterangan	Index
9.1.1	Kebijakan kontrol akses	1.54
9.2.1	Registrasi pengguna	1.10
9.2.2	Manajemen hak istimewa atau khusus	0.89
9.2.3	Manajemen password user	0.50
9.2.4	Tinjauan terhadap hak akses user	1.20
9.3.1	Penggunaan password	0.90
9.3.2	Peralatan pengguna yang tidak dijaga	2.10
9.3.3	Kebijakan clear desk dan clear screen	1.20
9.4.1	Kebijakan penggunaan layanan jaringan	1.40
9.4.2	Otentikasi pengguna untuk melakukan koneksi keluar	1.00
9.4.5	Pemisahan dengan jaringan	1.20
9.4.6	Kontrol terhadap koneksi jaringan	0.50
9.4.7	Kontrol terhadap routing jaringan	1.20
9.5.1	Prosedur log-on yang aman	1.67
9.5.2	Identifikasi dan otentifikasi user	2.67
9.5.3	Sistem manajemen password	2.78
9.5.4	Penggunaan utilitas sistem	1.50
9.5.5	Sesi time-out	1.40

Tabel 5. HASIL PERHITUNGAN MATURITY LEVEL KLAUSUL 9: AKSES KONTROL [LANJUTAN]

Kontrol Keamanan	Keterangan	Index
9.5.6	Batasan waktu koneksi	1.75
9.6.1	Pembatasan akses informasi	1.90
9.6.2	Isolasi sistem yang sensitif	1.20
9.7.1	Komunikasi dan terkomputerisasi yang bergerak	2.00
Rata-Rata		**1.44**

Hasil perhitungan tingkat kematangan pada klausul 9 dapat ditunjukkan dalam bentuk grafik, dapat dilihat pada Gambar 2 berikut ini :



Gambar 2. REPRESENTASI NILAI MATURITY LEVEL KLAUSUL 9 AKSES KONTROL

2. Hasil Maturity level Klausul 11: Keamanan Fisik dan Lingkungan

Berdasarkan perhitungan nilai tingkat kematangan yang diperoleh pada proses 11 tentang keamanan fisik dan lingkungan berada pada tingkat yang dapat diulang namun bersifat intuitif pada nilai posisi 2,47 yang berarti sistem informasi informasi keamanan informasi terkini harus dikembangkan menjadi tahap yang lebih baik. Sampai saat ini belum ada informasi proses analisis keamanan pada sistem informasi akademik, namun kebijakan yang dikeluarkan oleh manajemen merata ke semua komponen yang ada. Catatan penting atau informasi penting dilindungi oleh sistem untuk menghindari kerusakan dan kerugian, seperti yang ditunjukkan pada Tabel 6.

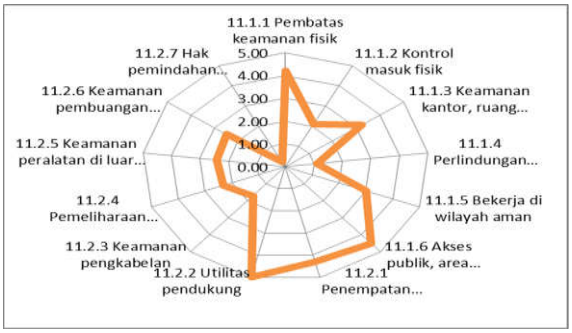
Tabel 6. HASIL PERHITUNGAN MATURITY LEVEL KLAUSUL 11: KEAMANAN FISIK DAN LINGKUNGAN

Kontrol Keamanan	Keterangan	Index
11.1.1	Pembatas keamanan fisik	4.14
11.1.2	Kontrol masuk fisik	2.10
11.1.3	Keamanan kantor, ruang dan fasilitasnya	3.23
11.1.4	Perlindungan terhadap serangan dari luar dan ancaman lingkungan sekitar	1.10
11.1.5	Bekerja di wilayah aman	3.00

Tabel 6. HASIL PERHITUNGAN MATURITY LEVEL KLAUSUL 11: KEAMANAN FISIK DAN LINGKUNGAN [LANJUTAN]

