Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standard ISO/IEC 27002:2013 Menggunakan SSE-CMM

Endang Kurniawan
14917118

Tesis diajukan sebagai syarat untuk meraih gelar Magister Komputer

Konsentrasi Forensika Digital

Program Studi Magister Teknik Informatika

Program Pascasarjana Fakultas Teknologi Industri

Universitas Islam Indonesia

2018

Lembar Pengesahan Penguji

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

Endang Kurniawan
14917118

Yogyakarta, 6 Februari 2018

Tim Penguji,

Dr. Imam Riadi, M.Kom
Ketua

Yudi Prayudi, S.Si., M.Kom.
Anggota I

Dr. Bambang Sugiantoro
Anggota II

Mengetahui,
Ketua Program Pascasarjana Fakultas Teknologi Industri
Universitas Islam Indonesia

Dr. R. Teduh Dirgahayu, ST., M.Sc.

Lembar Pengesahan Penguji

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

Endang Kurniawan
14917118

Yogyakarta, 6 Februari 2018

Tim Penguji,

Dr. Imam Riadi, M.Kom
Ketua

Yudi Prayudi, S.Si., M.Kom.
Anggota I

Dr. Bambang Sugiantoro
Anggota II

Mengetahui,
Ketua Program Pascasarjana Fakultas Teknologi Industri
Universitas Islam Indonesia

Dr. R. Teduh Dirgahayu, ST., M.Sc.

Abstrak

Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standard ISO/IEC 27002:2013 Menggunakan SSE-CMM

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

Sistem Informasi Akademik, Keamanan Sistem Informasi, Maturity Level, SSE-CMM

Abstract

Security Level Analysis Of Academic Information Systems Based On Standard ISO / IEC 27002: 2013 Using SSE-CMM

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.

Keywords

Acedemic Information System, Security System, Maturity Level, SSE-CMM

Pernyataan Keaslian Tulisan

Dengan ini saya menyatakan bahwa tesis ini merupakan tulisan asli dari penulis, dan tidak berisi material yang telah diterbitkan sebelumnya atau tulisan dari penulis lain terkecuali referensi atas material tersebut telah disebutkan dalam tesis. Apabila ada kontribusi dari penulis lain dalam tesis ini, maka penulis lain tersebut secara eksplisit telah disebutkan dalam tesis ini.

Dengan ini saya juga menyatakan bahwa segala kontribusi dari pihak lain terhadap tesis ini, termasuk bantuan analisis statistik, desain survei, analisis data, prosedur teknis yang bersifat signifikan, dan segala bentuk aktivitas penelitian yang dipergunakan atau dilaporkan dalam tesis ini telah secara eksplisit disebutkan dalam tesis ini.

Segala bentuk hak ciptayang terdapat dalam material dokumen tesis ini berada dalam kepemilikan pemilik hak cipta masing-masing. Apabila dibutuhkan, penulis juga telah mendapatkan izin dari pemilik hak cipta untuk menggunakan ulang materialnya dalam tesis ini.

Yogyakarta, Februari 2018

Endang Kurniawan, S.Kom., M.M.

Daftar Publikasi

Kurniawan, E., Riadi, I. (2018). Security Level Analysis Of Academic Information Systems Based On Standard ISO 27002 : 2013 Using SSE-CMM. *International Journal of Computer Science and Information Security, 16(1), pp. 139–147.*

<u>Publikasi yang menjadi bagian dari tesis</u>

Sitasi publikasi 1

Kontributor	Jenis Kontribusi
Endang Kurniawan	Mendesain eksperimen (60%) Menulis *paper* (70%)
Imam Riadi	Mendesain eksperimen (40%) Menulis dan mengedit *paper* (30%)

Halaman Kontribusi

Ada beberapa pihak terkait yang memiliki kontribusi dalam penyelesaian penyusunan penelitian tesis ini :

1. Bapak Dr. Imam Riadi, M. Kom., selaku Pembimbing dan Ketua Penguji yang telah memberikan arahan kepada penulis, sehingga penyusunan tesis ini dapat diselesaikan dengan baik dan tepat pada waktunya.
2. Bapak Dr. Bambang Sugiantoro, selaku anggota penguji yang telah memberikan bahan penelitian sehingga penelitian ini dapat diselesaikan.

Halaman Persembahan

Tesis ini penulis persembahkan untuk :

1. Ayah dan Ibu tercinta yang tak henti-hentinya mendukung penulis baik moril maupun materil serta memberikan doa dan semangat sehingga dapat menyelesaikan program pascasarjana di Universitas Islam Indonesia Konsenstrasi Forensika Digital.
2. Istri dan anak-anak yang penulis cintai yang telah memberikan doa dan dukungannya yang membuat penulis lebih semangat dalam menyelesaikan tesis ini.
3. Seluruh rekan-rekan magister teknik informatika angkatan X (sepuluh) yang membanggakan atas kerjasama dan bantuannya yang telah diberikan kepada penulis dalam penyelesaian tesis ini
4. Almamater tercinta Universitas Islam Indonesia.

Kata Pengantar

Puji syukur kehadirat Allah SWT yang telah melimpahkan rahmat dan inayahnya sehingga penulis dapat menyelesaikan laporan penelitian tesis yang berjudul Analisis Tingkat Keamanan Sistem Informasi Akademik Berdasarkan Standard ISO/IEC 27002:2013Menggunakan SSE-CMM.

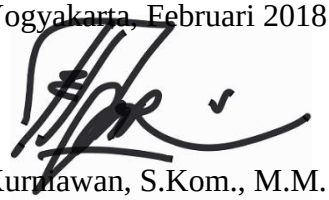
Tesis ini disusun guna memperoleh gelar Magister Komputer pada Program Studi Magister Teknik Informatika.

Keamanan sistem informasi saat ini merupakanhal penting karena secara tidak langsung dapat memastikan kontinuitas bisnis,mengurangi resiko, mengoptimalkan return of Investment dan mencari kesempatanbisnis. Dari hasil penilitian yang penulis lakukan membuktikan bahwa sistem informasi akademik yang diterapkan sangat membantu mahasiswa dalam mengakses informasi secara mudah dan membantu pemangku kepentingan dalam pengambilan keputusan secara cepat dan tepat.

Penulis mengucapkan terima kasih yang sebesar-besarnya atas bimbingan dalam proses penyusunan laporan tesis ini kepada :

1. Dr. R. teduh Dirgahayu, ST., M.Sc selaku Ketua Program Pascasarjana Fakultas Teknologi Industri Universitas Islam Indonesia
2. Dr. Imam Riadi, M.Kom selaku pembimbing dalam penyusunan tesis ini
3. Istri dan anak-anak tercinta, yang telah memberikan semangat dan dukungan sehingga tesis ini dapat diselesaikan.
4. Seluruh rekan-rekan angkatan X (sepuluh) Magister Teknik Informatika UII yang telah banyak membantu serta memberikan masukan, kritik serta saran kepada penulis.
5. Serta semua pihak yang tidak dapat disebutkan satu persatu yang telah banyak membantu dan mendukung selesainya penyusunan tesis ini.

Yogyakarta, Februari 2018



Endang Kurniawan, S.Kom., M.M.

Daftar Isi

Daftar Tabel

Daftar Gambar

BAB 1
Pendahuluan

1.1 Latar Belakang

Kebutuhan sistem informasi pada dewasa ini semakin menarik untuk dicermati. Semua bidang baik dalam bidang pendidikan, industri, pemerintahan, konsultan, dan lain sebagainya sangat bergantung terhadap sistem informasi. Dalam perancangannya, kebutuhan akan sistem informasi di lakukan dengan menganalisa kebutuhan fungsional dan kebutuhan non fungsional. Kebutuhan fungsional merupakan kebutuhan yang berisi proses-proses apa saja yang nantinya dilakukan oleh sistem. Sedangkan kebutuhan nonfungsional merupakan kebutuhan yang menitikberatkan pada properti prilaku yang dimiliki oleh sistem

Dalam dunia pendidikan, kebutuhan sistem informasi dapat diartikan sebagai kemampuan, syarat atau kriteria yang harus ada atau dipenuhi oleh sistem informasi, sehingga apa yang diinginkan pemakai dari sistem informasi dapat diwujudkan.

Sistemi informasi akademik, sudah banyak digunakan oleh hampir semua perguruan tinggi di Indonesia khususnya, hal ini dimaksudkan untuk mempermudah penyampaian informasi kepada peserta didik, dan tenaga pengajar maupun tenaga administrasi dalam pengelolaannya. Semakin banyak interaksi antara sistem dan pengguna maka sistem akan menjadi rentan untuk disusupi atau dirusak oleh pihak-pihak yang tidak bertanggung. Hal ini akan menjadi masalah baru dari sisi keamanan.

Rahardjo (2005: 1) menyatakan bahwa masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Terjadinya masalah keamanan dapat menimbulkan kerugian bagi organisasi misalnya kerugian apabila sistem informasi tidak bekerja selama kurun waktu tertentu, kerugian apabila ada kesalahan data atau informasi dan kehilangan data. Sementara itu, selama penerapan aplikasi sistem informasi akademik ini telah terjadi beberapa permasalahan antara lain sering ditemukan terjadinya kebocoran informasi pada karyawan yang tidak berhak atas informasi tersebut dan hal tersebut dapat mengancam kerahasiaan organisasi. Selain itu, dikhawatirkan dapat merambat pada terjadinya penyalahgunaan informasi yang merugikan organisasi dalam persaingan dengan

para kompetitor. Kendala lain yang ditemukan adalah kerusakan peralatan sistem informasi yang dapat menyebabkan hilangnya data perusahaan dan sistem yang sering hang. Di samping itu, terjadi gangguan-gangguan yang menyebabkan kekacauan antara lain kerusakan data, file-file yang tidak bisa dibuka, dan lain-lain.Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi bagaimana penyusup dapat masuk kedalam sistem melalui jaringan yang tersedia.(Hermaduanti, et al, 2016).

Selama ini sistem infromasi akademik yang dikelola oleh PUSKOM-PSI belum pernah melakukan analisa penyebab terjadinya permasalahan tersebut dan PUSKOM-PSI tidak mengetahui sampai di mana tingkat keamanan sistem informasi yang milikinya.Oleh karena itu PUSKOM-PSI membutuhkan evaluasi keamanan sistem informasi untuk menjaga keamanan sistem informasi yang dimilikinya.Analisa keamanan sistem informasi dapat dilakukan dengan pemeriksaan keamanan sistem informasi (Asmuni dan Firdaus, 2005: 23). Keamanan informasi ditujukan untuk menjaga aspek kerahasiaan (Confidentiality), keutuhan (Integrity) dan ketersediaan (Availability) dari Informasi (ISO/IEC 27002, 2005: 1).

Sistem dapat terus berjalan sesuai dengan kebutuhan dan kegunaannya maka diperlukan proses pengukuran kinerja yang ditempuh melalui pemeriksaan. Agar pemeriksaan keamanan sistem informasi dapat berjalan dengan baik diperlukan suatu standar untuk melakukannya. (Rosmiati , et al, 2016).

Agar dalam pemeriksaan keamanan sistem informasi dapat berjalan dengan baik diperlukan suatu standar untuk melakukan audit tersebut (Tanuwijaya & Sarno, 2010). Menurut (Syafrizal, 2007) tidak ada acuan baku mengenai standar apa yang akan digunakan atau dipilih oleh perusahaan untuk melaksanakan pemeriksaan keamanan sistem informasi. Pemilihan standar ditentukan oleh PUSKOM-PSI untuk menggunakan standar ISO 27002.

Salah satu alasan memilih menggunakan ISO 27002 ini karena PUSKOM-PSI telah menggunakan standarisasi ISO tetang sistem manajemen mutu yaitu ISO 9001: 2008, selain itu dengan pertimbangan bahwa standar ini sangat fleksibel dikembangkan tergantung pada kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis, jumlah pegawai dan ukuran struktur organisasi.

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.

Dengan adanya pemeriksaan keamanan sistem informasi pada sistem informasi akademik dapat mengetahui kelemahan-kelemahan sistem yang menjadi penyebab permasalahan keamanan informasi yang selama ini terjadi. Selain itu, pemeriksaan ini dapat mengukur tingkat keamanan sistem informasi yang dimiliki pihak perguruan tinggi. Dari hasil pemeriksaan, maka dapat merekomendasikan tentang perbaikan yang harus dilakukan untuk meningkatkan keamanan informasi pada sistem informasi akademik, serta menjadi pertimbangan untuk memperoleh ISMS certification dengan standar ISO 27002 pada masa mendatang.

1.2 Perumusan Masalah

Berdasarkan penjelasan pada latar belakang, maka perumusan masalah yang di dapat adalah sebagai berikut :

a. Apakah sistem keamanan pada sisteminformasi akademik yang digunakan sudah sesuai dengan standard ISO 27002, dan sejauh mana kesiapan sistem informasi akademik dalam penerapan standar keamanan informasi ?
b. Bagaimanakah peranan standarisasi keamanan sistem informasi dalam menjaga informasi yang tersimpan dari berbagai ancaman yang ada ?
c. Bagaimana menyusun hasil pemeriksaan keamanan sistem informasi akademik berdasarkan standar ISO 27002 ?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut :

a. Klausul ISO 27002 : 2013 yang digunakan sesuai kesepakatan dengan pimpinan PUSKOM-PSI sebagai pengelola dari sistem informasi akademik, yaitu:
    1) Klausul 9 : Kontrol Akses
    2) Klausul 11 : Keamanan Fisik dan Lingkungan
    3) Klausul 14 : Akuisisi Sistem Informasi, Pengembangan, dan Pemeliharaan

    Selain kesepakatan diatas, berdasarkan permasalahan yang dijelaskan dalam latar belakang sebelumnya yang menyangkut permasalahan sumber daya manusia, keamanan fisik dan lingkungan, operasional sistem informasi, kontrol akses, dan kejadian-kejadian yang menyangkut keamanan informasi pada data center.

b. Sistem Informasi yang diperiksa adalah sistem informasi akademik yang dikelola oleh PUSKOM-PSI.

1.4 Tujuan Penelitian

Untuk melihat sejauh mana sistem informasi akademik yang dikelola oleh PUSKOM-PSI dapat berjalan dengan baik sesuai dengan tujuan organisasi maka dilakukan analisa untuk dipakai sebagai alat bantu dalam pemeriksaan tentang adanya kemungkinan penyimpangan pada sistem yang telah ditentukan dan memberikan umpan balik kepada pihak manajemen atas pemanfaatan TI.

Beradasarkan perumusan masalah yang sudah dijelaskan sebelumnya, maka tujuan yang ingin dicapai dalam penelitian ini adalah :

a. Mendapatkan hasil pengukuran yang akurat dalam hal keamanan informasi pada sistem informasi akademik dan meningkatkan kualitas keamanan informasi sesuai standar ISO 27002.
b. Mengetahui tingkat kematangan sistem keamanan yang digunakan pada sistem informasi akademik.
c. Menyusun hasil analisa keamanan sistem informasi akademik berdasarkan standar ISO 27002 ke dalam laporan hasil analisa yang berupa temuan dan rekomendasi yang dapat digunakan untuk perbaikan dan peningkatan keamanan sistem pada sistem informasi akademik.

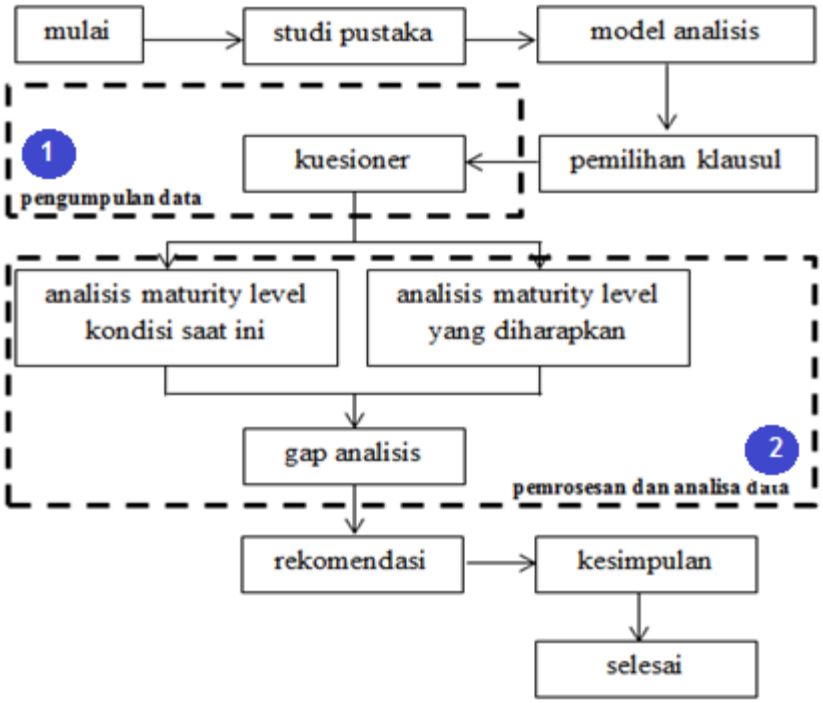
1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah :

a. Meningkatkan keamanan pada layanan sistem informasi akademik
b. Bagi pihak pengelola system informasi akademik tidak perlu mengeluarkan biaya untuk menyewa suatu perusahaan yang menjual jasa keamanan, dan dapat mengembangkan dan melakukan perbaikan secara mandiri dari hasil pemeriksaan yang sudah dilakukan.
c. Bagi penulis dapat menambah pengetahuan dan pemahaman tentang standard keamanan sistem informasi.
d. Bagi mahasiswa penelitian ini bermanfaat untuk keamanan dan kenyamanan dalam menggunakan layanan dihalaman system informasi akademik.

1.6 Metodologi Penelitian

Penelitian yang akan dilakukan merupakan proses analisis terhadap sistem informasi akademikdari awal kegiatan hingga hasil akhir yang didapat, sebagaimana terlihat dalam Gambar 1.1 berikut ini :



Gambar 1.1 Tahapan Metodologi Penelitian

1.7 Review Penelitian

Irmawati Carolina, dalam penilitiannya yang berjudul pengukuran tingkat kematangan tata kelola teknologi informasi berdasarkan 34 kerangka kerja Cobit 4.1 dimana sudah dipublikasikan dalam jurnal SWABUMI, Vol.5 Maret 2017 mengatakan bahwa pada implementasi teknologi informasi ditempat penelitian untuk mencapai tingkat kematangan pada level 3 (define process) berdasarkan visi, misi, tujuan dan arah pengembangan perusahaan prosedur sudah standard dan terdokumentasi dan dikomunikasikan melalui pelatihan, tetapi pelaksanaannya diserahkan pada tim untuk mengikuti proses tersebut, sehingga penyimpangan bisa diketahui, prosedurnya disempurnakan untuk formalitas praktek yang ada.

Rosmiati, dalam jurnal IJCA yang dipublikasikan pada volume 141 – No.8, May 2016 menyimpulkan bahwa prosedur yang terkandung dalam pengiriman dan dukungan pengendalian telah dikembangkan dalam proses menangani tugas, dan diikuti oleh semua orang yang terlibat. Tidak ada pelatihan dan komunikasi prosedur standard.

Tanggungjawab diserahkan keapda masing-masing karyawan.Kepercayaan karyawan sangat tinggi, sehingga bisa terjadi kesalahan.

Muhammad Ikhsan, dalam penelitiannya di STFB (Sekolah Tinggi Farmasi Bandung) mengenai keamanan sistem informasi akademik yang dipublikasikan dalam jurnal e-Proceeding of Engineering : Vol.3, No.3 December 2016 menemukan beberapa kelemahan terhadap sistem informasi akademik. Dengan menggunakan model CMMI, Berdasarkan hasil analisis risikodalampenelitian ini, ditentukan 16 kontrol objektif dan 57 kontrol keamanan yang tersebar dalam 4 klausal ISO 27001.Darihasil audit dapat disimpulkan bahwa nilai tingkat kematangan tata kelola keamanan sistem informasi STFB adalah2,5 yang berarti tingkat keamanan masih berada pada level 2 planned and tracked (sudah direncanakan dan dilacaksecara aktif) namun telah mendekati level 3 well defined (telah didefinisikan dengan baik).

Herman Afandi, dalam penelitiannya yang berjudul audit keamanan informasi menggunakan ISO 27002 pada perusahaan data center telah mempublikasikan hasil penelitian di jurnal Tim Darmajaya Vol. 01 No. 02 Oktober 2015 menemukan beberapakelemahan-kelemahan aturan dan prosedur keamanan sistem informasi mengakibatkan perusahaan rentan terhadap ancaman keamaman informasiyang dapat menyebabkan timbulnya resiko-resiko, antara lain: penyalah gunaaninformasi, kekacauan pada internal perusahaan, dan hilangnya data perusahaan yangakan merugikan perusahaan itu sendiri.

Adi Supriyatna, pada jurnal prosiding seminar nasional aplikasi sains dan teknologi (SNAST) 2014, di Yogjakarta pada tanggal 15 November 2014 mengatakan bahwa keamanan informasi merupakan suatu hal yang wajib diperhatikan. Masalah tersebut pentingkarena jika informasi dapat diakses oleh orang yang tidak bertanggung jawab maka keakurataninformasi tersebut akan diragukan bahkan bisa menjadi informasi yang menyesatkan. Dari hasil penelitian yang telah dilakukan ditemukan bahwa tingkat kematangan keamanan informasi sisteminformasi akademik adalah berada pada rata-rata level 1 berarti bahwa saat ini keamanan informasisistem informasi akademik masih perlu diperbaiki karena masih berada di bawah level 3. Namun adabeberapa klausa yang memiliki nilai di atas 3 yaitu klausa ke-6, klausa ke-7 dan klausa ke-8 yangberarti sudah memenuhi standar BS-7799.