Kontrol Keamanan	Keterangan	Index
11.1.6	Akses publik, area pengiriman dan penurunan barang	3.50
11.2.1	Penempatan peralatan dan perlindunganya	4.30
11.2.2	Utilitas pendukung	2.34
11.2.3	Keamanan pengkabelan	1.71
11.2.4	Pemeliharaan peralatan	1.56
11.2.5	Keamanan peralatan di luar tempat kerja yang tidak diisyaratkan	2.41
11.2.6	Keamanan pembuangan atau pemanfaatan kembali peralatan	2.50
11.2.7	Hak pemindahan peralatan	0.25
Rata-rata		**2.47**

Hasil perhitungan tingkat kematangan pada klausul 11 dapat ditunjukkan dalam bentuk grafik, dapat dilihat pada Gambar 3 berikut ini :



Gambar 3. REPRESENTASI NILAI MATURITY LEVEL KLAUSUL 9 AKSES KONTROL

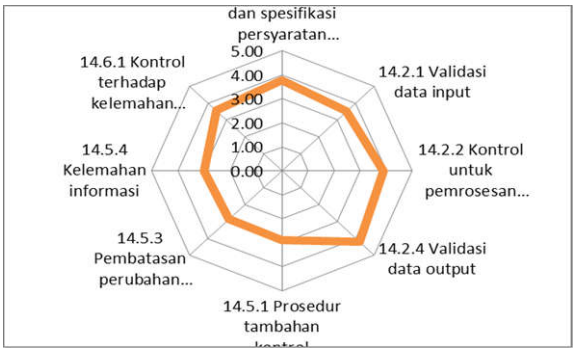
3. Hasil Maturity level Klausul 14: Akuisisi Sistem Informasi, Pengembangan, dan Pemeliharaan

Berdasarkan perhitungan nilai tingkat kematangan yang diperoleh pada proses 14 tentang akuisisi sistem informasi, pengembangan, dan pemeliharaan berada pada tingkat yang dikelola dan dapat diukur pada nilai posisi 3,63 yang berarti keamanan informasi adalah standar dan harus didokumentasikan kemudian dipublikasikan melalui pelatihan. Sistem informasi akademik merupakan sistem interaktif karena setiap validasi, sistem akan menjadi isu pesan yang berkaitan dengan aktivitas yang dimulai pengguna. Semua sistem informasi yang dirancang dan dibangun oleh Divisi Teknologi Informasi tanpa ada campur tangan pihak luar dan sumber, seperti yang ditunjukkan pada Tabel 7 berikut ini :

Tabel 7. HASIL PERHITUNGAN MATURITY LEVEL KLAUSUL 14: AKUISISI SISTEM INFORMASI, PENGEMBANGAN, DAN PEMELIHARAAN

Kontrol Keamanan	Keterangan	Index
14.1.1	Analisa dan spesifikasi persyaratan keamanan	3.85
14.2.1	Validasi data input	3.50
14.2.2	Kontrol untuk pemrosesan internal	3.90
14.2.4	Validasi data output	3.40
14.5.1	Prosedur tambahan kontrol	3.68
14.5.3	Pembatasan perubahan paket software	3.51
14.5.4	Kelemahan informasi	3.42
14.6.1	Kontrol terhadap kelemahan secara teknis (Vurnerability)	3.75
Rata-rata		**3.63**

Hasil perhitungan tingkat kematangan pada klausul 11 dapat ditunjukkan dalam bentuk grafik, dapat dilihat pada Gambar 4 berikut ini :



Gambar 4. REPRESENTASI NILAI MATURITY LEVEL KLAUSUL 14 AKUISISI SISTEM INFORMASI, PENGEMBANGAN, DAN PEMELIHARAAN

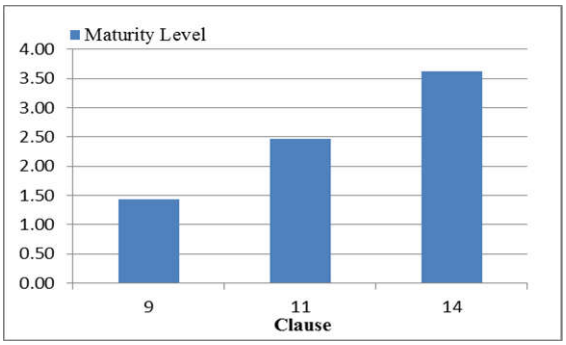
Setelah perhitungan maturity level pada klausul 9,11, dan 14 diperoleh berdasarkan standar ISO 27002, maka dapat dilihat nilai rata-rata tingkat kematangan atau maturity level pada sistem informasi akademik, sebagaimana dijelaskan dalam Tabel 8 dibawah ini :

Tabel 8. HASIL PERHITUNGAN MATURITY LEVEL

Kontrol Keamanan	Keterangan	Index	Level
9	Akses Kontrol	1.44	1
11	Keamanan Fisik dan Lingkungan	2.47	2
14	Akuisisi Sistem Informasi, Pengembangan, dan Pemeliharaan	3.63	3
Rata-rata maturity level		**2.51**	**3**

Hasil perhitungan untuk mendapatkan nilai rata-rata pengendalian keamanan informasi pada sistem informasi akademik sebesar 2,51 Dari nilai ini, dapat disimpulkan bahwa informasi keamanan berada pada level tiga, yang didefinisikan dengan baik atau rata-rata pengolahan

standar telah dijalankan. sesuai dengan prosedur. Berdasarkan hasil Tabel 8 diatas, untuk setiap proses dalam klausa, diperoleh grafik seperti pada Gambar 5 dibawah ini :



Gambar 5. PENGUKURAN GRAFIK PADA MATURITY LEVEL

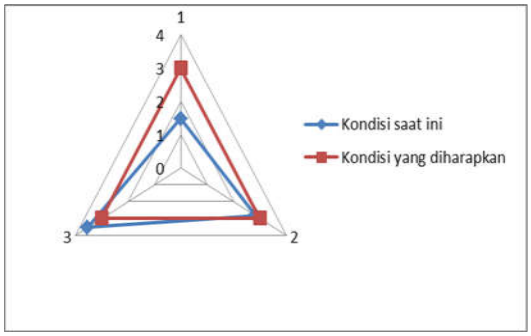
B. Analisis Gap Terhadap Tingkat Kematangan

Berdasarkan perhitungan tingkat kematangan keamanan informasi dari sistem informasi akademik saat ini bernilai 2,51 (define) masuk dalam level 3 dan diharapkan tingkat kematangannya adalah 5 (dioptimalkan). Alasannya adalah kesiapan organisasi dalam kebijakan, prosedur dan proses keamanan lapangan, dan keamanan informasi pengendalian akses, dapat dilihat Tabel 9 di bawah ini:

Tabel 9. HASIL PERHITUNGAN NILAI KESENJANGAN (GAP)

Klausul	Keterangan	Maturity Level		Gap
		Kondisi saat ini	Kondisi yang diharapkan	
9	Akses Kontrol	1.44	5	3.56
11	Keamanan Fisik dan Lingkungan	2.47	5	2.53
14	Akuisisi Sistem Informasi, Pengembangan, dan Pemeliharaan	3.63	5	1.37
Rata-rata				**2.49**

Berdasarkan Tabel 9, nilai kesenjangan antara kondisi saat ini dengan kondisi yang diharapkan untuk masing-masing klausa adalah klausul 9 bernilai 3.56, klausul 11 bernilai 2.53, dan pada klausul 14 bernilai 1,37. Dari hasil tersebut, kemudian dirata-rata untuk mendapatkan nilai gap atau kesenjangan maka nilai yang dihasilkan adalah 2.49 berarti nilai kesenjangan antara kondisi saat ini dengan kondisi yang diharapkan memiliki celah yang cukup besar, maka diperlukan penyesuaian masing-masing kontrol. Rekomendasi akan diberikan kepada masing-masing kontrol sehingga fokus pada peningkatan kontrol yang lemah. Rasio nilai tingkat kematangan saat ini dan nilai tingkat kematangan yang diharapkan digambarkan pada Gambar 8, berikut:



Gambar 6. HASIL PERHITUNGAN GAP ANALISIS

Seperti yang ditunjukkan pada Gambar 6, bahwa kondisi saat ini pada maturiry level diwakili oleh garis biru sementara pada garis merah adalah kondisi yang diharapkan. Dari gambar tersebut diatas terlihat bahwa maturity level pada kondisi yang diharapkan meningkat terus menerus yang menandakan standarnya telah sempurna dan fokus untuk beradaptasi terhadap perubahan. Tingkat seleksi sasaran ini didasarkan pada pertimbangan hasil analisis dimana nilai kontrol keamanannya tersebar diantara nilai 1 dan 3.