Dalam penelitian terdahulu jika disusun dalam bentuk tabel dapat terlihat pada table 1.1 berikut ini :

Tabel 1.1 Literatur review terhadap penelitian sebelumnya

No	Paper Utama	Information Security Management	Framework	Pengujian
1.	**Irmawati Carolina / 2017**	-	COBIT 4.1	Pengukuran Tingkat Kematangan Tata Kelola Ti Berdasarkan 34 Kerangka Kerja
2.	**Rosmiati / 2016**	ISO 27001	COBIT-SSE CMM	Pengukuran Implementasi IT diperusahaan
3.	**Muhammad Ikhsan / 2016**	ISO 27001	CMMI	Audit terhadap keamanan sistem informasi STFB Bandung dengan menggunakan SNI ISO 27001:2009 berbasis risiko sebagai bahan referensi penentuan kebijakan pengelolaan keamanan informasi Sistem Informasi Akademik (SIA) STFB yang akan datang
4.	**Herman Afandi / 2015**	ISO 27002	CMMI	Pengukuran Kemanan Informasi Menggunakan ISO 27002 Perusahaan Data Center
5.	**Adi Supriyatna / 2014**	BS7799	SSE-CMM	Pengukuran kualitas keamanan sistem informasi akademik dan kematangan sistem keamanan yang digunakan
Usulan Penelitian				
Solusi yang diusulkan		Dengan adanya analisa dari proses keamanan sistem informasi pada sistem informasi akademik dapat mengetahui kelemahan-kelemahan sistem yang menjadi penyebab permasalahan keamanan informasi yang selama ini terjadi. Selain itu, analisis ini dapat mengukur tingkat keamanan sistem informasi yang dimiliki organisasi. Dari hasil pemeriksaan, maka dapat merekomendasikan tentang perbaikan yang harus dilakukan untuk meningkatkan keamanan informasi pada sistem informasi akademik, serta menjadi pertimbangan untuk memperoleh ISMS certification dengan standar ISO 27002 pada masa mendatang		

1.8 Sistematika Penulisan

Untuk mempermudah proses pembahasan dalam penelitian yang dilakukan, maka dibuat sistematika penulisan pada penelitian ini :

BAB I PENDAHULUAN

Pendahuluan merupakan pengantar terhadap permasalahan yang akan dibahas. Didalamnya menguraikan tentang gambaran suatu penelitian yang terdiri dari latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, manfaat penelitian, metodologi penelitian, review penelitian, serta sistematika penulisan.

BAB II KAJIAN TEORI

Pada Bab ini menjelaskan teori-teori yang digunakan untuk memecahkan masalah dalam penelitian ini.Teori yang dibahas pada bagian ini merupakan teori yang berhubungan keamanan sistem informasi, ISO 27002, dan Pengukuran Tingkat Kematangan (SSE-CMM), dan tahapan-tahapan dalam melakukan analisis.

BAB III METODOLOGI PENELITIAN

Bab ini membahas tentang langlah-langkah dalam penelitian analisis keamanaan sistem informasi, model simulasi, skenario analisis, dan penyusunan laporan pemerikasaan keamanan informasi.

BAB IV PEMBAHASAN

Hasil dan Pembahasan, berisi tentang pembahasan penyelsaian masalah yang diangkat, evaluasi, dan penentuan hasil analisis berupa rekomendasi.

BAB V KESIMPULAN DAN SARAN

Simpulan dan Saran, memuat kesimpulan-kesimpulan dari hasil penelitian dan saran-saran yang perlu diperhatikan berdasar keterbatasan yang ditemukan dan asumsi-asumsi yang dibuat selama melakukan penelitian dan juga rekomendasi yang dibuat untuk pengembangan penelitian selanjutnya.

BAB 2
Tinjauan Pustaka

2.1 Analisis

Dalam Kamus Besar Bahasa Indonesia karangan Suharso dan Ana Retnoningsih (2005), analisis adalah penyelidikan terhadap suatu peristiwa (karangan, perbuatan dan sebagainya) untuk mengetahui keadaan yang sebenarnya (sebab musabab, duduk perkara dan sebagainya).

Dalam Kamus Besar Bahasa Indonesia Departemen Pendidikan Nasional (2005) menjelaskan bahwa analisis adalah penyelidikan terhadap suatu peristiwa untuk mengetahui keadaan yang sebenarnya.

Sedangkan dalam kamus besar ekonomi pengertian Analisis yaitu melakukan evaluasi terhadap kondisi dari pos-pos atau ayat-ayat yang berkaitan dengan akuntansi dan alasan-alasan yang memungkinkan tentang perbedaan yang muncul.

Dalam Kamus Bahasa Indonesia Kontemporer karangan Peter Salim dan Yenni Salim (2002) menjabarkan pengertian analisis sebagai berikut :

a. Analisis adalah penyelidikan terhadap suatu peristiwa (perbuatan, karangandan sebagainya) untuk mendapatkan fakta yang tepat (asal usul, sebab, penyebab sebenarnya, dan sebagainya).
b. Analisis adalah penguraian pokok persoalan atas bagian-bagian, penelaahan bagian-bagian tersebut dan hubungan antar bagian untuk mendapatkan pengertian yang tepat dengan pemahaman secara keseluruhan.
c. Analisis adalah penjabaran (pembentangan) sesuatu hal, dan sebagainya setelah ditelaah secara seksama.
d. Analisis adalah proses pemecahan masalah yang dimulai dengan hipotesis (dugaan, dan sebagainya) sampai terbukti kebenarannya melalui beberapa kepastian (pengamatan, percobaan, dan sebagainya).
e. Analisis adalah proses pemecahan masalah (melalui akal) ke dalam bagian-bagiannya berdasarkan metode yang konsisten untuk mencapai pengertian tentang prinsip-prinsip dasarnya..

2.2 Keamanan Informasi

Keamanan informasi menggambarkan usaha untuk melindungi komputer dan nonperalatan komputer, fasilitas, data, dan informasi dari penyalahgunaan oleh orang yang tidak bertanggung jawab. Definisi ini meliputi pengutip, fax mesin, dan semua jenis media, termasuk dokumen kertas dan smartphone. Untuk penggunaan smartphone, dalam hal berkomunikasi sudah menjadi kebutuhan sehari-hari. Dari beberapa kasus, penggunaan smartphone dapat disalahgunakan untuk tindak kejahatan komputer, dari mulai penipuan, sampai pemerasaan. (Kohar, Abdul, et al, 2015)

Keamanan Informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis (business continuity), meminimalisasi risiko bisnis (reduce business risk) dan memaksimalkan atau mempercepat pengembalian investasi dan peluang. (Sarno dan Iffano, 2009: 27)

Contoh keamanan informasi menurut Sarno dan Iffano (2009: 27) adalah sebagai berikut :

a. Physical Security adalah keamanan informasi yang memfokuskan pada strategi untuk mengamankan individu atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
b. Personal Security adalah keamanan informasi yang berhubungan dengan keamanan personil. Biasanya saling berhubungan dengan ruang lingkup “physical security”.
c. Operation Security adalah keamanan informasi yang membahas bagaimana strategi suatu organisasi untuk mengamankan kemampuan organisasi tersebut untuk beroperasi tanpa gangguan.
d. Communications Security adalah keamanan informasi bertujuan mengamankan media komunikasi, teknologi komunikasi, serta apa yang ada di dalamnya. Serta kemampuan untuk memanfaatkan media dan teknologi komunikasi untu kemncapai tujuan organisasi.
e. Network Security adalah keamanan informasi yang memfokuskan pada bagaimana pengamanan peralatan jaringan, data organisasi, jaringannya dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

Aspek Keamanan Informasi meliputi ketiga hal, yaitu: Confidentiality, Integrity, dan Availability (CIA). Aspek tersebut sebagaimana dijelaskan sebagai berikut :

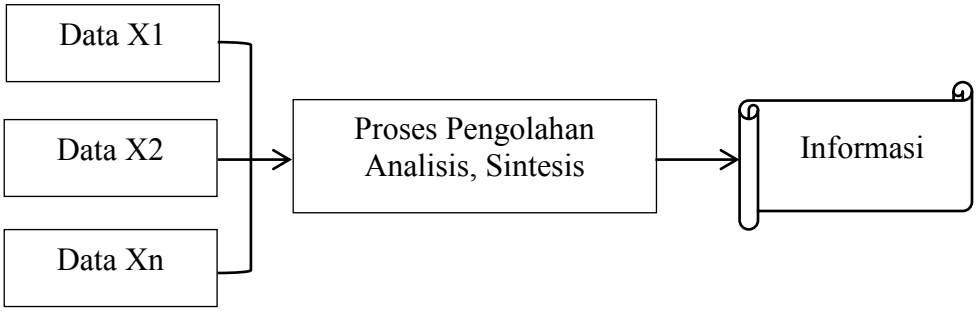
a. Confidentiality : Keamanan Informasi seharusnya menjamin bahwa hanya mereka yang memiliki hak yang boleh mengakses Informasi tertentu.
b. Integrity : Keamanan Informasi seharusnya menjamin kelengkapan Informasi dan menjaga dari korupsi, kerusakan, atau ancaman lain yang menyebabkannya berubah Informasi dari aslinya.
c. Availability : Keamanan Informasi seharusnya menjamin pengguna dapat mengakses Informasi kapanpun tanpa adanya gangguan dan tidak dalam format yang bisa digunakan. Pengguna, dalam hal ini bisa jadi manusia, atau komputer yang tentunya dalam hal ini memiliki otorisasi untuk mengakses Informasi.

2.3 Sistem Informasi

Sistem informasi merupakan suatu perkumpulan data yang terorganisasi beserta tatacara penggunaanya yang mencangkup lebih jauh dari pada sekedar penyajian.Istilah tersebut menyiratkan suatu maksud yang ingin dicapai dengan jalan memilih dan mengatur data serta menyusun tatacara penggunaanya.

Isu mendasar tentang pengembangan perangkat lunak yang mendukung jaringan forensik adalah bagaimana menentukan metode yang tepatmemudahkan pengolahan data log menjadi data yang mudah diproses. (Imam Riadi, 2013). Keberhasilan suatu sistem informasi yang diukur berdasarkan maksud pembuatanya tergantung pada tiga faktor utama, yaitu : keserasian dan mutu data, pengorganisasian data, dan tatacara penggunaanya.untuk memenuhi permintaan penggunaan tertentu, maka struktur dan cara kerja sistem informasi berbeda-beda bergantung pada macam keperluan atau macam permintaan yang harus dipenuhi.

Suatu persamaan yang menonjol ialah suatu sistem informasi menggabungkan berbagai ragam data yang dikumpulkan dari berbagai sumber.Untuk dapat menggabungkan data yang berasal dari berbagai sumber suatu sistem alih rupa (transformation) data sehingga jadi tergabungkan (compatible).Berapa pun ukurannya dan apapun ruang lingkupnya suatu sistem informasi perlu memiliki ketergabungan (compatibility) data yang disimpannya.Selanjutnya dijelaskan dalam gambar 2.1 berikut :



Gambar 2.1 Proses Sistem Informasi

Terdapat berbagai macam pengertian Sistem Informasi menurut beberapa ahli, diantaranya :

a. Sistem Informasi adalah suatu system didalam organisasi yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasi, bersifat manajerial dan kegiatan strategis dari suatu organisasi dan menyediakan pihak luar tertentu dengan laporan-laporan yang diperlukan. (Jogiyanto, 2009)
b. Sistem Informasi adalah kumpulan elemen yang saling berhubungan satu sama lain untuk membentuk suatu kesatuan untuk mengintegrasi data, memproses dan menyimpan serta mendistribusikan informsi tersebut. (Kristanto, 2007)
c. Sistem informasi adalah suatu sistem buatan manusia yang secara umum terdiri atas sekumpulan komponen berbasis computer dan manual yang dibuat untuk menghimpun, menyimpan, dan mengolah data serta menyediakan informasi keluaran kepada pemakai. (Kadir, 2009).
d. Sistem informasi adalah suatu sistem didalam suatu organisasi yang mempertemukan kebutuhan pengelolaan transaksi harian, mendukung operasi, yang bersifat manajerial, dan kegiatan strategi dari suatu organisasi dan meyediakan pihak luar tertentu dengan laporan-laporan yang dibutuhkan. (Jeperson Hutahaean, 2014)

Jadi definisi sistem informasi adalah suatu kumpulan sumber daya manusia atau alat yang terpadu serta modal yang bertanggung jawab untuk mengumpulkan data dan mengolah data demi menghasilkan suatu informasi yang berguna bagi seluruh tingkat operasi untuk kegiatan perencanaan, pelaksanaan, pekerjaan, pengendalian, dan pengambilan keputusan dalam sebuah organisasi.

Informasi dalam lingkup sistem informasi memiliki beberapa ciri yaitu:

a. Baru, informasi yang didapat sama sekali baru dan segar bagi penerima.
b. Tambahan, informasi dapat memperbaharui atau memberikan tambahan pada informasi yang telah ada.
c. Korektif, informasi dapat menjadi suatu koreksi atas informasi yang salah sebelumnya.
d. Penegas, informasi dapat mempertegas informasi yang telah ada.

2.4 Sistem Informasi Akademik

Sistem informasi akademik adalah suatu disiplin akademik atau bidang studi, juga merupakan suatu cabang pengetahuan yang diajarkan atau diteliti ditingkat sekolah dan perguruan tinggi. Disiplin akademik ini didefinisikan dan diakui jurnal akademik yang mempublikasikan riset pada suatu bidang serta masyarakat terpelajar dan departemen atau fakultas akademik yang menjadi tempat para praktisi tersebut. (Pambudi, 2015)

Tujuan diadakan pengolahan data kuliah yaitu untuk memperlancar kegiatan belajar mengajar didukung administrasi yang rapi dan terstruktur, menyajikan informasi yang penting dalam bentuk tertulis serta penyimpanan semua dokumen.

Sistem informasi akademik adalah suatu bentuk pelayanan publik yang diberikan oleh pihak universitas untuk mahasiswa, dosen, dan karyawan dalam mendapatkan informasi di bidang akademik.Sistem Informasi Akademik selain merupakan sumber daya informasi di kampus, juga dapat digunakan sebagai sarana media komunikasi antara dosen dan mahasiswa, mahasiswa dengan mahasiswa dosen dengan pejabat kampus terkait dan siapa saja yang ada di lingkungan kampus tersebut.Karena menggunakan teknologi internet tidak hanya dilakukan dalam kampus saja tetapi diluar kampuspun bisa dilakukan bahkan dimana saja di seluruh dunia ini asalkan ada sebuah komputer yang terhubung dengan internet. Sistem Informasi Akademik adalah merupakan sistem informasi yang berbasis web yang bertujuan untuk membentuk Knowledge Based System yang dapat diakses internet, sebagai contoh macam informasi yang ada didalamnya adalah :

a. Berita, berisi informasi terbaru yang diterbitkan oleh lembaga pendidikan maupun informasi teknologi dari berbagai sumber berita.
b. Pendidikan, berisi informasi yang berkaitan dengan perkuliahan yang terdapat dilembaga pendidikan, misalnya kurikulum, Satuan Acara Perkuliahan (SAP), dosen, materi kuliah, Kerja Praktek, tugas akhir dan penelitian.

e. Jadwal Perkuliahan, yang berisi tentang jadwal kuliah, kegiatan mahasiswa, memonitor jadwal perkuliahan dosen, jumlah kehadiran dalam mengikuti perkuliahan.
f. Perpustakaan, berisi tentang informasi buku melalui catalog online.
g. Electronic Mail (Email), fasilitas ini untuk mengirim dan menerima surat/pesan sekaligus dapat dijadikan sebagai sarana atau alat diskusi antar mahasiswa, dosen bahkan karyawan dalam lembaga pendidikan

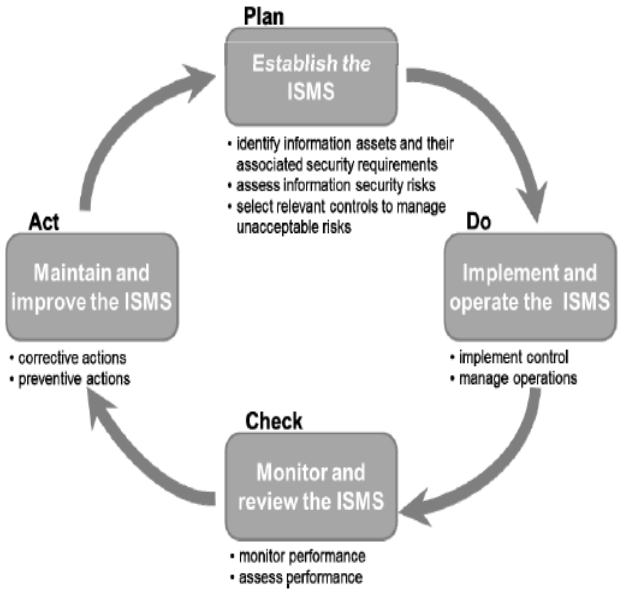
2.5 Standar Manajemen Keamanan Sistem Informasi

ISO adalah badan penetap standar internasional yang terdiri dari wakil-wakil dari badan standardisasi nasional setiap negara.Didirikan pada 23 Februari 1947, ISO menetapkan standar-standar industrial dan komersial dunia. ISO merupakan lembaga nirlaba internasional, pada awalnya dibentuk untuk membuat dan memperkenalkan standardisasi internasional untuk apa saja. Standar yang sudah kita kenal antara lain standar jenis film fotografi, ukuran kartu telepon, kartu ATM Bank, ukuran dan ketebalan kertas dan lainnya.

Dalam menetapkan suatu standar tersebut mereka mengundang wakil anggotanya dari 130 negara untuk duduk dalam Komite Teknis (TC), Sub Komite (SC) dan Kelompok Kerja (WG). Peserta ISO termasuk satu badan standar nasional dari setiap negara dan perusahaan-perusahaan besar.ISO bekerja sama dengan Komisi Elektroteknik Internasional (IEC) yang bertanggung jawab terhadap standardisasi peralatan elektronik.

Sejak tahun 2005, International Organization for Standardization (ISO) atau Organisasi Internasional untuk Standarisasi telah mengembangkan sejumlah standar tentang Information Security Management Systems (ISMS) atau Sistem Manajemen Keamanan Informasi (SMKI) baik dalam bentuk persyaratan maupun panduan.

ISO 27000 diterbitkan pda tahun 2009 untuk memberikan gambaran tentang standar ISO 27000 serta dasar konseptual secara umum. Terdapat 46 keamanan informasi dasar yang didefinisikan dalam dalam “Term and Condition” ISO 27000.Keamanan informasi didasarkan dari perusahaan yang bisnis prosesnya tergantung dengan infrastruktur IT yang rentan terhadap kegagalan dan gangguan.Sama halnya dengan standar teknologi informasi yang lain, ISO 27000 merujuk pada siklus PDCA (Plan – Do – Check – Action), siklus yang terkenal dari manajemen mutu.



Gambar 2.2 Siklus PDCA pada ISO 27000 Series

ISO 27000 Series (juga dikenal sebagai "ISMS Family of Standards" atau yang singkat "ISO27K") berisi information security standards yang diterbitkan bersama oleh ISO dan IEC. ISO 27000 memuat: Information technology - Security techniques - Information security management systems - Overview and vocabulary. Standard tersebut dikembangkan oleh sub-committee 27 (SC27) dari the first Joint Technical Committee (JTC1) dari International Organization for Standarization dan International Electrotechnical Commission.

ISO 27000 memberikan:

a. Gambaran dan pengenalan tentang Information Security Management Systems (ISMS) dari ISO 27000 series.
b. Sebuah glossary atau kosa kata dari istilah dasar dan definisi yang digunakan dalam ISO 27000 series.

International Standards Organization (ISO) mengelompokkan semua standar keamanan informasi ke dalam satu struktur penomoran, seperti pada serial ISO 27000. Adapun beberapa standar di seri ISO ini adalah sebagai berikut:

a. ISO 27000 : dokumen definisi-definisi keamanan informasi yang digunakan sebagai istilah dasar dalam serial ISO 27000.
b. ISO 27001 : berisi aspek-aspek pendukung realisasi serta implementasi sistem manajemen keamanan informasi perusahaan

c. ISO 27002 : terkait dengan dokumen ISO 27001, namun dalam dokumen ini terdapat panduan praktis pelaksanaan dan implementasi sistem manajemen keamanan informasi perusahaan.

d. ISO 27003 : panduan implementasi sistem manajemen keamanan informasi perusahaan.

e. ISO 27004 : dokumen yang berisi matriks dan metode pengukuran keberhasilan implementasi sistem manajemen keamanan informasi.

f. ISO 27005 : dokumen panduan pelaksanaan manajemen risiko.

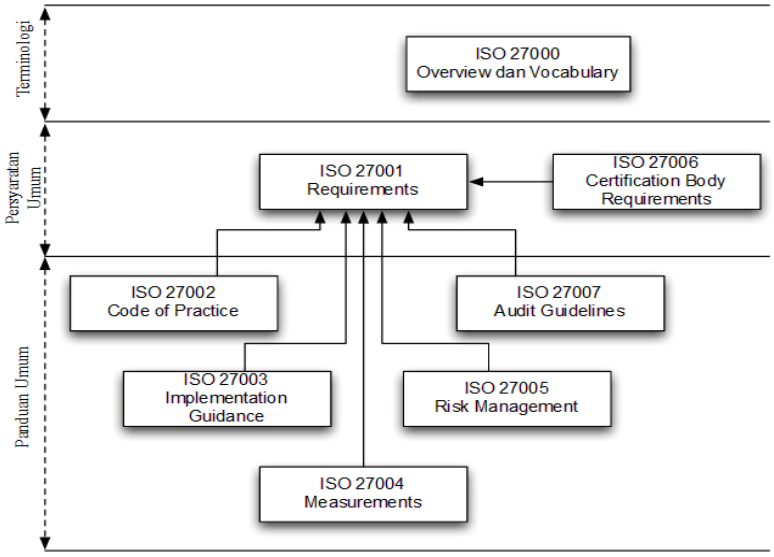
g. ISO 27006 : dokumen panduan untuk sertifikasi sistem manajemen keamanan informasi perusahaan.

h. ISO 27007 : dokumen panduan audit sistem manajemen keamanan informasi perusahaan.

i. ISO 27799 : panduan ISO 27001 untuk industri kesehatan.

Dari standar seri ISO 27000 ini, hingga September 2011, baru ISO/IEC 27001:2005 yang telah diadopsi Badan Standarisasi Nasional (BSN) sebagai Standar Nasional Indonesia (SNI) berbahasa Indonesia bernomor SNI ISO/IEC 27001:2009.

Standar ini dirilis tahun 2009, memuat prinsip-prinsip dasar Information Security Management Systems (Sistem Manajemen Keamanan Informasi–SMKI), definisi sejumlah istilah penting dan hubungan antar standar dalam keluarga SMKI, baik yang telah diterbitkan maupun sedang dalam tahap pengembangan. Hubungan antar standar dari keluarga ISO 27000 dapat dilihat pada Gambar 2.3 berikut:



Gambar 2.3 Hubungan Antar Standar Keluarga ISO 27000

Sebagaimana tercantum dalam Gambar 2.3, dapat dijelaskan bahwa :

a. ISO/IEC 27001 – Persyaratan Sistem Manajemen Keamanan Informasi

SNI ISO/IEC 27001 yang diterbitkan tahun 2009 dan merupakan versi Indonesia dari ISO/IEC 27001:2005, berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan.

Standar ini dikembangkan dengan pendekatan proses sebagai suatu model bagi penetapan, penerapan, pengoperasian, pemantauan, tinjau ulang (review), pemeliharaan dan peningkatan suatu SMKI. Pendekatan proses mendorong pengguna menekankan pentingnya:

1) Pemahaman persyaratan keamanan informasi organisasi dan kebutuhan terhadap kebijakan serta sasaran keamanan informasi
2) Penerapan dan pengoperasian control untuk mengelola risiko keamanan informasi dalam konteks risiko bisnis organisasi secara keseluruhan
3) Pemantauan dan tinjau ulang kinerja dan efektivitas SMKI, dan
4) Peningkatan berkelanjutan berdasarkan pada pengukuran tingkat ketercapaian sasaran.

Model PLAN – DO – CHECK – ACT (PDCA) diterapkan terhadap struktur keseluruhan proses SMKI. Dalam model PDCA, keseluruhan proses SMKI dapat dipetakan seperti Tabel 2.1.

Tabel 2.1 Peta PDCA dalam proses SMKI

PLAN(Menetapkan SMKI)	Menetapkan kebijakan SMKI, sasaran, proses dan proseduryang relevan untuk mengelolarisiko dan meningkatkan keamananinformasi agar memberikan hasilsesuai dengan
DO (Menerapkan dan mengoperasikan SMKI)	Menerapkan danmengoperasikan kebijakan SMKI, kontrol, proses danprosedur-prosedur.
CHECK(Memantau dan melakukan tinjau ulang SMKI)	Mengkajidan mengukurkinerja proses terhadap kebijakan, sasaran, praktek-praktek dalam menjalankan SMKIdanmelaporkan hasilnyakepada manajemen untuk ditinjau efektivitasnya.
ACT(Memeliharadan meningkatkan SMKI)	Melakukan tindakan perbaikan dan pencegahan, berdasarkan hasilevaluasi,auditinternal dan tinjauan manajemen tentangSMKI atau kegiatan pemantauan lainnyauntuk mencapai peningkatanyang berkelanjutan.

Standar menyatakan persyaratan utama yang harus dipenuhi menyangkut:

1) Sistem manajemen keamanan informasi (kerangka kerja, proses dan dokumentasi)
2) Tanggung jawab manajemen
3) Audit internal SMKI
4) Manajemen tinjau ulang SMKI
5) Peningkatan berkelanjutan

Disamping persyaratan utama di atas, standar ini mensyaratkan penetapan sasaran kontrol dan kontrol-kontrol keamanan informasi meliputi 11 area pengamanan sebagai berikut:

1) Kebijakan keamanan informasi
2) Organisasi keamanan informasi
3) Manajemen aset
4) Sumber daya manusia menyangkut keamanan informasi
5) Keamanan fisik dan lingkungan
6) Komunikasi dan manajemen operasi
7) Akses kontrol
8) Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi
9) Pengelolaan insiden keamanan informasi
10) Manajemen kelangsungan usaha (business continuity management)
11) Kepatuhan

b. ISO/IEC 27002 – Code of Practice for ISMS

ISO/IEC 27002 atau disebut juga ISO/IEC 17799 berisi panduan yang menjelaskan contoh penerapan keamanan informasi dengan menggunakan bentuk-bentuk kontrol tertentu agar mencapai sasaran control yang ditetapkan. Bentuk-bentuk kontrol yang disajikan seluruhnya menyangkut 11 area pengamanan sebagaimana ditetapkan dalam ISO/IEC 27001.

ISO/IEC27002 tidak mengharuskan bentuk-bentuk kontrol yang tertentu tetapi menyerahkan kepada pengguna untuk memilih dan menerapkan control yang tepat sesuai kebutuhannya, dengan mempertimbangkan hasil kajian risiko yang telah dilakukannya. Pengguna juga dapat memilih kontrol di luar daftar kontrol yang dimuat standar ini sepanjang sasaran kontrolnya dipenuhi.

c. ISO/IEC 27003 – Information Security Management System Implementation Guidance

Tujuan dari ISO/IEC 27003 adalah untuk memberikan panduan bagi perancangan dan penerapan SMKI agar memenuhi persyaratan ISO 27001.

Standar ini menjelaskan proses pembangunan SMKI meliputi persiapan, perancangan dan penyusunan/pengembangan SMKI yang digambarkan sebagai suatu kegiatan proyek. Sebagai kegiatan proyek, tahapan utama yang dijelaskan dalam standar ini meliputi

1) Mendapatkan persetujuan manajemen untuk memulai proyek SMKI
2) Mendefinisikan ruang lingkup, batasan dan kebijakan SMKI
3) Melakukan analisis persyaratan SMKI
4) Melakukan kajian risiko dan rencana penanggulangan risiko
5) Merancang SMKI
6) Merencanakan penerapan SMKI

Standar ini diterbitkan pada bulan Januari 2010.

d. ISO/IEC 27004 - Information Security Management Measurement

Standar ini menyediakan panduan penyusunan dan penggunaan teknik pengukuran untuk mengkaji efektivitas penerapan SMKI dan kontrol sebagaimana dipersyaratkan ISO/IEC 27001.Standar ini juga membantu organisasi dalam mengukur ketercapaian sasaran keamanan yang ditetapkan.Standar ini mencakup bagian utama sebagai berikut:

1) Penjelasan tentang pengukuran keamanan informasi;
2) Tanggung jawab manajemen;
3) Pengembangan metode pengukuran;
4) Pengukuran operasi;
5) Analisis data dan pelaporan hasil pengukuran;
6) Evaluasi dan perbaikan program pengukuran keamanan informasi.

Standar ini diterbitkan bulan Desember 2009

e. ISO/IEC27005 - Information Security Risk Management

Standar ini menyediakan panduan bagi kegiatan manajemen risiko keamanan informasi dalam suatu organisasi, khususnya dalam rangka mendukung persyaratan-persyaratan SMKI sebagaimana didefinisikan oleh ISO/IEC 27001.

Standar ini diterbitkan pada bulan Juni 2008.

f. ISO/IEC 27006 - Requirements for Bodies Providing Audit and Certification of Information Security Management Systems.

Standar ini menetapkan persyaratan dan memberikan panduan bagi organisasi yang memiliki kewenangan untuk melakukan audit dan sertifikasi sistem manajemen keamanan informasi (SMKI). Standar ini utamanya dimaksudkan untuk mendukung proses akreditasi Badan Sertifikasi ISO/IEC 27001 oleh Komite Akreditasi dari negara masing-masing.

2.6 ISO 27002:2013

Dalam pembahasan ini penulis ingin menjelaskan mengenai perbedaan ISO 27001 dan ISO 27002 serta membandingkan antara ISO 27002:2005 dengan ISO 27002:2013.

2.6.1 Perbedaan ISO 27001 dengan ISO 27002

Terkait dengan judul penelitian yang diangkat, penulis membaca beberapa literatur yang terkait dengan standard international ini, baik berupa definisi, cakupan ataupun sertifikasinya.Mungkin yang sering terdengar dan lebih populer untuk masalah security system dengan ISO 27001. Sama- sama merupakan standar yang bekerja di bidang IT, ISO 27001 dan ISO 27002 memiliki beberapa perbedaan yang menarik untuk kita ketahui.

ISO 27002 adalah seperangkat standar dan prosedur yang berkaitan dengan keamanan dan kontrol informasi yang memungkinkan bisnis untuk menerapkan keamanan yang tepat.Standar ini sebagian besar dilengkapi dengan ISO 27001 yang merinci tugas manajerial seperti penilaian risiko dan meninjau keamanan.Dilain pihak, ISO 27002 banyak berbicara tentang aspek kontrol.

Dua standar juga pernah digunakan sebelum ISO 27002 diadopsi.Pertama adalah BS7799 yang digunakan di Inggris dan muncul pada tahun 1995.Setelah direvisi, BS7799 diterbitkan lagi oleh ISO sebagai ISO 17799.Pada tahun 2005, setelah suntingan lebih lanjut, ISO 17799 dikenal sebagai ISO 27002.Sementara setiap versi berbeda namun ketiganya sama-sama berurusan dengan keamanan informasi.

ISO 27002 memuat ratusan cara untuk menangani keamanan informasi dan memiliki banyak bab tentang cara mengamankan informasi. Beberapa bab berkaitan dengan sumber daya manusia dan interaksi mereka dengan informasi, sementara yang lain memuat cara sebuah bisnis untuk mengontrol akses dan kelangsungan usaha dengan prosedur keamanan mereka. Keamanan informasi biasanya identik dengan teknologi informasi (TI), tetapi ISO 27002 juga berkaitan dengan mengamankan informasi diatas kertas, meskipun sebagian besar dari standar ini ditujukan untuk departemen TI.

Dalam rilis pertama, standar 27002 dimaksudkan untuk meliputi semua lembaga yang membutuhkan keamanan informasi. Ini berarti perusahaan, organisasi non-profit, lembaga pemerintah, dan entitas bisnis semua akan mengikuti standar yang sama. Namun, versi selanjutnya memisahkan standar untuk berbagai sektor agar lebih efisien.ISO 27002 berisi rincian tentang pengendalian dan prosedur yang digunakan untuk menjaga informasi tetap aman.Standar lainnya, seperti ISO 27001, hanya berisi bagian kecil tentang kontrol.Sebaliknya, 27002 banyak berkaitan dengan kontrol tapi menawarkan sedikit dalam hal manajemen.Pada ISO 27001, semua aspek manajemen tersebut turut dimasukkan.

Kontrol dari ISO 27002 meliputi:

a. Security Policy
b. Information security policies
c. Organization of information security
d. Human resource security
e. Asset management.
f. Access control
g. Cryptography
h. Physical and environmental security
i. Operations management
j. Communications security
k. System acquisition, development and maintenance
l. Supplier relationships
m. Information security incident management
n. Information security aspects of business continuity management
o. Compliance

Sementara itu, ISO 27001 merupakan standard internasional yang paling banyak digunakan untuk information security management.Sampai dengan akhir 2009, lebih dari 12.000 organisasi di seluruh dunia telah memiliki sertifikasi ISO 27001.ISO 27001 digunakan untuk melindungi confidentiality, integrity dan availability dari informasi. ISO 27001 bukan merupakan technical standard yang akan menjelaskan ISMS ke dalam technical detail, dan tidak hanya fokus pada IT tetapi juga aset penting lainnya di dalam organisasi. ISO 27001 fokus pada business process dan business asset, pengurangan resiko

terhadap informasi yang bernilai tinggi bagi organisasi.Informasi tersebut dapat terkait ataupun tidak terkait dengan IT, dapat berbentuk ataupun tidak berbentuk format digital.

Persyaratan yang harus diterapkan untuk dokumentasi ISMS, dijelaskan dalam standar melalui penetapan konten penting, dokumen yang diperlukan serta spesifikasi dan struktur pemantauan untuk manajemen dokumen, seperti:

a. Proses perubahan dan persetujuan
b. Kontrol versi
c. Aturan untuk hak akses dan perlindungan akses
d. Spesifikasi untuk sistem pengarsipan

Berikut table ISO 20071 sebagaimana penjelasan diatas:

Tabel 2.2 ISO 27001 Control Objective

No	Domain	Control objectives
1	Security policy	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.
2	Organization of information security	To manage information security within the organization.
		To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.
3	Asset management	To achieve and maintain appropriate protection of organizational assets.
		To ensure that information receives an appropriate level of protection.
4	Human resources security	To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and to reduce the risk of theft, fraud or misuse of facilities.
		To ensure that all employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.
		To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.
5	Physical and environmental security	To prevent unauthorized physical access, damage and interference to organization's premises and information.
		To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.
6	Communications and operations management	To ensure the correct and secure operation of information processing facilities.
		To implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements.
		To minimize the risk of systems failures.
		To protect the integrity of software and information.
		To maintain the integrity and availability of information and information processing facilities.
		To ensure the protection of information in networks and the protection of the supporting infrastructure.
		To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.
		To maintain security of information and software exchanged within an organization and with external entities.

No	Domain	Control objectives
		To ensure the security of electronic commerce services, and their secure use.
		To detect unauthorized information processing activities.
7	Access control	To control access to information.
		To ensure authorized user access and to prevent unauthorized access to information systems.
		To prevent unauthorized user access, compromise or theft of information and information processing facilities.
		To prevent unauthorized access to networked services.
		To prevent unauthorized access to operating systems.
		To prevent unauthorized access to information held in application systems.
		To ensure information security when using mobile computing and teleworking facilities.
8	Information systems acquisition, development and maintenance	To ensure that security is an integral part of information systems.
		To prevent errors, loss, unauthorized modification or misuse of information in applications.
		To protect the confidentiality, authenticity or integrity of information by cryptographic means.
		To ensure the security of system files.
		To maintain the security of application system software and information.
		To reduce risks resulting from exploitation of published technical vulnerabilities.
9	Information security incident management	To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.
		To ensure a consistent and effective approach is applied to the management of information security incidents.
10	Business continuity management	To counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.
11	Compliance	To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.
		To ensure compliance of systems with organizational security policies and standards.
		To maximize the effectiveness of and to minimize interference to/from the information systems audit process.

Itu sebab, banyak orang bingung membedakan ISO 27001 dan 27002 karena keduanya menangani subyek yang sama meskipun dengan cara yang berbeda. Pemisahan dilakukan karena jika keduanya disatukan akan menghasilkan dokumen yang terlalu panjang dan malah membingungkan.

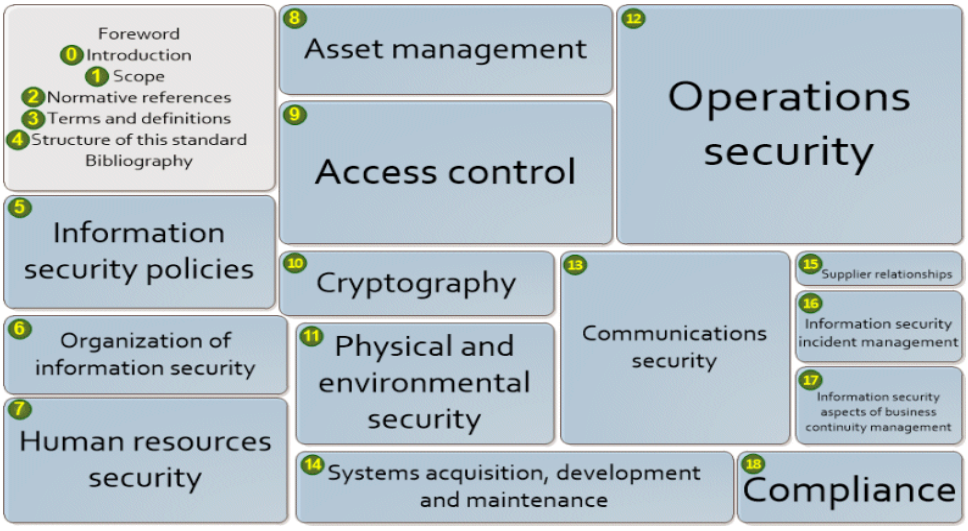
Dengan kata lain, ISO/IEC 27001 mengandung persyaratan untuk sebuah Sistem Manajemen Keamanan Informasi (SMKI) sementara lingkup ISO 27002 adalah untuk membentuk pedoman dan prinsip-prinsip umum dalam penginisialisasian, pengimplementasian, pemeliharaan dan perbaikan manajemen keamanan informasi dalam suatu organisasi. Standar ini mencakup kebijakan keamanan, organisasi keamanan, pengaturan dan klasifikasi aset, keamanan personil, keamanan lingkungan dan fisik, manajemen operasi dan komunikasi, pengaturan akses, pengembangan dan pemeliharaan sistem dan manajemen keberlangsungan bisnis.

2.6.2 Perbedaan ISO 27002:2005 dengan ISO 27002:2013

Standar ini merupakan adopsi identik dari ISO/IEC 27002:2005, yang menetapkan pedoman dan prinsip-prinsip umum untuk memulai, melaksanakan, memelihara, dan meningkatkan manajemen keamanan informasi dalam suatu organisasi. Tujuan standar ini yaitu untuk memberikan penjelasan tentang panduan umum terkait diterimanya tujuan umum manajemen keamanan informasi.

SNI ISO/IEC 27002:2013 berisi pelaksanaan terbaik dari tujuan pengendalian dan kontrol di bidang manajemen keamanan informasi, yang mencakup: kebijakan keamanan; organisasi keamanan informasi; manajemen aset; keamanan sumber daya manusia; keamanan fisik dan lingkungan; komunikasi dan manajemen operasi; kontrol akses; sistem informasi akuisisi, pengembangan dan pemeliharaan; manajemen insiden keamanan informasi; manajemen bisnis berkelanjutan; dan kesesuaian. (Buletin Badan Standarisasi Nasional, Volume 1 No. 2, Juni 2013)

Sebagaimana informasi pada halaman website http://www.27000.org dijelaskan bahwa perbedaan terbesar antara standar lama dan yang baru adalah struktur. ISO IEC 27002 2005 memiliki 11 bagian utama (5 sampai 14) sedangkan ISO IEC 27002 2013 kini memiliki 14 bagian utama (5 sampai 18).Sebagaimana terlihat dalam Gambar 2.4, berikut ini :



Gambar 2.4 Skema Control Objective ISO 27002:2013

Pada gambar diatas dijelaskan bahwa bagian membahas kriptografi, keamanan komunikasi, dan hubungan pemasok (bagian 10, 13, dan 15 masing-masing).Namun, sementara standar baru memiliki tiga bagian yang lebih, itu adalah sebenarnya lebih pendek dan lebih fokus daripada yang lama.Standar lama memiliki 106 halaman konten

sementara yang baru hanya memiliki 78.ISO IEC 27002 2013 juga memiliki beberapa subbagian baru. ini baru subbagian membahas keamanan manajemen proyek (6.1.5), asset penanganan (8.2.3), instalasi perangkat lunak (12.6.2), pengembangan aman (14.2.1), prinsip aman sistem rekayasa (14.2.5), aman pembangunan lingkungan (14.2.6), pengujian sistem keamanan (14.2.8), keamanan pemasok (15.1.1, 15.1.2, dan 15.1.3), penilaian peristiwa keamanan (16.1.4), perencanaan, pelaksanaan, dan memverifikasi kontinuitas keamanan informasi (17.1.1, 17.1.2, dan 17.1.3), dan penggunaan fasilitas pengolahan informasi yang berlebihan (17.2.1).

Selain itu, sebagian besar bagian telah ditulis ulang, setidaknya untuk beberapa batas, dan beberapa bagian telah berpisah atau pindah ke lain bagian. Misalnya, bagian berusia 14 pada kelangsungan bisnis telah sepenuhnya dikerjakan ulang. Selain itu, bagian yang lama tentang cara mengatur keamanan (6), komunikasi dan operasi (10), dan kontrol akses (11) semua sepenuhnya dikerjakan ulang, berpisah, dan pindah ke bagian lain yang lebih cocok. Dan bagian pengantar pada manajemen risiko sepenuhnya dihapus, mungkin karena ISO IEC 27005 dan ISO 31000 sekarang membahas hal ini secara rinci dan ISO IEC 27002 tidak perlu dibahas lagi.