Dan dijelaskan bahwa tingkat keamanan saat ini dari nilai gap analisis terendah adalah 3,56 pada klausul 9 dengan tingkat kematangan keamanan informasi pada level 1,44 kondisi saat ini. Sedangkan pada klausul 14 dengan nilai tingkat kematangan mencapai 3,63 sehingga memiliki nilai kesenjangan terendah yaitu 1,37. Dengan demikian semakin tinggi nilai gap pada suatu klausul, semakin besar kemungkinan untuk terjadi pelanggaran keamanan dan semakin rendahnya nilai gap pada klausul maka semakin kecil kemungkinan terjadinya masalah keamanan.

C. Rekomendasi

Setelah melakukan analisis keamanan informasi sistem terhadap sistem informasi akademik, pengelola sistem informasi akademik dapat melakukan perbaikan sesuai dengan kontrol keamanan ISO 27002 yang telah ditetapkan. Adapun rekomendasi yang dapat diberikan pada klausul 9 pada akses kontrol , pengguna sistem informasi akademik secara berkala dapat merubah password dan memiliki kombinasi angka, huruf, ataupun simbol dengan panjang minimal 8 karakter agar password sulit dicuri oleh orang lain. Untuk klausul 11 tentang keamanan fisik dan lingkungan dapat menggunakan CCTV ataupun kunci akses masuk kedalam ruang server untuk mencegah pencurian, ataupun perusakan server oleh orang yang tidak berkepentingan..Dan untuk klausul 12 tentang akusisi, pengembangan dan pemeliharaan sistem informasi perlu dibuatkan prosedur untuk memeriksa keabsahan dari penggunaan sistem informasi akademik dari kerusakan ataupun kesalahan pengolahan data.

IV. KESIMPULAN DAN SARAN

Dari hasil analisis keamanan sistem informasi yang telah dilakukan pada sistem informasi akademik diperoleh hasil 2.51 yang dikategorikan pada level Define yang berarti bahwa mekanisme perencanaan pengadaan barang kebutuhan TI memiliki prosedur dan telah didokumentasikan serta dikomunikasikan melalui pelatihan. Sedangkan perencanaan anggaran, mekanisme pengembangan infrastuktur teknologi informasi dan menjaga hubungan kinerja vendor masih perlu ditingkatkan, prosedur yang digunakan belum sesuai standar tetapi diformulasikan pada dalam kegiatan sehari-hari. Dari kesimpulan diatas, maka disarankan untuk mencapai hasil yang optimal bagi pengelola sistem informasi akademik dapat melakukan perbaikan keamanan sistem informasi, dan prosedur keamanan sistem informasi agar ancaman terkait dengan keamanan sistem informasi dapat dibatasi.

DAFTAR PUSTAKA

[1] Hermaduanti, Ninki & Riadi, Imam. Automation framework for rogue access point mitigation in ieee 802.1X-based WLAN. *Journal of Theoretical and Applied Information Technology*. 93. 287-296. 2016

[2] Imam Riadi, Jazi Eko Istiyanto, Ahmad Ashari and Subanar, "Internet Forensics Framework Based-on Clustering" *International Journal of Advanced Computer Science and Applications(IJACSA)*, 4(12), 2013.

[3] Elachgar, H., Boulafdour, B., Makoudi, M., & Regragui, B. *Information security, 4TH wave*. 2012

[4] Tractenberg, R. E., Yumoto, F., Aisen, P. S., Kaye, J. A., & Mislevy, R. J. (2012). *Using the Guttman scale to define and estimate measurement error in items over time: The case of cognitive decline and the meaning of "points lost." PLoS ONE*, 7(2).2012

[5] Luhua, Z. (2012). Analysis of software capability maturity model (CMM). *In Proceedings of the 2012 National Conference on Information Technology and Computer Science*, CITCS 2012 (pp. 830–833)