Ada juga beberapa perubahan dalam terminologi. wewenang telah menjadi hak akses istimewa, password kata memiliki sebagian besar telah digantikan oleh frase rahasia yang lebih rumit informasi otentikasi, pengguna pihak ketiga yang sekarang dikenal sebagai pengguna pihak eksternal, cek kata kerja telah digantikan oleh memverifikasi, kode berbahaya sekarang malware, audit log sekarang event log, secara online transaksi sekarang disebut sebagai transaksi layanan aplikasi, dan favorit kami: perdagangan elektronik sekarang layanan aplikasi melewati jaringan publik. (Sumber : http://www.praxiom.com)

ISO 27002: 2005 berisi panduan yang menjelaskan contoh penerapan keamanan informasi dengan menggunakan bentuk-bentuk kontrol tertentu agar mencapai sasaran kontrol yang ditetapkan.Bentuk-bentuk kontrol yang disajikan seluruhnya menyangkut 11 area pengamanan sebagaimana ditetapkan didalam ISO/IEC 27001. Sarno dan Iffano (2009: 187) mengatakan kontrol keamanan berdasarkan ISO/IEC 27001 terdiri dari 11 klausul kontrol keamanan (security control clauses), 39 objektif kontrol (control objectives) dan 133 kontrol keamanan/ kontrol (controls) yang dapat dilihat dalam berikut :

Tabel 2.3 Ringkasan Jumlah Klausul Kontrol Keamanan, Objektif Kontrol, dan Kontrol ISO 27002:2005

Klausul	Jumlah	
	Objektif Kontrol	Kontrol
5	1	3
6	2	11
7	2	5
8	3	9
9	2	13
10	10	31
11	7	25
12	6	16
13	2	5
14	1	5
15	3	10
11	**39**	**133**

2.7 SSE-CMM (System Security Engineering - Capability Maturity Model)

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. SSE-CMM terdiri dari dua bagian, yaitu:

a. Model untuk teknik keamanan proses, proyek dan organisasi, dan
b. Metode penilaian untuk mengetahui kematangan proses.

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. Model ini merupakan standar untuk mempraktekkan rekayasa keamanan yang meliputi:

a. Siklus hidup, secara keseluruhan termasuk pengembangan, pengoperasian dan kegiatan pemulihan kembali.
b. Organisasi, keseluruhan termasuk pengelolaan, pengorganiasian dan kegiatan rekayasa.
c. Prilaku, berinteraksi dengan disiplin lain, seperti sistem, perangkat lunak, perangkat keras, faktor manusia, rekayasa pengujian, pengelolaan sistem, operasi dan pemeliharaan.

d. Berinteraksi dengan organisasi lain termasuk pengambil alihan, pengelolaan manajemen, sertifikasi, akreditasi dan evaluasi.

Model SSE-CMM memberikan gambaran menyeluruh tentang prinsip-prinsip dan arsitektur yang didasarkan SSE-CMM, gambaran eksekutif dari model, saran untuk pengggunaan model yang tepat, praktek-praktek yang termasuk dalam model, dan deskripsi atribut dari model. Metode penilaian SSE-CMM menjelaskan proses dan alat untuk mengevaluasi kemampuan teknik keamanan informasi.

Ruang lingkup SSE-CMM meliputi beberapa hal yaitu:

a. SSE-CMM ditujukan untuk kegiatan rekayasa keamanan yang meliputi produk yang terpercaya atau siklus hidup keamanan sistem, termasuk definisi konsep, analisa kebutuhan, perancangan, pengembangan, integrasi, instalasi, operasi, perawatan dan pengawasan.
b. SSE-CMM diterapkan untuk mengamankan pengembang produk, keamanan pengembang sistem dan integrator dan organisasi yang menyediakan jasa keamanan dan rekayasa keamanan.
c. SSE-CMM diterapkan untuk semua jenis dan ukuran rekayasa keamanan organisasi, seperti komersial, pemerintahan dan akademisi.

Untuk mengidentifikasi sejauh mana perusahaan/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 2.4 berikut ini :

Tabel 2.4 Kriteria Index Penilaian Pada Tingkat Kematangan

Range	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

Sebagaimana dijelaskan dalam tabel 2.4 diatas, bahwa SSE-CMM mempunyai lima tingkat kemampuan untuk menunjukkan tingkat kematangan proses, berikut penjelasannya :

a. Tingkat 0 tidak semua praktek dasar dilakukan.
b. Tingkat 1 semua praktek dasar dilakukan namun secara informal, yang artinya tidak ada dokumentasi, tidak ada standar dan dilakukan secara terpisah.

c. Tingkat 2 planned dan tracked yang menandakan komitmen merencanakan proses standar.

d. Tingkat 3 well defined yang berarti proses standar telah berjalan sesuai dengan definisi.

e. Tingkat 4 dikendalikan secara kuantitatif, yang berarti peningkatan kualitas melalui monitoring setiap proses.

f. Tingkat 5 ditingkatkan terus-menerus yang menandakan standar telah sempurna dan fokus untuk beradaptasi terhadap perubahan.

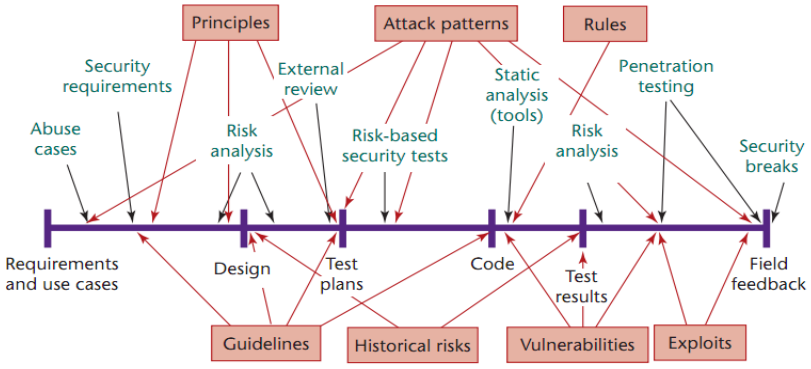
Metode SSE-CMM digunakan dengan memberikan skor pada setiap area proses yang dipilih antara 0 sampai 5 untuk setiap area proses

2.8 Keamanan Piranti Lunak

Keamanan piranti lunak merupakan proses mendesain, membangun dan melakukan uji coba sebuah piranti lunak dengan memperhatikan keamanan di tiap bagiannya agar piranti lunak tersebut dapat menahan serangan (G. McGraw, 2006). Untuk membangun piranti lunak yang aman pada umumnya bergantung pada proses saat rekayasa perangkat lunak, bahasa pemrograman yang digunakan dan teknik keamanan yang diterapkan.

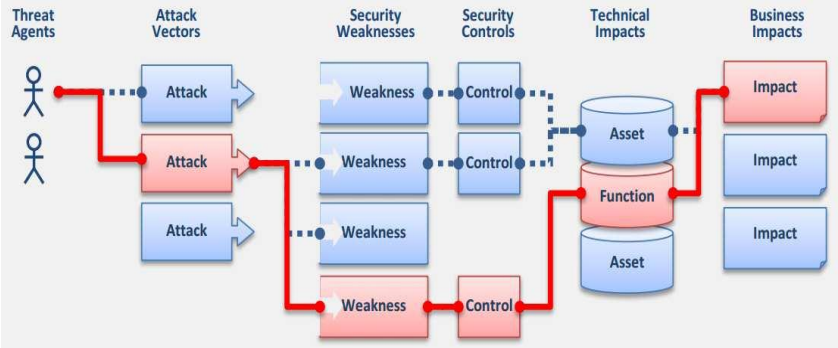
Membangun sebuah piranti lunak yang tanpa celah keamanan tidaklah mungkin. Hanya menunggu waktu, cara atau kesempatan bagi penyerang untuk dapat menemukan celah keamanan tersebut. Untuk itu pentingnya kesadaran akan keamanan sejak piranti lunak akan dibangun. Terdapat tiga pillar keamanan piranti lunak yakni manajemen resiko, touchpoint, dan pengetahuan. Dengan menerapkan ketiganya secara bertahap dan ukuran yang sesuai maka program keamanan piranti lunak yang standar dan hemat dapat terwujud.

Adapun tahapan pembangunan piranti lunak yang aman dengan dasar tiga pilar tersebut menurut Gary McGraw adalah sebagai berikut :



Gambar 2.5 Tahapan Secure Software Development Life Cycle (SDLC)

Setiap potensi resiko keamanan software dapat memberikan dampak yang berbeda bagi pengguna software, sehingga setiap potensi resiko kemanan tersebut harus diperhatikan. Gambaran resiko kemanan dan dampaknya terhadap pengguna software dapat dijelaskan dalam Gambar 2.6 berikut:



Gambar 2.6 Setiap potensi serangan dapat memberikan dampak yang berbeda

Dengan mengetahui dampak yang ditimbulkan maka dalam pengembangan software harus dilakukan hal-hal yang memungkinkan hal itu dapat terjadi.

2.9 Skala Guttman

Skala ini dikembangkan oleh Louis Guttman.Skala ini memiliki ciri penting, yaitu skala ini merupakan skala kumulatif dan skala ini digunakan untuk mengukur satu dimensi saja dari satu variable yang multi dimensi, sehingga skala ini termasuk mempunyai sifat undimensional.Skala ini juga disebut dengan metode Scalogram atau analisa skala (scale analysis).Skala Guttman sangat baik untuk meyakinkan peneliti tentang kesatuan dimensi dari sikap atau sifat yang diteliti, yang sering disebut isi universal (universe of content) atau atribut universal (universe attribute). Sebagai mana skala Thurstone, pernyataan-pernyataan memiliki bobot yang berbeda, dan jika responden menyetujui pernyataan yang memiliki bobot lebih berat, maka diharapkan akan menyetujui pernyataan yang berbobot lebih rendah. Untuk menilai undimensionalnya suatu variable pada skala ini, diadakan analisis skalogram untuk mendapatkan koefisien reproduksibilitas (Kr), dan koefisien skalabilitas (Ks), dimana jika nilai Kr = ≥ 0,90 dan Ks = ≥ 0,60 skala dianggap bagus (layak).

Guttman dengan skala ini bermaksud menetapkan apakah sikap yang sedang diselidiki itu benar-benar hanya menyangkut satu dimensi saja. Suatu sikap dianggap berdimensi tunggal hanya jika sikap itu menghasilkan skala kumulatif, yaitu skala yang butir-butirnya berkaitan satu sama lain sehingga seorang subjek yang setuju dengan

pernyataan nomor 2, akan juga setuju dengan pernyataan nomor 1; subjek yang setuju dengan nomor 3, maka akan juga setuju dengan pernyataan nomor 1 dan 2; dan seterusnya. Jadi seseorang yang menyetujui pernyataan tertentu dalam skala ini akan mempunyai skor skala keseluruhan yang lebih tinggi daripada orang yang tidak menyetujui pernyataan tersebut.

Jadi skala Guttman ialah skala yang digunakan untuk jawaban yang bersifat jelas (tegas dan konsisten). Misalnya yakin-tidak yakin; ya – tidak; benar – salah; positif – negative; pernah-belum pernah ; setuju – tidak setuju; dan sebagainya. (Sugiyono, 2009)

2.10 Gap Analisis

Gap Analysis adalah perbandingan kinerja aktual dengan kinerja potensial atau yang diharapkan. Metode ini merupakan alat evaluasi bisnis yang menitikberatkan pada kesenjangan kinerja perusahaan saat ini dengan kinerja yang sudah ditargetkan sebelumnya, misalnya yang sudah tercantum pada rencana bisnis atau rencana tahunan pada masing-masing fungsi perusahaan. Analisis kesenjangan juga mengidentifikasi tindakan-tindakan apa saja yang diperlukan untuk mengurangi kesenjangan atau mencapai kinerja yang diharapkan pada masa datang. Selain itu, analisis ini memperkirakan waktu, biaya, dan sumberdaya yang dibutuhkan untuk mencapai keadaan perusahaan yang diharapkan.(Jennings, M. D. ,2000).

BAB 3
Metodologi Penelitian

3.1 Analisis

Dalam penelitian ini penulis menggunakan metode penelitian kualitatif, data yang diperoleh berdasarkan hasil penyebaran kuesioner yang diberikan ke bagian Pusat Komputer dan Pengembangan Sistem Informasi (PUSKOM-PSI) .

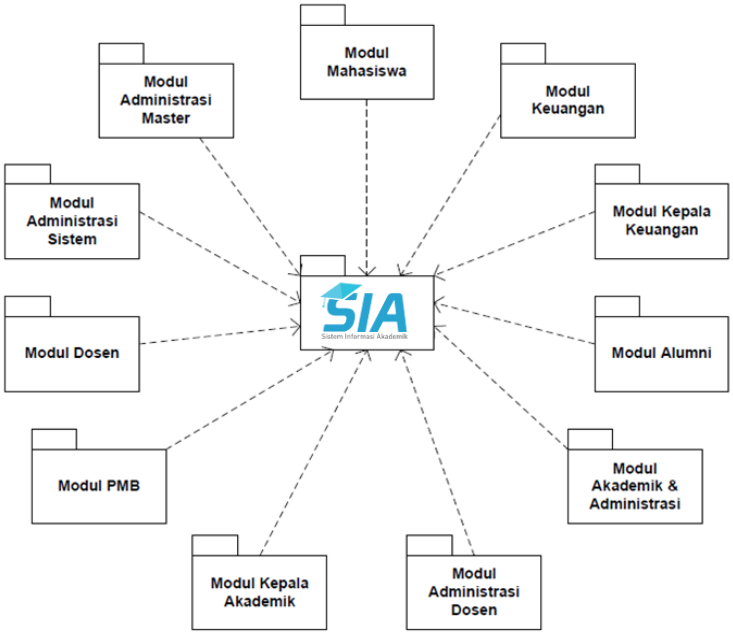
Populasi dalam penelitian ini yaitu karyawan pada PUSKOM-PSI yang berjumlah 7 orang. Penentuan jumlah sampel dari populasi tertentu yang dikembangkan dari Isaac dan Michael, untuk jumlah populasi 7 jumlah anggota sampel sebenarnya hanya 9,56 tetapi dibulatkan menjadi 7. (Sugiyono, 2011). Responden yang dilibatkan berjumlah 7 orang yang terdiri dari satu orang koordinator bagian, enam orang anggota tim.

Teknik pengambilan sampel yang digunakan adalah purposive sampling, dimana sampel dipilih oleh peneliti dalam penelitian ini adalah orang yang ahli dalam bidang tersebut.Teknik ini digunakan karena responden yang dipilih merupakan orang yang memang berkepentingan untuk mengelola dan bertanggungjawab terhadap sistem informasi akademik.

3.1.1 Desain Sistem Informasi Akademik

Sistem informasi akademik merupakan akses utama untuk mengatur segala urusan perkuliahan dan hal-hal lainnya yang berkaitan dengan akademik.Sistem informasi akademik ini merupakan salah satu pelayanan publik bagi dosen, mahasiswa, dan karyawan guna mempertingkat kinerja mereka. Sistem informasi akademik mempunyai komponen yang sama dengan sistem informasi lainnya. Komponen sistem informasi yaitu hardware, software, data, prosedur, dan manusia.

Sistem infromasi akademik yang dimaksud adalah sistem pengolahan data yang berhubungan dengan proses belajar mengajar perguruan tinggi antara lain: pengolahan data mahasiswa, mata kuliah, data dosen, data nilai, kelas dan juga sistem untuk penyimpanan data dan persiapan dokumen untuk membantu dalam pengambilan keputusan, sebagaimana desain dari modul yang tersedia dalam sistem informasi akademik pada Gambar 3.1 berikut ini :



Gambar 3.1 Modul Sistem Informasi Akademik

Dari Gambar 3.1 diatas, dapat dijelaskan fungsi dari masing-masing modul berikut ini:

a. Modul Administrasi Sistem

Modul ini adalah modul untuk mengelola sistem informasi akademik. Tugas-tugas ini meliputi:pengelolaan pengguna untuk tiap level pengguna, pengelolaan Group modul, Modul dan Sub-modul, pengelolaan modul pencetakan, dan tugas-tugas pemeliharaan lain. Tugas ini hanya dapat dilakukan oleh seorang Administrator Sistem.

b. Modul Administrasi Master

Modul ini adalah modul untuk mengelola tabel-tabel master. Tugas- tugas ini meliputi: data identitas perguruan tinggi pengguna, struktur organisasi, pengguna, pengelolaan master kampus, pengelolaan master fakultas dan jurusan, pengelolaan master program, pengelolaan master ruang/kelas, master mahasiswa, master jenis mata kuliah, master jenis pembayaran, setup prefix NIM, setup ijazah, master tanda tangan, dan pengelolaan master-master lain.

c. Modul Penerimaan Mahasiswa Baru

Modul ini adalah modul untuk pengelolaan penerimaan mahasiswa baru. Tugas-tugas ini meliputi: Penentuan pra-syarat PMB, setup prefix nomer PMB, penentuan biaya PMB, sub- modul pendaftaran, daftar mahasiswa baru, sub-modul program member-get-member, proses penerimaan dan pembatalan mahasiswa baru, sub-modul laporan dan statistik, sub-modul administrasi PMB, dan lainya.

d. Modul Administrasi Akademik

Modul ini adalah modul untuk pengelolaan operasional bidang akademik. Tugas-tugas ini meliputi: Penentuan kalendar akademik, ubah status mahasiswa, penjadwalan kuliah, penjadwalan ruang, administrasi KRS mahasiswa, absensi mahasiswa dan dosen, penundaan mata kuliah dan nilai mahasiswa, penjadwalan ujian, administrasi tugas akhir,data kelulusan mahasiswa, pencetakan formulir absensi, pencetakan ijazah, pencetakan KHS, pencetakan kartu mahasiswa, pencetakan kartu penyetaraan, pencetakan nilai mahasiswa, pencetakan pengawas ujian, pencetakan transkrip nilai, pencetakan transkrip sementara, pencetakan kartu realisasi perkuliahan, pencetakan laporan kehadiran mahasiswa.

e. Modul Kepala Akademik

Modul ini adalah modul khusus untuk kepala akademik. Tugas-tugas ini meliputi: pengelolaan kurikulum, pengelolaan tahun akademik, pengelolaan mata kuliah berdasarkan semester/cawu dan berdasarkan jenis mata kuliah, pengelolaan prasyarat mata kuliah, pengelolaan master jumlah maksimum SKS berdasarkan IPS, dispensasi KRS, edit mata kuliah mahasiswa, pembuatan password dosen untuk file nilai secara otomatis, rekapitulasi data mahasiswa, monitor IPK/IPS mahasiswa, pembuatan surat keputusan mengajar.

f. Modul Administrasi Keuangan

Modul ini adalah modul untuk pengelolaan keuangan mahasiswa. Tugas-tugas itu meliputi: sub-modul pembayaran, sub-modul pengembalian.

g. Modul Kepala Keuangan

Modul ini adalah modul khusus untuk kepala keuangan. Tugas-tugas itu meliputi: setup laporan kewajiban, laporan kewajiban, setup master BPP Pokok, setup program BPP Pokok, setup master biaya, administrasi master keuangan mahasiswa, proses keuangan, laporan mahasiswa belum lunas, laporan penerimaan, laporan pengembalian.

h. Modul Dosen

Modul ini adalah modul khusus untuk dosen. Tugas-tugas itu meliputi: melihat jadwal mengajar per dosen, pemberian nilai mahasiswa, penundaan nilai mata kuliah mahasiswa, sub-modul perwalian, sub-modul pembimbingan tugas akhir mahasiswa, lihat jadwal ujian dan jaga ujian, cetak nilai mahasiswa.

i. Modul Administrasi Dosen

Modul ini adalah modul untuk mengelola dosen dan atributnya. Modul ini meliputi: pengelolaan jabatan organisasi, pengelolaan master dosen, setup honor per program, sub-modul honor dosen, rekapitulasi honor dosen, rekapitulasi kehadiran dosen, evaluasi dosen, perincian dosen pembimbing.

j. Modul Mahasiswa

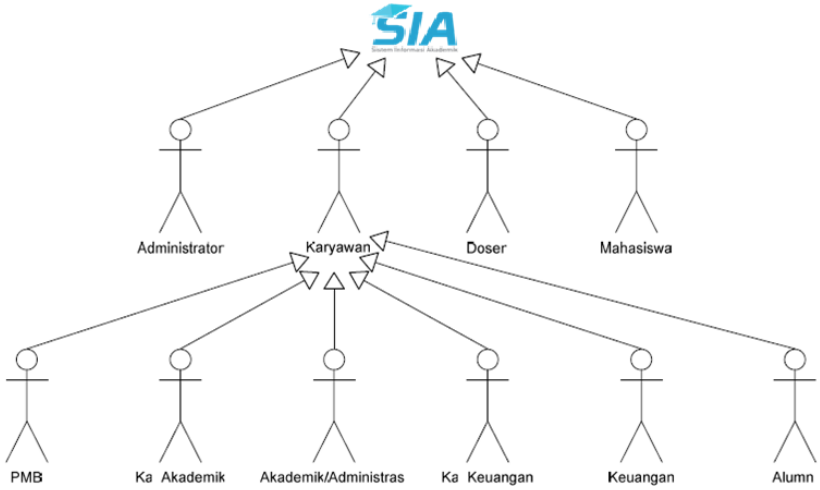
Modul ini adalah modul khusus untuk mahasiswa. Modul ini meliputi: lihat jadwal kuliah, lihat kalendar akademik, proses registrasi ulang mahasiswa, pengisian KRS, lihat KHS, lihat jadwal ujian, lihat riwayat Index Prestasi Kumulatif, riwayat mata kuliah yang telah diambil, lihat riwayat keuangan mahasiswa.

k. Modul Alumni

Modul ini adalah modul untuk mengelola alumni. Modul ini meliputi: sub-modul pengelolaan alumni, statistik alumni.

3.1.2 Pengguna Sistem Informasi Akademik

Dalam penggunaan sistem informasi akademik, ada beberapa aktor yang terlibat dalam proses pengolahan data, sebagaimana dijelaskan dalam Gambar 3.2 berikut :



Gambar 3.2 Pengguna Sistem Informasi Akademik

Sistem informasi akdemik mendefinisikan pengguna dalam 4 level, yaitu: Administrator, Karyawan, Dosen dan Mahasiswa. Sedangkan karyawan sendiri terbagi menjadi 6 jenis, yaitu: Staff, PMB, Kepala Akademik, Staff Akademik atau Administrasi, Kepala Keuangan, Staff Keuangan, dan Staff pengurus alumni.

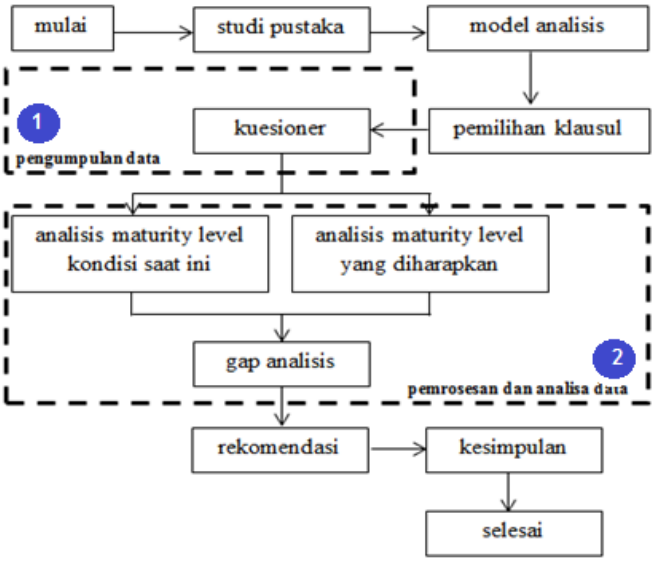
3.1.3 Hak Akses

Masing-masing level memiliki hak akses yang berbeda. Hak akses terhadap modul-modul juga dibatasi pada level pengguna yang bersangkutan. Sebelum pengguna dapat menggunakan, pengguna memiliki hak akses dengan username dan password yang sudah dibuatkan oleh pengelola sistem informasi akademik sebagaimana terlihat dalam Gambar 3.3. Berikut penjelasan mengenai hak akses dari penggunaan masing-masing modul :

Gambar 3.3 Login Sistem Informasi Akademik

3.2 Tahapan Penelitian

Dalam bab ini akan dijelaskan bagaimana penelitian dilakukan sehingga dapat diketahui urutan langkah-langkah yang dibuat secara sistematis. Adapun langkah-langkah atau tahapan-tahapan pada penelitian ini dapat dilihat pada Gambar 3.4 berikut dibawah ini :



Gambar 3.4 Langkah-langkah Kegiatan Penelitian

Langkah-langkah kegiatan pemeriksaan yang akan dilakukan telah dijelaskan pada Gambar 3.4. Untuk garis terputus pada nomor satu menunjukan langkah kegiatan awal yang akan dilakukan sebagai persiapan, sementara pada garis terputus nomor dua merupakan merupakan inputan yang digunakan untuk kegiatan inti tersebut. Untuk penjabaran dari aktivitas kegiatan yang lebih detail akan dijelaskan pada sub bab dalam metode penelitian ini.

3.3 Pengumpulan Data

Data yang diperoleh dalam penelitian ini terbagi menjadi dua macam yaitu data primer yang merupakan data utama penelitian dan data sekunder yang merupakan data pendukung penelitian.

Data primer merupakan data utama yang digunakan dalam penelitian yang diperoleh melalui :

a. Observasi, yaitu pengamatan di lapangan terhadap penerapan dan penggunaan sistem informasi akademik yang dikelola oleh PUSKOM-PSI
b. Wawancara, yaitu dengan memberikan pertanyaan-pertanyaan kepada narasumber yang juga dijadikan sebagai responden.
c. Survei, yaitu dengan memberikan kuisioner yang dibagikan kepada responden yang dipilih sebagai sampel dalam 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 3.1 adalah pemetaan yang telah disepakati untuk dilakukan penelitian yang merujuk pada standar ISO 27002.

Tabel 3.1 Tabel Klausa ISO 27002:2013

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

Pada penyebaran kuesioner penulis membuat daftar pertanyaan berdasarkan standar yang terdapat pada ISO 27002 / 17799 / BS 7799 tentang petunjuk pelaksanaan manajemen keamanan informasi yang terdiri 13 kontrol obyektif dan 43 kontrol keamanan yang tersebar dalam 3 klausul. Data sekunder yang penulis gunakan dalam penelitian ini diperoleh melalui literatur atau studi pustaka seperti buku, jurnal, prosiding dan laman.Dari hasil dari penyebaran kuesioner kemudian diolah.

Dalam penelitian ini adalah 7 responden, seperti yang ditunjukkan pada Tabel 3.2. Skala yang digunakan dalam kuesioner ini menggunakan skala Guttman. Skala pengukuran dengan tipe ini, akan didapat jawaban yang tegas, yaitu ya-tidak, benar-salah, pernah-tidak pernah, positif-negatif, dan lain-lain.

Tabel 3.2 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

Sesuai dengan visi misi dan tujuan dari penerapan sistem informasi akademik dalam penyusunan kuesioner dengan mengacu pada teori guttman (Skala Guttman)bahwa peneliti ingin memperoleh jawaban yang tegas dari setiap butir item kuesioneragar hasil yang diharapkan lebih akurat sesuai dengan permasalahan yang ada.

Untuk jawaban kuesioner disediakan dua pilihan yaitu pilihan jawaban Ya dan Pilihan jawaban Tidak, sebagaimana terlihat contoh penggunaan skala Guttman dalam Tabel 3.3. Dalam perhitungannya, jawaban Y (Ya) dikonversi menjadi nilai 1, dan jawaban T (Tidak) dikonversi menjadi nilai 0.Penelitian dengan menggunakan skala Guttman dilakukan bila ingin mendapatkan jawaban yang tegas terhadap suatu permasalahan yang ditanyakan (Sugiyono, 2011).

Tabel 3.3 Contoh Penggunaan Skala Guttman

Klausul	:	9.	Keamanan Fisik dan Lingkungan	
Kategori Keamanan Utama	:	9.1	Wilayah Aman	
Kontrol Keamanan	:	9.1.1	Pembatas Keamanan Fisik	
No	**Pernyataan**			**Ya**	**Tidak**
1.	Terdapat perlindungan keamanan fisik (dinding, kartu akses masuk atau penjaga pintu.				
2.	Terdapat perimeter keamanan untuk melindungi ruangan yang berisikan fasilitas pemrosesan informasi				

Perangkat lunak yang digunakan dalam perhitungan maturity level ini adalah Microsoft Excel. Setelah semua hasil kuesioner dimasukkan dalam tabel, kemudian dihitung maturity level tiap proses dalam masing-masing klausa untuk setiap responden. Hasil maturity level tiap klausa dari 7 responden kemudian dicari rata-ratanya, dan hasil rata-rata tersebut akan menjadi nilai maturity level atau tingkat kematangan keamanan informasi pada sistem informasi akademik.

Analisis dan Interprestasi data dari hasil pengolahan data dan hasil wawancara dengan pihak pengelola sistem informasi akademik dapat dijadikan sebagai temuan penelitian, berdasarkan hasil perhitungan tingkat kematangan, maka dapat melihat gap yang ada dan dapat menentukan nilai expected yang akan jadikan rekomendasi dari masing-masing kontrol objectif yang perlu dilakukan perbaikan.

3.4 Pemrosesan dan Analisa Data

3.4.1 Melakukan Uji Kematangan

Alat yang digunakan untuk memetakan posisi proses sistem informasi akademik adalah dengan menggunakan kuesioner. Temuan untuk masing-masing objective berdasarkan hasil kuesioner dan wawancara, maka gap yang ada dapat ditentukan tingkat expected maturity level sebagaimana tujuan dari organisasi dan pencapaian visi misi organisasi pada level 3 atau define process untuk penggunaan sistem infromasi akademik, maka hasil ini dapat dijadikan rekomendasi untuk setiap control objective yang memiliki gap maturity level berdasarkan detail control objective.

Penelitian kemudian dilanjutkan dengan melakukan penilaian tingkat kematangan saat ini (current maturity level) melalui kuesioner dan interview kepada reponden yang terkait dengan sistem informasi akademik.

Setelah melakukan pemeriksaan dan mendokumentasikan bukti-bukti pemeriksaan, setiap pernyataan dinilai tingkat kepatutannya sesuai dengan hasil pemeriksaan yang ada menggunakan kriteria penilaian yang ada dalam standar penilaian maturity level.

Tingkat kriteria yang digunakan meliputi non-eksisten yang memiliki nilai 0 (nol) hingga ke tingkat optimal yang memiliki nilai 5 (lima). Jumlah kriteria nilai yang ada dibagi dengan jumlah seluruh pernyataan dalam satu kontrol keamanan untuk mendapatkan nilai maturity level pada kontrol keamanan tersebut. Contoh kerangka kerja perhitungan maturity level dapat dilihat pada Tabel 3.4berikut :

Tabel 3.4 Contoh Kerangka Kerja Perhitungan Maturity Level

Klausul		:	9.	Keamanan Fisik dan Lingkungan							
Kategori Keamanan Utama		:	9.1	Wilayah Aman							
Kontrol Keamanan		:	9.1.1	Pembatas Keamanan Fisik							
No	**Pernyataan**	**Hasil Pemeriksaan**			**Nilai**						**Σ**
					0	**1**	**2**	**3**	**4**	**5**	
1.	Terdapat perlindungan keamanan fisik (dinding, kartu akses masuk atau penjaga pintu.	Perlindungan keamanan fisik telah dikendalikan dengan baik. Terdapat pagar besi harmonika, dinding, sekat, penjaga pintu, resepsionis berawak, kartu tanda pengenal, dan ruangan server memiliki batasan akses masuk dan kunci tersendiri									

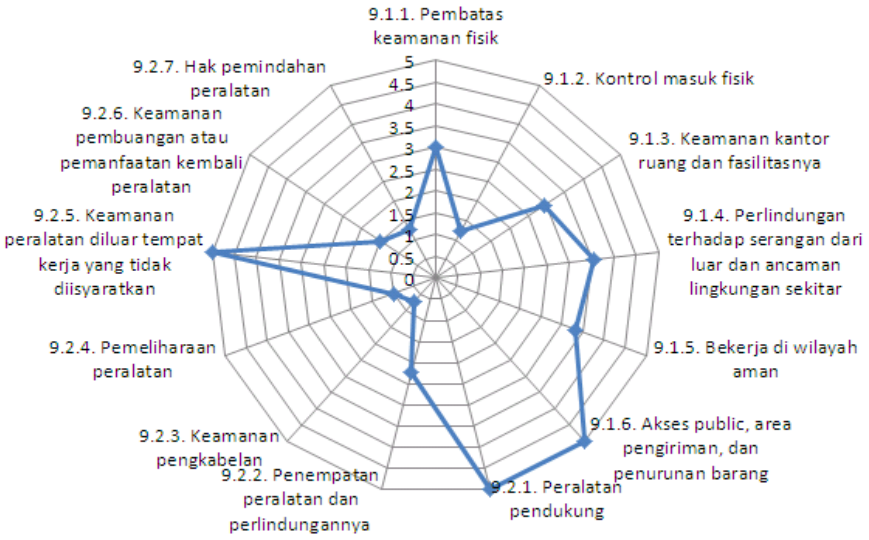
		Bukti: a. Pagar besi harmonika b. Dinding dan sekat c. Penjaga pintu d. Resepsionis e. Kartu tanda pengenal f. Ruangan server memiliki batasan akses masuk dan kunci tersendiri.							

Setelah maturity level setiap kontrol keamanan ISO diketahui, maka langkah selanjutnya adalah menghitung maturity level setiap objektif kontrol yang diambil dari rata-rata maturity level setiap kontol keamanan yang ada. Dan rata-rata maturity level keseluruhan objektif kontrol yang ada pada klausul bersangkutan merupakan maturity level pada klausul tersebut. Contoh tabel penentuan maturity level ISO 27002 dapat dilihat pada Tabel 3.5 berikut ini :

Tabel 3.5 Contoh Tabel Penentuan Maturity Level ISO 27002

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
9. Keamanan Fisik dan Lingkungan	9.1. Wilayah Aman	9.1.1 Pembatas keamanan fisik	3.00	3.18
		9.1.2 Kontrol masuk fisik	1.22	
		9.1.3 Keamanan kantor ruang dan fasilitasnya	2.94	
		9.1.4 Perlindungan terhadap serangan dari luar dan ancaman lingkungan sekitar	3.56	
		9.1.5 Bekerja di wilayah aman	3.33	
		9.1.6 Akses public, area pengiriman, dan penurunan barang	5.00	
	9.2. Keamanan Peralatan	9.2.1 Peralatan pendukung	5.00	2.38
		9.2.2 Penempatan peralatan dan perlindungannya	2.22	
		9.2.3 Keamanan pengkabelan	0.71	
		9.2.4 Pemeliharaan peralatan	1.00	
		9.2.5 Keamanan peralatan diluar tempat kerja yang tidak diisyaratkan	5.00	
		9.2.6 Keamanan pembuangan atau pemanfaatan kembali peralatan	1.50	
		9.2.7 Hak pemindahan peralatan	1.25	
Marturity level Klausul 9				**2.78**

Setelah dihasilkan nilai maturity level yang didapat dari seluruh rata-rata nilai tingkat kemampuan kontrol keamanan, selanjutnya nilai-nilai tersebut akan direpresentasikan ke dalam diagram jaring yang ada pada Gambar 3.5.



Gambar 3.5 Contoh Representatif Nilai Maturity Level Klausul 9

3.4.2 Gap Analisis

Gap analisis ditentukan setelah nilai kematangan dihitung. Analisis gap digunakan sebagai alat evaluasi untuk melakukan perbandingan kinerja actual dengan kinerja potensial atau yang diharapkan.

Analisis ini juga mengidentifikasi tindakan-tindakan apa saja yang diperlukan untuk mengurangi kesenjangan atau mencapai kinerja yang diharapkan pada masa datang. Lebih dari itu analisis ini juga memperkirakan waktu, biaya, dan sumberdaya yang dibutuhkan untuk mencapai keadaan perusahaan yang diharapkan. Sebagaimana dijelaskan dalam Tabel 3.6 berikut ini :

Tabel 3.6 Contoh Hasil Perhitungan Gap Analisis

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**

3.4.3 Melakukan Dokumentasi Data dan Bukti

Pada tahapan ini dilakukan pengarsipan dan pendokumentasian baik berupa data maupun bukti-bukti hasil temuan atau fakta yang ada dari hasil pemeriksaan yang telah dilakukan.Bukti-bukti tersebut dapat berupa foto, rekaman audio, data digital, video, serta surat-surat pendukung sebagai bahan laporan.

Contoh dari bentuk pendokumentasian fakta dan bukti dapat dilihat pada Tabel 3.7dibawahini :

Tabel 3.7 Contoh Pendokumentasian Berdasarkan Fakta dan Bukti

Klausul	:	9.	Keamanan Fisik dan Lingkungan	
Kategori Keamanan Utama	:	9.1	Wilayah Aman	
Kontrol Keamanan	:	9.1.1	Pembatas Keamanan Fisik	
No	**Pernyataan**			**Hasil Pemeriksaan**
1.	Terdapat perlindungan keamanan fisik (dinding, kartu akses masuk atau penjaga pintu.			

3.5 Rekomendasi

Pada proses penentuan temuan dan rekomendasi langkah yang dilakukan adalah memeriksa data profil organisasi, kebijakan, standar, prosedur dan portopolio serta mengobservasi standard operating procedure, melakukan wawancara kepada pengguna sistem informasi akademik hingga melakukan pemeriksaan atau pengujian baik secara compliance test maupun substantive test. Seluruh aktivitas tersebut menghasilkan bukti (evidence) yang berarti terkait dengan sistem yang berlangsung di organisasi.

Masih dibutuhkannya banyak evaluasi dan perbaikan yang harus dijalankan untuk meningkatkan keamanan informasi pada universitas, serta menjadi acuan untuk memperoleh ISMS certification dengan standar ISO 27002. Ada proses yang telah dilakukan dengan baik, namun terdapat juga beberapa temuan yang masih perlu diperbaiki. Diadakan analisa sebab dan akibat untuk temuan tersebut, serta diberikan rekomendasi untuk universitas agar penerapan kontrol keamanan dapat diterapkan dengan lebih baik dan sesuai dengan standar ISO 27002.Berikut dibawah ini adalah contoh Tabel 3.8 mengenai hasil temuan dan rekomendasi.

Tabel 3.8 Contoh Hasil Temuan dan Rekomendasi

Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
9 Keamanan Fisik dan Lingkungan	9.1 Wilayah Aman	9.1.1 Pembatas Keamanan Fisik		
		9.1.2 Kontrol Masuk Fisik		

BAB 4
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 27002:2013 yang melibatkan 3 klausul, 13 objek kontrol, dan 43 kontrol keamanan.

4.1 Hasil Penetapan Klausul

Setelah dilakukan observasi maka hasil yang diperoleh adalah penetapanruang lingkup analisisyaitu keamanan sistem informasi dan standar yang digunakanadalah ISO 27002. Dari tahap identifikasi ini dihasilkan juga pemetaan klausul,objektif kontrol, dan kontrol keamanan yang telah disepakati oleh Universitas.

Klausul yang digunakan adalah klausul 9 tentang Keamanan Fisik dan Lingkungan, klausul 11 tentang Keamanan Fisik dan Lingkungan, dan klausul 14 tentang Akuisisi Sistem Informasi, Pembangunan, dan Pemeliharaan.

Klausul, objektif kontrol, dan kontrol keamanan yang tidak digunakan dapat dilihat pada Tabel 4.1 sedangkan klausul, objektif kontrol, dan kontrol keamanan yang telah ditetapkan dapat dilihat pada Tabel 4.2. Penentuan ruang lingkup yang telah disepakati ini juga dituangkan ke dalam engagement letter atau surat kesepakatan (lampiran C.1)

Tabel 4.1 Klausul, Objektif Kontrol dan Kontrol Keamanan ISO 27002 yang Tidak Digunakan

Klausul	Kontrol Keamanan	Alasan
5. Kebijakan Keamanan	Pada seluruh kontrol keamanaan	Belum memiliki kebijakan khusus tentang keamanan informasi
6. Organisasi Keamaan Informasi	Pada seluruh kontrol keamanaan	Belum memiliki pengaturan untuk menangani keamanan informasi
7. Keamanan Sumber Daya Manusia	Pada seluruh kontrol keamanaan	Sudah terintegrasi dengan ISO 9001
8. Manajemen Aset	Pada seluruh kontrol keamanaan	Kontrol keamanan yang ada dalam Klausul 8, tidak diijinkan untuk mengaudit manajemen aset organisasi
10. Kriptografi	Pada seluruh kontrol keamanaan	Tidak diperlukan untuk saat ini, dan sebagian sudah menggunakan .
13. Keamanan Komunikasi	Pada seluruh kontrol keamanaan	Kontrol keamanan yang ada dalam Klausul 13, tidak diijinkan untuk dilakukan analisis

Klausul	Kontrol Keamanan	Alasan
12. Keamanan Operasi	Pada seluruh kontrol keamanaan	Kontrol keamanan yang ada dalam Klausul 12, tidak diijinkan untuk dilakukan analisis
15. Hubungan Pemasok	Pada seluruh kontrol keamanaan	Sudah menggunakan standard ISO 9001
16. Manajemen Insiden Keamanan Informasi	Pada seluruh kontrol keamanaan	Kontrol keamanan yang ada dalam Klausul 16, tidak diijinkan untuk dilakukan analisis
17. Aspek Keamanan Informasi Manajemen Kesinambungan Bisnis	Pada seluruh kontrol keamanan	Kontrol keamanan yang ada dalam Klausul 17, tidak diijinkan untuk dilakukan analisis
18. Kepatutan	Pada seluruh kontrol keamanan	Sudah dilakukan pada ISO 9001

Tabel 4.2 Klausul, Objektif Kontrol dan Kontrol Keamanan ISO 27002 yang Telah Ditetapkan

No	Klausul	Objektif Kontrol	Kontrol Keamanan
	9 Kontrol Akses	9.1 Persyaratan bisnis untuk kontrol akses	9.1.1 Kebijakan kontrol akses
		9.2 Manajemen akses user	9.2.1 Registrasi pengguna
			9.2.2 Manajemen hak istimewa atau khusus
			9.2.3 Manajemen password user
			9.2.4 Tinjauan terhadap hak akses user
		9.3 Tanggung jawab pengguna	9.3.1 Penggunaan password
			9.3.2 Peralatan pengguna yang tidak dijaga
			9.3.3 Kebijakan clear desk dan clear screen
		9.4 Kontrol akses jaringan	9.4.1 Kebijakan penggunaan layanan jaringan
			9.4.2 Otentikasi pengguna untuk melakukan koneksi keluar
			9.4.5 Pemisahan dengan jaringan
			9.4.6 Kontrol terhadap koneksi jaringan
			9.4.7 Kontrol terhadap routing jaringan
		9.5 Kontrol akses sistem operasi	9.5.1 Prosedur log-on yang aman
			9.5.2 Identifikasi dan otentifikasi user
			9.5.3 Sistem manajemen password
			9.5.4 Penggunaan utilitas sistem
			9.5.5 Sesi time-out
			9.5.6 Batasan waktu koneksi
		9.6 Kontrol akses informasi dan aplikasi	9.6.1 Pembatasan akses informasi

No	Klausul	Objektif Kontrol	Kontrol Keamanan
			9.6.2 Isolasi sistem yang sensitif
		9.7 Komputasi bergerak dan teleworking	9.7.1 Komunikasi dan terkomputerisasi yang bergerak
	11 Keamanan Fisik dan Lingkungan	11.1 Wilayah aman	11.1.1 Pembatas keamanan fisik
			11.1.2 Kontrol masuk fisik
			11.1.3 Keamanan kantor, ruang, dan fasilitasnya
			11.1.4 Perlindungan terhadap serangan dari luar dan ancaman lingkungan sekitar
			11.1.5 Bekerja di wilayah aman
			11.1.6 Akses publik, area pengiriman, dan penurunan barang
		11.2 Keamanan peralatan	11.2.1 Penempatan peralatan dan perlindungannya
			11.2.2 Utilitas pendukung
			11.2.3 Keamanan pengkabelan
			11.2.4 Pemeliharaan peralatan
			11.2.5 Keamanan peralatan di luar tempat kerja yang tidak diisyaratkan
			11.2.6 Keamanan pembuangan atau pemanfaatan kembali peralatan
			11.2.7 Hak pemindahan peralatan
	14 Akuisisi Sistem Informasi, Pembangunan, dan Pemeliharaan	14.1 Persyaratan keamanan untuk sistem informasi	14.1.1 Analisa dan spesifikasi persyaratan keamanan
		14.2 Pemrosesan yang benar dalam aplikasi	14.2.1 Validasi data input
			14.2.2 Kontrol untuk pemrosesan internal
			14.2.4 Validasi data output
		14.5 Keamanan dalam pembangunan dan proses-proses pendukung	14.5.1 Prosedur tambahan kontrol
			14.5.3 Pembatasan perubahan paket software
			12.5.4 Kelemahan informasi
		14.6 Manajemen teknik kelemahan (Vurnerability)	14.6.1 Kontrol terhadap kelemahan secara teknis (Vurnerability)

4.2 Hasil Penentuan Jadwal (*Working Plan*)

Hasil dari proses penyusunan analisis working plan berupa tabel yang berisi tentang aktifitas yang dilakukan selama penelitian berlangsung.

Pelaksanaan analisis keamanan sistem informasi dilakukan secara bertahap sesuai dengan jadwal yang dapat dilihat pada Tabel 4.3 dibawah ini:

Tabel 4.3 Jadwal Kegiatan

No	Kegiatan	Bulan															
		Oktober				Nopember				Desember				Januari			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1.	Studi Literatur																
2.	Penentuan ruang lingkup																
3.	Pengumpulan Bukti ▪ Peninjauan Struktur Organisasi ▪ Peninjauan kebijakan dan prosedur yang terkait dengan TI ▪ Peninjauan standar yang terkait dengan TI																
	▪ Peninjauan dokumentasi pengelolaan SI/TI ▪ Wawancara																
	Pengobservasian proses dan kinerja staff dan karyawan																
4.	Pelaksanaan uji kepatutan																
5.	Penentuan tingkat kematangan																
6.	Penentuan hasil pemeriksaan																
7.	Penyusunan laporan pemeriksaan																

4.3 Hasil Pengumpulan Data

Hasil dokumentasi berisi data maupun bukti yang ada mengenai temuan-temuan yang ditemukan saat pelaksanaan pemeriksaan. Bukti-bukti tersebut dapat berupa foto, rekaman, data atau video.

Hasil dokumentasi dan foto dapat dilihat pada Tabel 4.4 dan selengkapnya dapat dilihat pada Lampiran D.

Tabel 4.4 Hasil Pemeriksaan Pernyataan Pada Kontrol Keamanan Pembatas Keamanan Fisik

Klausul	:	11.	Keamanan Fisik dan Lingkungan
Kategori Keamanan Utama	:	11.1	Wilayah Aman
Kontrol Keamanan	:	11.1.1	Pembatas Keamanan Fisik

No	Pernyataan	Hasil Pemeriksaan
1.	Terdapat perlindungan keamanan fisik (dinding, kartu akses masuk atau penjaga pintu)	Perlindungan keamanan fisik telah dikendalikan dengan baik. Bukti: ▪ Terdapat pagar besi harmonika ▪ Terdapat dinding ▪ Terdapat penjaga pintu ▪ Terdapat resepsionis berawak ▪ Tidak terdapat kartu akses masuk ▪ Terdapat kartu tanda pengenal ▪ Ruangan server memiliki batasan akses masuk dan kunci tersendiri.

4.4 Hasil Pemrosesan Data Uji Kematangan

Berdasarkan analisa dari wawancara dengan auditee, pemeriksaan, dan pengumpulan bukti, maka diperoleh hasil uji kepatutan dari tingkat kematangan untuk masing-masing kontrol.

Adapun tingkat kematangan tersebut diperoleh dari masing-masing analisa yang dapat dilihat pada kerangka kerja perhitungan maturity level pada Lampiran A.

Hasil perhitungan tingkat kematangan hasil audit keamanan sistem informasi adalah sebagai berikut :

a. Hasil Maturity Level Klausul 9: Kontrol Akses

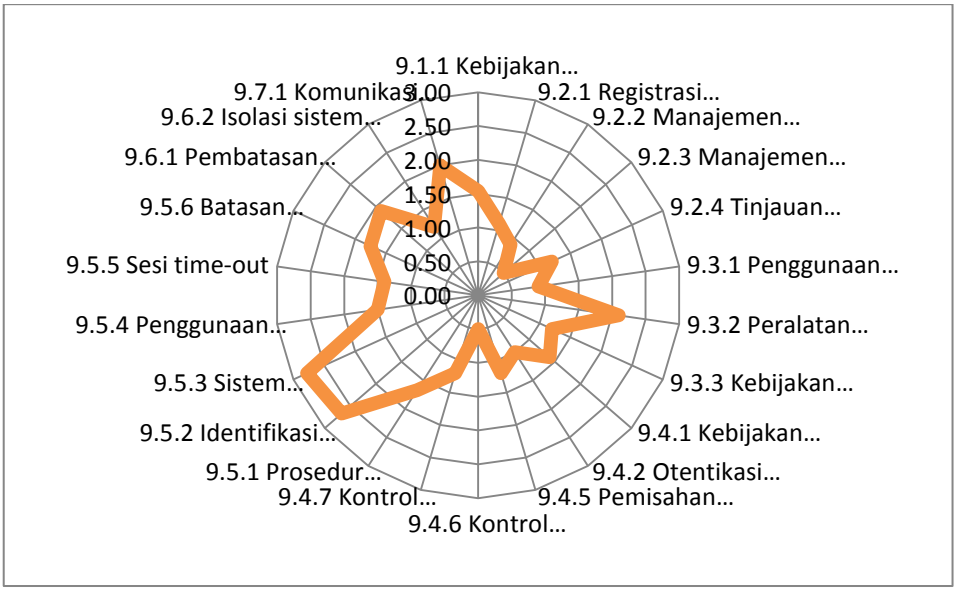
Hasil dari proses perhitungan maturity level pada klausul 9 kontrol akses adalah 1.44 yaitu initial yang berarti tidak ada manajemen proyek, tidak adanya quality assurance, tidak adanya mekanisme manajemen perubahan (change management), tidak ada dokumentasi, adanya seorang ahli yang tahu segalanya tentang perangkat lunak yang dikembangkan, dan sangat bergantung pada kemampuan individual. Hasil tersebut menunjukkan bahwa proses persyaratan bisnis untuk kontrol akses dilakukan secara tidak konsisten dan informal. Hal tersebut dapat dilihat tidak adanya pernyataan resmi yang ditandatangani untuk menjaga password, tidak adanya tinjauan terhadap hak akses user, dan terdapat kebijakan yang masih dilakukan secara informal misalnya kebijakan dan otorisasi terhadap keamanan informasi, persyaratan bisnis kontrol akses, persyaratan keamanan, dan lain-lain. Hasil perhitungan tersebut dapat dilihat pada Tabel 4.5.

Hasil perhitungan maturity level pada klausul 9 kontrol akses dapat direpresentasikan dalam bentuk grafik. Hasil representasi perhitungan maturity level klausul 9 kontrol akses dapat dilihat pada Gambar 4.1.

Tabel 4.5 Hasil Maturity Level Klausul 9:Kontrol Akses

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
9 Kontrol Akses	9.1 Persyaratan bisnis untuk kontrol akses	9.1.1 Kebijakan kontrol akses	1.54	1.54
	9.2 Manajemen akses user	9.2.1 Registrasi pengguna	1.10	0.92
		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 Tanggung jawab pengguna	9.3.1 Penggunaan password	0.90	1.40
		9.3.2 Peralatan pengguna yang tidak dijaga	2.10	
		9.3.3 Kebijakan clear desk dan clear screen	1.20	
	9.4 Kontrol akses jaringan	9.4.1 Kebijakan penggunaan layanan jaringan	1.40	1.06

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
		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 Kontrol akses sistem operasi	9.5.1 Prosedur log-on yang aman	1.67	1.96
		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	
		9.5.6 Batasan waktu koneksi	1.75	
	9.6 Kontrol akses informasi dan aplikasi	9.6.1 Pembatasan akses informasi	1.90	1.55
		9.6.2 Isolasi sistem yang sensitif	1.20	
	9.7 Komputasi bergerak dan bekerja dari lain tempat/teleworking	9.7.1 Komunikasi dan terkomputerisasi yang bergerak	2.00	2.00
Marturity level Klausul 9				**1.44**



Gambar 4.1 Representasi Nilai Maturity Level Klausul 9 Kontrol Akses

b. Hasil Maturity Level Klausul 11 : Keamanan Fisik dan Lingkungan

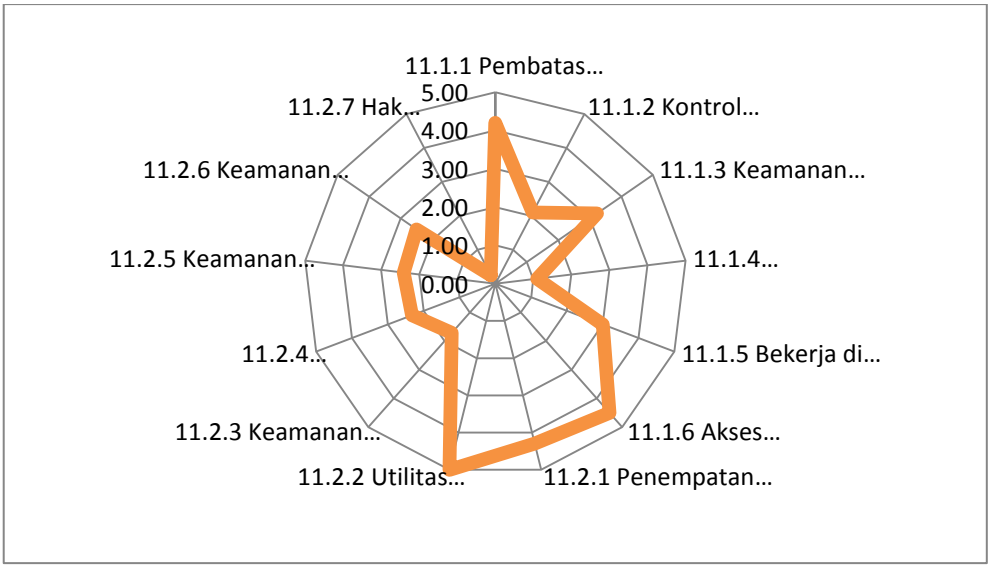
Hasil dari proses perhitungan maturity level pada klausul 11 wilayah aman adalah 2.47 yaitu define process yang berarti proses standar telah berjalan sesuai dengan definisi. Hasil tersebut menunjukkan bahwa SDLC sudah ditentukan, ada komitmen untuk mengikuti SDLC dalam keadaan apapun, kualitas proses dan produk masih bersifat kualitatif atau hanya perkiraan saja, tidak menerapkan Activity Based Costing, dan tidak adanya mekanisme umpan balik yang baku.

Hal tersebut dapat dilihat dengan adanya beberapa prosedur yang belum terdokumentasi dan masih banyak kontrol yang belum dilakukan misalnya pemasangan tanda bahaya, log datang dan perginya pengunjung, pemeliharaan peralatan yang terabaikan, tidak adanya catatan peminjaman peralatan, dan lain-lain. Hasil perhitungan maturity level pada klausul 11 wilayah aman dapat direpresentasikan dalam bentuk Tabel 4.6. Hasil representasi perhitungan maturity level klausul 11 wilayah aman dalam bentuk grafik dapat dilihat pada Gambar 4.2.

Tabel 4.6 Hasil Maturity Level Klausul 11 : Keamanan Fisik dan Lingkungan

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
11 Keamanan Fisik dan Lingkungan	11.1 Wilayah aman	11.1.1 Pembatas keamanan fisik	4.14	3.01
		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	
		11.1.6 Akses publik, area pengiriman dan penurunan barang	4.50	
	11.2 Keamanan peralatan	11.2.1 Penempatan peralatan dan perlindunganya	4.30	2.64
		11.2.2 Utilitas pendukung	5.00	
		11.2.3 Keamanan pengkabelan	1.71	
		11.2.4 Pemeliharaan peralatan	2.32	
		11.2.5 Keamanan peralatan di luar tempat kerja yang tidak diisyaratkan	2.41	

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
		11.2.6 Keamanan pembuangan atau pemanfaatan kembali peralatan	2.50	
		11.2.7 Hak pemindahan peralatan	0.25	
Marturity level Klausul 11				**2.47**



Gambar 4.2 Representasi Hasil Maturity Level Klausul 11 : Keamanan Fisik dan Lingkungan

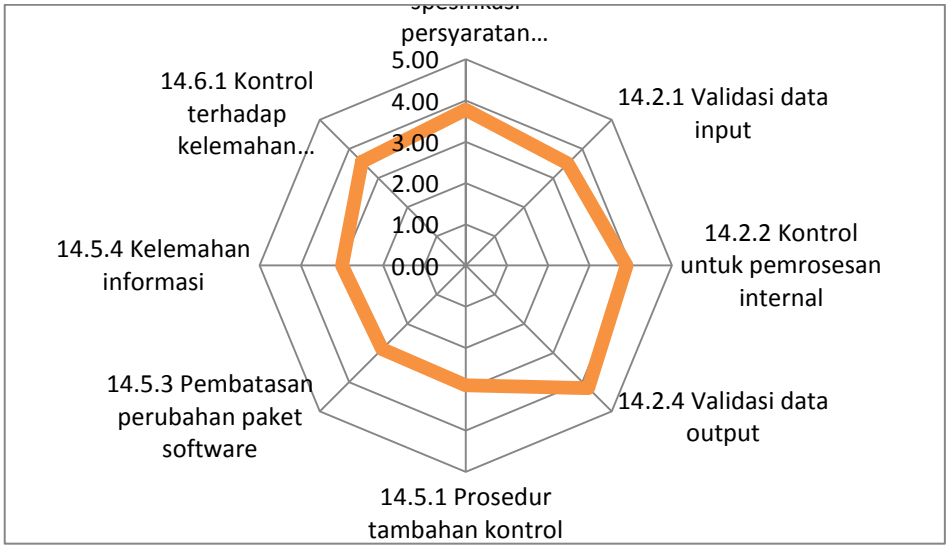
c. Hasil Maturity Level Klausul 14 : Akuisisi Sistem Informasi, Pembangunan, dan Pemeliharaan

Hasil dari proses perhitungan maturity level pada 14 akuisisi sistem informasi, pembangunan, dan pemeliharaan adalah 3.63 yaitu manage yang berarti sudah ada Activity Based Costing dan digunakan untuk estimasi proyek berikutnya, proses penilaian kualitas perangkat lunak dan proyek bersifat kuantitatif, terjadi pemborosan biaya untuk pengumpulan data karena proses pengumpulan data masih dilakukan secara manual, cenderung belum jelas disebabkan karena manusia ketika diperhatikan perilakunya cenderung berubah, tidak ada mekanisme pencegahan defect dan adanya mekanisme umpan balik. Hasil tersebut menunjukkan bahwa proses akuisisi sistem informasi, pembangunan, dan pemeliharaan yang ada pada organisasi dilakukan secara konsisten dan formal. Hal tersebut dapat dilihat dengan adanya modifikasi pada software telah diuji, hanya saja belum dilakukan pada suatu badan yang independen.Hasil perhitungan tersebut dapat dilihat pada Tabel 4.7.

Hasil perhitungan maturity level pada klausul 14 akuisisi sistem informasi, pembangunan, dan pemeliharaan dapat direpresentasikan dalam bentuk grafik. Hasil representasi perhitungan maturity level klausul 12 akuisisi sistem informasi, pembangunan, dan pemeliharaan dapat dilihat pada Gambar 4.3.

Tabel 4.7 Hasil Maturity Level Klausul 14:Akuisisi Sistem Informasi, Pembangunan, dan Pemeliharaan

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
14 Akuisisi Sistem Informasi, Pembangunan, dan Pemeliharaan	14.1 Persyaratan keamanan untuk sistem informasi	14.1.1 Analisa dan spesifikasi persyaratan keamanan	3.78	3.78
	14.2 Pemrosesan yang benar dalam aplikasi	14.2.1 Validasi data input	3.50	3.87
		14.2.2 Kontrol untuk pemrosesan internal	3.90	
		14.2.4 Validasi data output	4.20	
	14.5 Keamanan dalam pembangunan dan proses-proses pendukung	14.5.1 Prosedur tambahan kontrol	2.90	2.92
		14.5.3 Pembatasan perubahan paket software	2.87	
		14.5.4 Kelemahan informasi	3.00	
	14.6 Manajemen teknik kelemahan (Vurnerability)	14.6.1 Kontrol terhadap kelemahan secara teknis (Vurnerability	3.56	3.56
Marturity level Klausul 14				**3.63**



Gambar 4.3 Representasi Nilai Maturity Level Klausul 14 Akuisisi Sistem Informasi,Pembangunan, dan Pemeliharaan

d. Hasil Pembahasan Pemeriksaan Keamanan Sistem Informasi Akademik.

Berdasarkan audit keamanan sistem informasi yang telah dilakukan, kebocoran informasi yang terjadi merupakan akibat dari adanya penyalahgunaan password yang terjadi. Berdasarkan temuan-temuan hasil audit penyalahgunaan password yang terjadi disebabkan karena peraturan Unipdu yang kurang tegas dan kurang spesifik untuk kerahasiaan password, belum adanya perjanjian atau pernyataan tertulis yang ditandatangani untuk benar-benar menjaga kerahasiaan password masing-masing, penerapan manajemen password yang tidak sesuai standar, tidak ada tinjauan terhadap hak akses user, dan kurangnya kesadaran serta pengetahuan karyawan terhadap pentingnya merahasiakan password, kontrol keamanan 11.2.3manajemen password user yang hanya memiliki nilai 0.50, kontrol keamanan 11.2.4 tinjauan terhadap akses user yang bernilai 1.20, dan kontrol keamanan 11.3.1 penggunaan password yang hanya memiliki nilai 0.90.

Kerusakan-kerusakan peralatan sistem informasi yang terjadi dan sistem yang sering hang merupakan salah satu akibat dari kurangnya pemeliharaan yang dilakukan oleh perusahaaan, kurangnya manajemen kapasitas yang dilakukan, dan pemindahan peralatan yang kurang dimanajemen. Hal tersebut dapat dilihat pada hasil maturity level kontrol keamanan 11.2.4 pemeliharaan peralatan yang memiliki nilai 2.32 kontrol keamanan 11.2.7 hak pemindahan peralatan yang bernilai 0.25, kontrol keamanan 10.3.1 manajemen kapasitas yang memiliki nilai 0.811.

Gangguan-gangguan sistem yang terjadi merupakan akibat dari serangan virus yang mengacau keberlangsungan operasional Unipdu. Berdasarkan temuan-temuan hasil audit permasalahan virus yang terjadi disebabkan oleh tidak ada pelatihan penggunaan perlindungan virus, tidak dilakukan penyelidikan secara formal tentang keberadaan kelompok data tanpa persetujuan, tidak dilakukan penyelidikan secara formal tentang perubahan tanpa otorisasi, dan kurangnya pengetahuan karyawan tentang virus. Hal tersebut dapat dilihat pada hasil maturity level kontrol keamanan 11.4.1 kontrol terhadap kode bahaya dengan nilai 1.47. Selain itu juga ditemukan kelemahan-kelemahan sistem informasi akademik dalam hal pendokumentasian prosedur-prosedur yang ada, pencatatan insiden keamanan informasi, dan rencana kelangsungan bisnis.

Dari hasil perhitungan tingkat kematangan keamanan informasi, dimana tingkat kematangan yang menjadi acuan dalam penelitian ini adalah pada level 3 (Define). Berdasarkan hasil perhitungan yang telah dilakukan maka dapat diperoleh bahwa tingkat kematangan keamanan informasi sistem informasi akademik adalah berada pada rata-rata

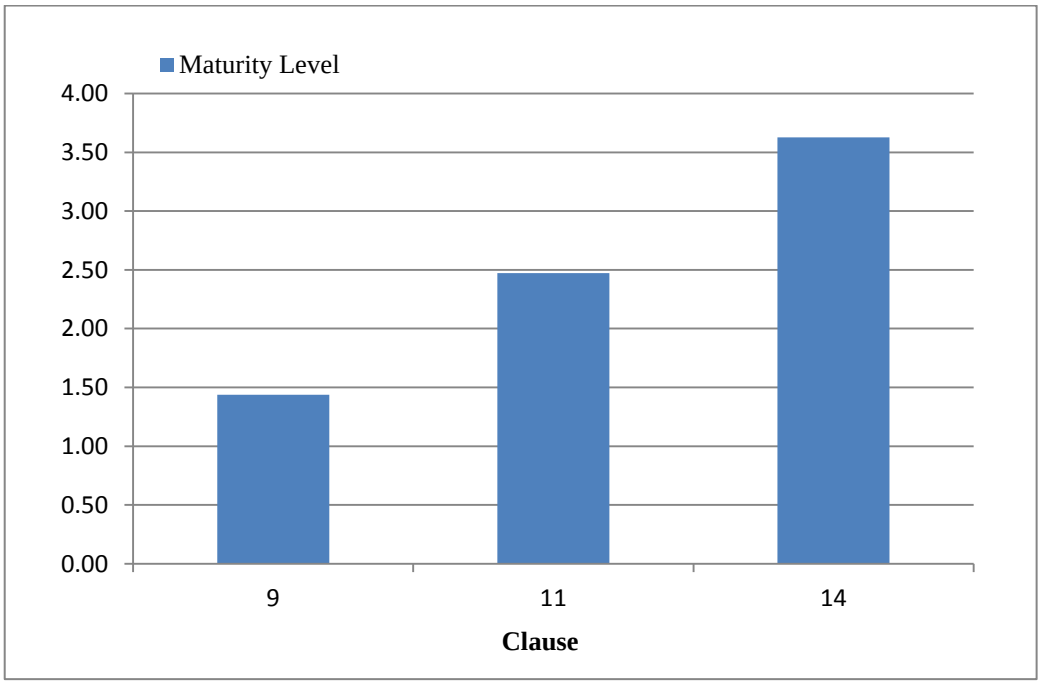
level 1 berarti bahwa saat ini keamanan informasi sistem informasi akademik masih perlu diperbaiki karena masih berada di bawah level 3. Namun ada beberapa klausa yang memiliki nilai di atas 3 yaitu , klausa 14 yang berarti sudah memenuhi standar ISO 27002.

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 4.8 dibawah ini :

Tabel 4.8 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 4.4 dibawah ini :



Gambar 4.4 Representasi Pengukuran Grafik Pada Maturity Level

4.5 Gap Analisis

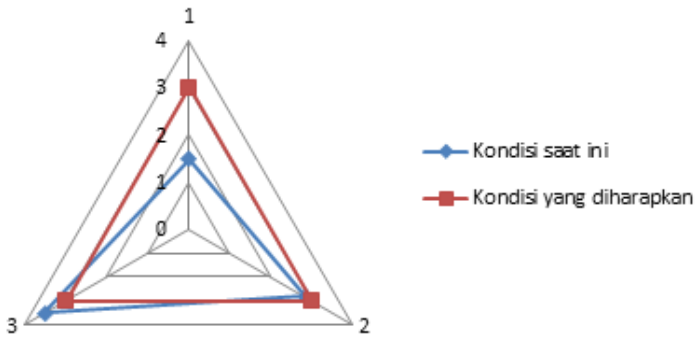
Berdasarkan perhitungan tingkat kematangan keamanan informasi dari sistem informasi akademik saat ini bernilai 2,51 (define) masuk dalam level 3 dan diharapkan tingkat kematangannya adalah 5 (dioptimalkan). Alasannya adalah kesiapan organisasi dalam kebijakan, prosedur dan proses keamanan lapangan, dan keamanan informasi pengendalian akses, dapat dilihat Tabel 4.9 di bawah ini:

Tabel 4.9 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 4.9 diatas, 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 4.5, berikut:



Gambar 4.5 Representasi Pengukuran Grafik Pada Gap Analisis

Seperti yang ditunjukkan pada Gambar 4.5, 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.

4.6 Rekomendasi

Penyusunan temuan dan rekomendasi sebagai hasil evaluasi dari pelaksanaan audit keamanan sistem informasi ini muncul setelah dilakukan pembandingan antara apa yang seharusnya dilakukan dengan proses yang sedang berlangsung pada penggunaan sistem informasi akademik.

Dari hasil temuan tersebut kemudian diberikan rekomendasi yang dapat digunakan untuk perbaikan proses sistem informasi di kemudian hari. Salah satu contoh hasil temuan dan rekomendasi pada klausul 11 keamanan fisik dan lingkungan dengan kontrol keamanan 11.1.2 kontrol masuk fisik dapat dilihat pada Tabel 4.10 dan untuk selengkapnya dapat dilihat pada Lampiran C..

Tabel 4.10 Hasil Temuan Dan Rekomendasi Klausul 9 : Akses Kontrol

Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
9 Akses Kontrol	9.1 Persyaratan Bisnis untuk kontrol akses	9.1.1 Kebijakan kontrol akses	Terdapat kebijakan dan otorisasi terhadap keamanan informasi persyaratan bisnis kontrol akses, persyaratan keamanan, namun masik dilakukan secara informal dan belum terdokumentasi (Bukti: Hasil pemeriksaan pada Lampiran C.1 kontrol keamanan 9.1.1)	✓ Melakukan review dan observasi dilapanagan ✓ Mendesain kebijakan dan sangsinya ✓ Mendokumentasikan kebijakan-kebijakan tersebut ✓ Melakukan distribusi informasi atau pengumuman mengenai kebijakan tersebut ✓ Memantau dan mengevaluasi pelaksanaan kebijakan yang telah dilaksanakan ✓ Contoh kebijakan control akses :

				organisasi harus melakukan pemisahan lingkungan (environment) untuk pengembangan, uji coba, dan produksi, termasuk pembatasan akses ke masing-masing lingkungannya (Ref. Pedoman Penerapan Manajemen Resiko dalam penggunaan Teknologi Informasi)

Tabel 4.11 Hasil Temuan Dan Rekomendasi Klausul 11 : Keamanan Fisik dan Lingkungan

Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
11 Keamanan Fisik dan Lingkungan	11.1 Wilayah Aman	11.1.2 Kontrol Masuk Fisik	Tidak ada pencatatan waktu kunjungan kedatangan maupun kepergian untuk pengunjung. (Bukti: Hasil pemeriksaan pada Lampiran C.2)	✓ Membuat buku tamu untuk mencatat kegiatan dan waktu berkunjung ✓ Mengajukan ke direksi untuk penambahan peralatan kontrol otentikasi seperti kartu gesek atau peralatan biometrik lainnya seperti finger print. (Ref: Pedoman Penerapan Manajemen Risiko dalam Penggunaan Teknologi Informasi).

Tabel 4.12 Hasil Temuan Dan RekomendasiKlausul 14 :Akuisisi Sistem Informasi, Pembangunan, dan Pemeliharaan

Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
14 Akuisisi Sistem Informasi, Pembangunan, dan Pemeliharaan	14.1 Persyaratan keamanan untuk sistem informasi	14.1.1 Analisa dan spesifikasi persyaratan keamanan	Untuk mengatasi penyusupan terhadap jaringan belum ada pemberitahuan yang signifikan kepada penanggungjawab sistem (Bukti: Hasil pemeriksaan pada Lampiran C.3)	✓ Membuat aplikasi pemberitahuan jika terjadi penyusupan ✓ Periksa aplikasi sistem informasi akademik secara berkala untuk mendeteksi celah keamanan yang terjadi . (Ref: SNORT, Acunetix, PHP).

Tabel 4.13 Hasil Pelaporan Temuan

Ringkasan	Temuan
Dari hasil pemeriksaan keamanan sistem informasi pada sistem informasi akademik yang telah dilakukan, maka didapatkan kesimpulan berupa : 1. Perencanaan keamanan sistem informasi akademik telah dilakukan sesuai standar, dimulai dengan melakukan perencanaan dan persiapan, pelaksanaan hingga pelaporan pemeriksaan.	**Hasil Tingkat Kematangan** Klausul 9 : 1.44 Klausul 11 : 2.47 Klausul 14 : 3.63 **Hasil Pemeriksanaan** 1. Ditemukannya beberapa kasus penyalahgunaan password yang dapat mengancam kerahasiaan sistem

Ringkasan	Temuan
2. Kebocoran informasi yang terjadi merupakan akibat dari adanya penyalahgunaan password yang terjadi. Penyalahgunaan password disebabkan karena peraturan organisasi yang kurang tegas dan kurang spesifik untuk kerahasiaan password masing-masing. Kurangnya kesadaran serta pengetahuan karyawan terhadap pentingnya merahasiakan password. Berdasarkan hasil pemeriksaan, temuan, dan bukti yang didapatkan maka rekomendasi yang tujukan kepada organisasi adalah : a. Membuat pernyataan tertulis pada masing-masing karyawan bahwa karyawan telah memahami tentang kondisi aksesnya dan wajib mengamankannya dan disertai dengan tandatangan karyawan. b. Melakukan pengkajian terhadap kasus penyalahgunaan password. c. Monitoring implementasi pencegahan penyalahgunaan password. d. Mempertegas sangsi yang akan diberikan terhadap penyalahgunaan password. 3. Terdapat banyak kebijakan dan prosedur yang belum terdokumentasi bahkan ada beberapa tindakan dalam Unipdu yang dilakukan berdasarkan spontanitas dan tanpa ada aturan baku yang bersifat formal. Kerusakan-kerusakan peralatan sistem informasi yang terjadi merupakan salah satu akibat kurangnya pemeliharaan yang dilakukan oleh Unipdu, kurangnya manajemen kapasitas yang dilakukan dan pemindahaan peralatan yang kurang terkordinasi.	2. Kurangnya pemeliharaan terhadap fasilitas pemrosesan informasi yang dapat menyebabkan sistem menjadi sering hang, jaringan down, hingga terbakarnya media penyimpanan yang menyebabkan hilangnya data-data mahasiswa dan karyawan. 3. Adanya kejadian penembusan sistem informasi akademik oleh mahasiswa yang ingin merekayasa nilai matakuliah menandakan perlunya pembuatan sebuah sistem manajemen insiden keamanan informasi agar kedepannya peristiwa tersebut bisa dicegah dan ditangani dengan lebih baik dari sebelumnya. 4. Server Sistem informasi akademik yang terkadang mati karena Gangguan listrik dari PLN perlu mendapat perhatian khusus denganmenyediakan UPS berbasis trafo atau genset dengan daya yang besar agar mampu mempertahankan computerserver tetap menyala ketika pemadaman 5. Sudah adanya prosedur keamanan untuk melindungi akses ke ruangan pengolahan informasi 6. Sudah adanya prosedur untuk merespon kesalahan validasi, pendefinisian tanggung jawab semua personelyang terlibat dalam proses masukan data.

BAB 5
Penutup

5.1 Kesimpulan

Dari hasil analisis keamanan sistem informasi yang telah dilakukan, maka didapatkan kesimpulan sebagai berikut:

a. Peranan Standar ISO 27002 dalam menjaga informasi yang tersimpan adalah sebagai acuan dalam melakukan kontrol keamanan sistem informasi berdasarkan resiko, peraturan, hukum dan undang-undang serta prinsip, tujuan dan kebutuhan informasi pada sistem informasi akademik. Penerapan standarisasi keamanan informasi pada sistem informasi akademik berdasarkan ISO-27002 masih belum siap karena dari tiga klausa yang ditetapkan, hanya satu klausa saja yang baru memenuhi standar tingkat kematangan yaitu klausa akuisisi sistem informasi, pengembangan dan pemeliharaan.
b. Tingkat kematangan keamanan informasi pada sistem informasi akademik masih berada di tingkat kedua (Initial/ad hoc) yaitu pada klausul akses kontrol. Untuk klausa keamanan fisik dan lingkungan pada tingkat kedua (Repeatable but invinite), serta pada klausa akuisisi sistem informasi, pengembangan dan pemeliharaan berada pada tingkat empat (managed).
c. Terdapat kebijakan dan prosedur yang belum terdokumentasi, bahkan ada beberapa tindakan dalam organisasi yang dilakukan berdasarkan spontanitas dan tanpa ada aturan baku yang bersifat formal

5.2 Saran

Saran yang dapat diberikan bagi pengembangan yang berkaitan dengan pencapaian hasil yang optimal dari pemeriksaan keamanan sistem sistem informasi ini sebagai berikut:

a. Diharapkan pengelola sistem informasi akademik dapat melakukan perbaikan manajemen keamanan sistem informasi, aturan, dan prosedur keamanan sistem informasi agar ancaman-ancaman terkait keamanan informasi dapat diminimalisir.

b. Diharapkan bagi pengembang dapat melakukan tata kelola keamanan sistem informasi dan audit keamanan sistem informasi kembali dengan menggunakan keseluruhan klausul dan kontrol keamanan ISO 27002 setelah pihak pengelola sistem informasi akademik melakukan perbaikan keamanan sistem informasinya.

DAFTAR PUSTAKA

Al Fatta, Hanif (2009). Analisis dan Perancangan Sistem Informasi untuk Keunggulan Bersaing Perusahaan dan Organisasi Modern. Yogjakarta: Andi

Asmuni, I. dan Firdaus, R. 2005. Peranan Pengendalian Berbasis Audit Sistem Informasi untuk Pengembangan Strategi Perusahaan Berbasis Komputer (Suatu Bahasan Teoritis atas Faktor Penentu Keberhasilan dan Penyimpangan Penerapan Sistem Informasi dalam Suatu Organisasi Usaha), Seminar Nasional Aplikasi Teknologi Informasi 2005. Yogyakarta.

Badara, M., & Saidin, S. (2013). Impact of the effective internal control system on the internal audit effectiveness at local government level. *Journal of Social and Development Sciences*, *4*(1), 16–23.

Flores , W., Sommestad , T., Holm , H., & Ekstedt , M. (2011). Assessing Future Value of Investments in Security-Related IT Governance Control Objectives – Surveying IT Professionals. Electronic Journal Information Systems Evaluation , 14.

Haryoko, S. (2008). Keamanan Sistem Komunikasi Berbasis Internet. *Keamanan Sistem Komunikasi*, *3*(1), 1–6.

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

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. http://dx.doi.org/10.14569/IJACSA.2013.041217

ISACA. (2011). Chapter VI: Audit/Assurance Program BCM Policy, standard and procedures. *ISACA*, 25.

ITGI. (2007). Framework Control Objectives Management Guidelines Maturity Models.

Jeperson Hutahaean. (2014). *Konsep Sistem Informasi*. *Konsep Sistem Informasi* (Vol. 53).

Jennings, M. D. (2000). Gap analysis: Concepts, methods, and recent results. Landscape Ecology, 15(1), 5–20. https://doi.org/10.1023/A:1008184408300

Jogiyanto. (2009). Analisis dan Desain. *Yogyakarta: Andi*, *53*, 160.

Kadir, A. (2009). *Pengenalan Sistem Informasi*. *American Enterprise Institute for Public Policy Research*.

Kania, W. (2011, September). Pengukuran Tingkat Kemapanan Penerapan Teknologi Rfid Di Perpustakaan Nasional Ri Berdasarkan Framework COBIT 4.1. Pascasarjana IPB.

Kohar, Abdul & Riadi, Imam & Lutfi, Ahmad. (2015). Analysis of Smartphone Users Awareness Activities Cybercrime. International Journal of Computer Applications. 129. 1-6. 10.5120/ijca2015906449

Kristanto, A. (2007). Pengertian sistem informasi. *Pengertian Sistem Informasi*, 7.

Lapão , L. V. (2011). Organizational Challenges and Barriers to Implementing IT Governance in a Hospital . IHMT , 14, pp37-45

Lin , F., Guan , L., & Fang , W. (2010). Critical Factors Affecting the Evaluation of Information Control Systems with the COBIT Framework. A Study of CPA Firms in Taiwan, 46, pp. 42–55

Margaretha, F., & Setiyaningrum, D. (2011). Pengaruh Resiko, Kualitas Manajemen, Ukuran dan Likuiditas Bank terhadap Capital Adequacy Ratio Bank-Bank yang Terdaftar di Bursa Efek Indonesia. *Jurnal Akuntansi Dan Keuangan*, *13*, 47–56.

Marrone, M., Hoffmann , L., & Kolbe , L. (2010, August 12-15). IT Executives' Perception of CobiT: Satisfaction, Business-IT Alignment and Benefits. Proceedings of the Sixteenth Americas Conference on Information Systems

Musa, A. A. (2009). Exploring COBIT Processes for ITG in Saudi Organizations: An empirical Study. The International Journal of Digital Accounting Research , 9, pp.99-126

Niekerk, L.V and Labuschagne, L. (2006). The Peculium Model: InformationSecurity Risk Management for The South African SMME. University ofJohannesburg: South Africa University of Johannesburg, South Africa.

Pambudi, S. A. (2015). Analisis Kesiapan Pengguna Sistem Informasi Akademik. *SEMNASTEKNOMEDIA ONLINE*, *3*(1), 2-1–127.

Pederiva , A. (2003). The COBIT Maturity Model in a Vendor Evaluation Case. Information Systems Audit and Control Association , 3.

Peterson , R. (2004). Integration Strategies and Tactics for Information Technology Governance. Integration Strategies and Tactics for Information Technology Governance .

PricewaterhouseCoopers(2003). Building a Strategic Internal Audit Function, PricewaterhouseCoopers. refers to the network of member firms of PricewaterhouseCoopers International Limited

Setiawan , A. (2008, Juni 21). Evaluasi Penerapan Teknologi Informasi Di Perguruan Tinggi Swasta Yogyakarta Dengan Menggunakan Model Cobit Framework. Seminar Nasional Aplikasi Teknologi Informasi (1907-5022).

Setiawan , A. (2010, mei 22). Pengaruh Kematangan, Kinerja Dan Perkembangan Teknologi Informasi Di Perguruan Tinggi Swasta Yogyakarta Dengan Model Cobit Framework. Seminar Nasional Informatika.

Sugiyono. (2009). Metode Penelitan Pendidikan. Bandung : CV. ALFABETA

Sugiyono. (2011). Metode Penelitian Kuantitatif, kualitatif dan R & D. *Bandung: Alfabeta*, 90. https://doi.org/10.1017/CBO9781107415324.004

Syafrizal, M. (2007). ISO 17799 : Standar Sistem Manajemen Keamanan Informasi. In *Seminar Nasional Teknologi 2007 (SNT 2007)* (Vol. 2007, pp. 1–12).

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

Rosmiati, Riadi, Imam. & Prayudi, Yudi. (2016). A Maturity Level Framework for Measurement of Information Security Performance. International Journal of Computer Applications. 141. 975-8887. 10.5120/ijca2016907930

Tanuwijaya, H., & Sarno, R. (2010). Comparation of CobiT Maturity Model and Structural Equation Model for Measuring the Alignment Between University Academic Regulations and Information Technology Goals. *IJCSNS International Journal of Computer Science and Network Security*, *10*(6), 80–92

Widiyasono, Nur & Riadi, Imam & Luthfi, Ahmad. (2016). Investigation on the Services of Private Cloud Computing by Using ADAM Method.International Journal of Electrical and Computer Engineering. 6. 2387-2395. 10.11591/ijece.v6i5.11527.

LAMPIRAN A

Perhitungan Maturity Level Indexs

Clause	Descriptions	Current Maturity	Expected Maturity	Maturity Level
9	Access Control	1.44	5	1
11	Physical Security and Environment	2.47	5	3
14	Acquisition of Information Systems, Development and Maintenance	3.63	5	4
Nilai Rata-Rata Maturity Level		**2.51**	5	3

Clausa 9

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
9 Kontrol Akses	9.1 Persyaratan bisnis untuk kontrol akses	9.1.1 Kebijakan kontrol akses	1.54	1.54
	9.2 Manajemen akses user	9.2.1 Registrasi pengguna	1.10	0.92
		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 Tanggung jawab pengguna	9.3.1 Penggunaan password	0.90	1.40
		9.3.2 Peralatan pengguna yang tidak dijaga	2.10	
		9.3.3 Kebijakan clear desk dan clear screen	1.20	
	9.4 Kontrol akses jaringan	9.4.1 Kebijakan penggunaan layanan jaringan	1.40	1.06
		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	

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
	9.5 Kontrol akses sistem operasi	9.5.1 Prosedur log-on yang aman	1.67	1.96
		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	
		9.5.6 Batasan waktu koneksi	1.75	
	9.6 Kontrol akses informasi dan aplikasi	9.6.1 Pembatasan akses informasi	1.90	1.55
		9.6.2 Isolasi sistem yang sensitif	1.20	
	9.7 Komputasi bergerak dan bekerja dari lain tempat/teleworking	9.7.1 Komunikasi dan terkomputerisasi yang bergerak	2.00	2.00
Marturity level Klausul 9				**1.44**

Clausa 11

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
11 Keamanan Fisik dan Lingkungan	11.1 Wilayah aman	11.1.1 Pembatas keamanan fisik	4.14	3.01
		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	
		11.1.6 Akses publik, area pengiriman dan penurunan barang	4.50	
	11.2 Keamanan peralatan	11.2.1 Penempatan peralatan dan perlindunganya	4.30	2.64
		11.2.2 Utilitas pendukung	5.00	
		11.2.3 Keamanan pengkabelan	1.71	
		11.2.4 Pemeliharaan peralatan	2.32	

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
		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	
Marturity level Klausul 11				**2.47**

Clausa 14

Klausul	Objektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-rata Objektif Kontrol
14 Akuisisi Sistem Informasi, Pembangunan, dan Pemeliharaan	14.1 Persyaratan keamanan untuk sistem informasi	14.1.1 Analisa dan spesifikasi persyaratan keamanan	3.78	3.78
	14.2 Pemrosesan yang benar dalam aplikasi	14.2.1 Validasi data input	3.50	3.87
		14.2.2 Kontrol untuk pemrosesan internal	3.90	
		14.2.4 Validasi data output	4.20	
	14.5 Keamanan dalam pembangunan dan proses-proses pendukung	14.5.1 Prosedur tambahan kontrol	2.90	2.92
		14.5.3 Pembatasan perubahan paket software	2.87	
		14.5.4 Kelemahan informasi	3.00	
	14.6 Manajemen teknik kelemahan (Vurnerability)	14.6.1 Kontrol terhadap kelemahan secara teknis (Vurnerability	3.56	3.56
Marturity level Klausul 14				**3.63**

Pembobotan

Klausul 11 (Keamanan Fisik dan Lingkungan)																		
Klausul 11.1 Wilayah Aman (Secure Areas)																		
ISO 27002 11.1.1 pembatas keamanan fisik (*Physical security perimeter*)			1	2	3	4	5	Resp.	B*R					∑	Nilai
No	Pernyataan	Hasil Pemeriksaan													
1	Adanya perlindungan keamanan fisik (dinding, kartu akses masuk atau penjaga pintu) terhadap ruangan pemrosesan informasi	Terdapat dinding untuk perlindungan keamanan fisik ruang pemrosesan informasi, tetapi penjaga pintu hanya terdapat pada pintu masuk terdapat penjaga pintu Bukti : Foto dinding pada ruang server	0	0	2	2	3	7	0	0	6	8	15	29	4.14

LAMPIRAN B

1. Engament Letter

Engagement Letter

Analisis Keamanan Sistem Informasi Akademik
Berdasarkan ISO/IEC 27002:2013

Yang bertandatangan dibawah ini :
Nama : **Yosi Agustiawan, ST., M.MT.**
Jabatan : Direkur PUSKOM
NIY : 01011201008
Bertindak atas nama PUSKOM Unipdu, menugaskan dan memberikan wewenang kepada :

Nama : **Endang Kurniawan, S.Kom., M.M.**
NIM : 14917118
Jurusan : Magister Teknik Informatika, Universitas Islam Indonesia
Sebagai auditor untuk melakukan pemeriksaan keamanan sistem informasi akademik pada Unipdu dengan ketentuan sebagai berikut :

TUJUAN
1. Melakukan evaluasi secara independen tentang keamanaan TI pada sistem informasi akademik.
2. Memberikan rekomendasi untuk perbaikan dan peningkatan keamanaan TI pada sistem informasi akademik.

PERIODE PENILITIAN
Analisis keamanan sistem informasi akademik akan dilaksanakan kurang lebih selama 4 (empat) bulan yaitu Oktober 2016 sampai Januari 2016

TUGAS DAN TANGGUNGJAWAB AUDITOR
1. Melakukan pemeriksaan keamanan sistem informasi sesuai dengan ruang lingkup
2. Auditor memeriksa data, dan dokumen sesuai dengan standar ISO 27002:2013
3. Memberikan penilaian tentang tingkat keamanan yang ada pada sistem informasi akademik
4. Melaporkan hal-hal penting yang berkaitan dengan kerusakan dan perbaikan tingkat keamanan sistem informasi akademik
5. Auditor membuat rekomendasi perbaikan berdasarkan temuan alat bukti
6. Menyusun laporan pemeriksaan keamanan sistem informasi akademik yang telah dilaksanakan

TUGAS DAN TANGGUNGJAWAB AUDITEE
1. Memberikan data sesuai kesepakatan bersama
2. Menjawab pertanyaan auditor sesuai dengan keadaan yang sebanarnya sesuai dengan ruang lingkup yang telah ditentukan

RUANG LINGKUP

1. Standar pemeriksaan yang digunakan adalah ISO 27002
2. Klausul ISO 27002 yang digunakan dalam pemeriksaan keamanan sistem informasi ini meliputi :
   a. Klausul 9 : Kontrol Akses
   b. Klausul 11 : Keamanan Fisik dan Lingkungan
   c. Klausul 14 : Akuisisi Sistem Informasi, Pengembangan, dan Pemeliharaan
3. Detil control keamanan ISO 27002 yang digunakan :

No	Klausul	Objektif Kontrol	Kontrol Keamanan
	9 Kontrol Akses	9.1 Persyaratan bisnis untuk kontrol akses	9.1.1 Kebijakan kontrol akses
		9.2 Manajemen akses user	9.2.1 Registrasi pengguna
			9.2.2 Manajemen hak istimewa atau khusus
			9.2.3 Manajemen password user
			9.2.4 Tinjauan terhadap hak akses user
		9.3 Tanggung jawab pengguna	9.3.1 Penggunaan password
			9.3.2 Peralatan pengguna yang tidak dijaga
			9.3.3 Kebijakan clear desk dan clear screen
		9.4 Kontrol akses jaringan	9.4.1 Kebijakan penggunaan layanan jaringan
			9.4.2 Otentikasi pengguna untuk melakukan koneksi keluar
			9.4.5 Pemisahan dengan jaringan
			9.4.6 Kontrol terhadap koneksi jaringan
			9.4.7 Kontrol terhadap routing jaringan
		9.5 Kontrol akses sistem operasi	9.5.1 Prosedur log-on yang aman
			9.5.2 Identifikasi dan otentifikasi user
			9.5.3 Sistem manajemen password
			9.5.4 Penggunaan utilitas sistem
			9.5.5 Sesi time-out
			9.5.6 Batasan waktu koneksi
		9.6 Kontrol akses informasi dan	9.6.1 Pembatasan akses informasi

No	Klausul	Objektif Kontrol	Kontrol Keamanan
		aplikasi	9.6.2 Isolasi sistem yang sensitif
		9.7 Komputasi bergerak dan teleworking	9.7.1 Komunikasi dan terkomputerisasi yang bergerak
	11 Keamanan Fisik dan Lingkungan	11.1 Wilayah aman	11.1.1 Pembatas keamanan fisik
			11.1.2 Kontrol masuk fisik
			11.1.3 Keamanan kantor, ruang, dan fasilitasnya
			11.1.4 Perlindungan terhadap serangan dari luar dan ancaman lingkungan sekitar
			11.1.5 Bekerja di wilayah aman
			11.1.6 Akses publik, area pengiriman, dan pemuatan barang
		11.2 Keamanan peralatan	11.2.1 Penempatan peralatan dan perlindungannya
			11.2.2 Utilitas pendukung
			11.2.3 Keamanan pengkabelan
			11.2.4 Pemeliharaan peralatan
			11.2.5 Keamanan peralatan di luar tempat kerja yang tidak diisyaratkan
			11.2.6 Keamanan pembuangan atau pemanfaatan kembali peralatan
			11.2.7 Hak pemindahan peralatan
	14 Akuisisi Sistem Informasi, Pembangunan, dan Pemeliharaan	14.1 Persyaratan keamanan untuk sistem informasi	12.1.1 Analisa dan spesifikasi persyaratan keamanan
		14.2 Pemrosesan yang benar dalam aplikasi	12.2.1 Validasi data input
			12.2.2 Kontrol untuk pemrosesan internal
			12.2.4 Validasi data output
		14.5 Keamanan dalam pembangunan dan proses-proses pendukung	12.5.1 Prosedur tambahan kontrol
			12.5.3 Pembatasan perubahan paket software
			12.5.4 Kelemahan informasi
		14.6 Manajemen teknik kelemahan (Vurnerability)	12.6.1 Kontrol terhadap kelemahan secara teknis (Vurnerability)

METODE KERJA

Pemeriksaan keamanan sistem informasi akademik akan dilaksanakan dengan beberapa metode pelaksaan, yaitu sebagai berikut :

1. Review kebijakan standar, prosedur, sturktur organisasi, arsitektur infrastruktur sistem informasi akademik untuk memahami proses bisnis dan teknologi informasi yang digunakan.
2. Observasi dan wawancara untuk memahami pelaksanaan operasional sistem informasi akademik

INDEPENDENSI

Dalam berbagai hal yang berkaitan dengan pemeriksaan keamanan sistem informasi, auditor akan menjaga independensi, baik secara factual maupun penampilan, dari organisasi atau hal yang diperiksa.

OBYEKTIFITAS

1. Audiotr akan menjaga obyektifitas dalam merencanakan, mempersiapkan, melaksanakan, dan melaporkan pemeriksaan keamanan sistem informasi
2. Auditor dikatakan bertindak obyektif bila bersikap tidak memihak, serta menghindari kemungkinan timbulnya benturan kepentingan.
   a. Auditor harus memiliki sikap mental yang obyektif, tidak memihak dan menghindari keungkinan benturan kepentingan dalam melakukan tugas pengawasan.
   b. Auditor harus dapat mengambil keputusan profesionalnya secara bebas, hasil kerjanya handal, dan dipercaya dan bebas dari pengaruh pihak luar sehingga dapat menghasilkan laporan yang obyektif serta dapat dipakai semua pihak terkait.

INTEGRITAS

Auditor menjaga integritas melalui :

1. Auditor dilarang menerima imbalan dalam bentuk apapun dari pegawai atau klien, ataupun mitra penyedia jasa aplikasi sehingga dapat mempengaruhi pertimbangan profesionalnya
2. Auditor harus menunjukan sikap mental yang jujur dan kesungguhan dalam melaksanakan tugas dan memenuhi tanggungjawabnya
3. Auditor tidak boleh secara sadar terlibat dalam tindakan atau kegiatan yang merusak citra organisasi.

KERAHASIAAN

Data, informasi, dan dokumen yang diperoleh auditor dari PUSKOM dalam rangka pelaksanaan pemeriksaan keamanan sistem informasi ini bersifat rahasia dan hanya untuk kepentingan penugasan ini saja. Auditor berkomitmen untuk menjaga kerahasiaan data dan informasi yang telah didapatkan dan tidak akan menyebarluaskan data dan informasi tersebut kepada siapapun dengan alas an apapun.

LAMPIRAN C

1. Hasil Temuan Dan RekomendasiKlausul 9 : Akses Kontrol

Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
9 Kontrol Akses	9.1 Persyaratan bisnis untuk kontrol akses	9.1.1 Kebijakan kontrol akses	Terdapat kebijakan dan otorisasi terhadap keamanan informasi persyaratan bisnis kontrol akses, persyaratan keamanan, namun masik dilakukan secara informal dan belum terdokumentasi	- Melakukan review dan observasi dilapangan terhadap hal-hal tersebut - Mendesain kebijakan dan sangsinya - Mendokumentasikan kebijakan-kebijakan tersebut - Melakukan distribusi informasi atau pengumuman mengenai kebijakan tersebut - Memantau dan mengevaluasi pelaksanaan kebijakan yang telah dilaksanakan - Contoh kebjikana Kontrol akses : Organisasi harus melakukan pemisahaan lingkungan (environment) untuk pengembangan, uji coba, dan produksi, termasuk pembatasan akses ke masing-masing laingkungan
	9.2 Manajemen akses user	9.2.1 Registrasi pengguna	- Tidak terdapat prosedur pendaftaran formal untuk pengguna dalam mengakses sistem informasi - Belum terdapat pernyataan tertulis pada setiap pegawai, namun pengguna telah diwajibkan untuk mengamankan hak akses masing-masing	- Organisasi harus memiliki prosedur formal tertulis tentang penggunaan user yang meliputi pendaftaran, perubahan, dan penghapusan user - Membuat pernyataan tertulis masing-masing pegawai dimana masing-masing pegawai telah memahami kondisi aksesnya dan wajib mengamankannya. - Organisasi harus mewajibkan menjaga kerahasiaan dan menghindari penulisan password dikertas dan tempat lainnya unntuk pengamanan yang memadai.
		9.2.2 Manajemen hak istimewa atau khusus	- Tidak ada identifikasi kategori pegawai yang akan dialokasikan - Belum ada catatan mengenai hak akses dan pemberian hak khusus	- Membuat surat perjanjian kerja dan terdapat pasal-pasal mengenai peraturan dan mengenai pemberian hak khusus tersebut serta ditandatangani manajemen terkait dan pegawai yang diberi hak khhusus tersebut. - Organisasi harus memiliki catatan tentang pengadministrasian pengguna yang meliputi

Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
				pendaftaran, perubahan, dan penghapusan user, termasuk pemberian hak khusus.
		9.2.3 Manajemen password user	- Tidak ada pernyataan resmi yang diitandatangani untuk menjaga password - Tidak terdapat prosedur penggantian password, pengguna mengajukan ganti password secara langsung kepada bagian TI terkait - Tidak terdapat teknologi lain untuk identifikasi dan otentikasi pengguna, misalnya biometric, yaitu pengesahan sidik jari, tandatangan, dan sebagainya.	- Membuat dan menandatangani pernyataan tertulis pada masing-masing pegawai bahwa pegawai tersebut telah memahami tentang kondisi aksesnya dan wajib untuk mengamankannya. - Organisasi harus mewajibkan atau menjaga kerahasiaan password menghindari penulisan password dikertas dan tempat lain untuk pengamanan yang memadai. - Organisasi harus memiliki prosedur formal tentang pengadministrasian yang meliputi pendaftaran, perubahan, dan penghapusan pengguna. - Menambah teknologi lain untuk identifikasi dan otentikasi pengguna, misalnya biometric, yaitu pengesahaan sidik jari, tandatangan.
		9.2.4 Tinjauan terhadap hak akses user	- Belum ada pengkajian ulang hak akses - Tidak ada pengkajian ulang otorisasi hak khusus - Tidak terdapat pemeriksaan alokasi hak khusus	- Menjadwalkan pengkajian ulang - Melakukan pengkajian ulang secara berkala mendokumentasikan pengkajian tersebut - Organisasi harus melakukan pemeriksaan berkala terhadap hak user untuk memastikan bahwa hak user yang diberikan sesuai dengan wewenang yang diberikan. - Pengkajian ulang hak akses sebaiknya dilakukan secara berkala (disarankan setiap 6 bulan) dan setelah ada perubahan - Otorisasi hak khusus harus dikaji ulang dalam rentang waktu yang lebih sering (disarankan setiap 3 bulan)
	9.3 Tanggung jawab pengguna	9.3.1 Penggunaan password	- Tidak terdapat pelatihan terhadap pengguna dalam pemilihan dan penggunaan password yang baik - Pengguna diwajibkan menjaga password secara rahasia. Namun hanya berupa himbauan saja. - Tidak ditemukan catatan tertulis tentang password pengguna	- Organisasi harus menetapkan prosedur pengendalian melalui pembberian password awal (initial password) kepada pengguna dengan memperhatikan : ✓ Password awal harus diganti saat login pertama kali

Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
			- Pengguna tidak diharuskan untuk merubah password secara berkala - Dalam sistem belum dapat melihat indikasi sistem atau password disalahgunakan - Belum menerapkan pemilihan password yang baik dengan panjang minimum. - Password yang ada masih memperbolehkan password hanya dengan satu karakter saja.	✓ Password awal diberikan secara aman, misalnya melalui amplop tertutup atau kertas berlapis dua ✓ Password awal bersifat khusus (unique) untuk setiap pengguna dan tidak mudah ditebak. ✓ Setiap pemilik UserID harus menandatangani pernyataan tanggungjawab atau perjanjian penggunaan UserID dan password saat menerima UserID dan password - Kriteria password yang baik : ✓ Panjang password yang memadai sehingga tidak mudah ditebak ✓ Mudah diingat dan terdiri dari sekurang0kurangnya kombinasi 2 tipe karakter (huruf, angka, atau karakter khusus ✓ Tidak didasarkan atas data pribadi pengguna seperti nama, nomor telepon, atau tanggal lahir - Organisasi harus mewajibkan user untuk : ✓ Menjaga kerahasiaan password ✓ Menghindari penulisan password dikertas dan tempat lain tanpa pengamanan yang memadai ✓ Memilih password yang berkualitas ✓ Mengubah password secara berkala ✓ Menghindari penggunaan password yang sama secara berulang - Organisasi harus menyediakan dan melakukan kajian ulang atas jejak log baik ditingkat jaringan, sistem, maupun aplikasi serta menetapkan jenis log, informasi yang harus dimasukan kedalam log, jangka waktu penyimpanan atau kapasitas log dengan memperhatikan ketentuan yang berlaku untuk keperluan penelusuran masalah - Memonitoring implementasi pencegahan penyalahgunaan password - Mempertegas sangsi yang diberikan terhadap penyalahgunaan password

Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
				- Menerapkan pencatatan login dalam sistem, baik untuk login yang berhasil atau untuk kegagalan login serta history aktifitas dalam sistem, sehingga terdapat indikasi apabila terjadi penyalahgunaan password atau penyalahgunaan sistem. - Mempelajari bagaimana pemilihan dan penerapan password yang baik - Mulai menerapkan dan mendistribusikan penerapan password dengan panjang minimum yang ditentukan dan perubahan password secara berkala
		9.3.2 Peralatan pengguna yang tidak dijaga	Tidak jaminan peralatan yang tak dijaga mendapat perlindungan yang tepat	- Melakukan pemetaan terhadap kepentingan fungsi setiap aset komputer - Mengamankan peralatan yang tak dijaga
		9.3.3 Kebijakan clear desk dan clear screen	Informasi bisnis yang sensitif dan penting telah disimpan terkunci jika tidak dipergunakan khususnya pada saat ruangan kantor kosong	Dokumen informasi sensitive dan dokumen informasi berklasifikasi dipindahkan langsung saat selesai tercetak.
	9.4 Kontrol akses jaringan	9.4.1 Kebijakan penggunaan layanan jaringan	- Tidak ada kontrol jaringan ke pengguna dilokasi publik/eksternal - Tidak ada kontrol manajemen untuk melindungi akses jaringan - Tidak ada prosedur perlindungan akses jaringan	- Melakukan review dan observasi di lapangan terhadap hal-hal tersebut - Mendesain kebijakan dan sangsinya - Mendokumentasikan kebijakan-kebijakan tersebut - Melakukan distribusi informasi atau pengumuman mengenai kebijakan tersebut. - Memantau dan mengevaluasi pelaksanaan kebijakan yang telah dilaksanakan - Pengguna seharusnya hanya disediakan akses terhadap layanan yang telah secara spesifik diotorisasi dalam penggunaanya.
		9.4.2 Otentikasi pengguna untuk melakukan koneksi keluar	Tidak ada otentikasi pengguna untuk melakukan koneksi keluar	- Mendesain dan menerapkan metode otentikasi untuk pengguna yang melakukan koneksi keluar - Metode otentikasi yang tepat seharusnya digunakan untuk akses kontrol dengan meremote pengguna.

Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
		9.4.5 Pemisahan dengan jaringan	Tidak ada pemisahan dengan jaringan. Semua jaringan intern saling terhubung	Grup layanan informasi, pengguna, dan sistem informasi seharusnya dipisahkan dalam jaringan
		9.4.6 Kontrol terhadap koneksi jaringan	Tidak ada control terhadap koneksi jaringan	- Untuk jaringan yang di share terutama yang diperluas diseluruh batasan organisasi, kemampuan pengguna untuk terhubung daam jaringan seharusnya dibatasi dan sejalan dengan kebijakan control akses dan syarat aplikasi - Memantau dan mengontrol koneksi jaringan yang ada
		9.4.7 Kontrol terhadap routing jaringan	Tidak ada control terhadap routing jaringan	- Kontrol routing seharusnya diimplementasikan terhadap jaringan untuk memastikan bahwa koneksi komputer dan aliran informasi tidak melanggar kebijakan kontrol akses dari aplikasi bisnis.
	9.5 Kontrol akses sistem operasi	9.5.1 Prosedur log-on yang aman	- Aplikasi belum menampilkan peringatan umum bahwa computer hanya boleh diakses oleh pengguna yang diijinkan - Aplikasi elum membatasi jumlah kegagalan log-on - Tidak terdapat pencatatan pada percobaan log-on yang gagal - Belum menggunakan time delay pada percobaan log-on selanjutnya setelah terjadi kegagalan, pegawai dapat mencoba kembali setelah gagal log-on - Tidak terdapat otorisasi khusus padaa percobaan log-on selanjutnya setelah terjadi kegagalan - Tidak ada pemutusan koneksi sambungan data yang dilakukan pada saat log-on gagal - Belum ada batasan waktu pada prosedur log-on - Tidak terdapat informasi tampilan tanggal log-on berhasil terakhir - Tidak terdapat informasi tampilan tanggal log-on berhasil terakhir yang berhasil	- Menampilkan pesan pada aplikasi sebagai peringatan bahwa computer hanya boleh diakses oleh pengguna yang diijinkan. - Membatasi jumlah keggagalan percobaan log-on sebanyak 3 kali dan mencatat setiap percobaan log-on, baik yang berhasil maupun yang gagal. - Organisasi harus menonaktifkan hak akses bila User ID tidak digunakan pada waktu tertentu, menetapkan jumlah maksimal kegagalan password (failed login attempt) dan menonaktifkan password setelah mencapai jumlah maksimal kegagalan password. - Menerapkan pengotorisasian khusus untuk log-on selanjutnya bila terjadi kegagalan - Menerapkan pemutusan koneksi sambungan data yang dilakukan pada saat log-on gagal - Membuat batasan waktu untuk proses log-on, yaitu sistem akan log-off otomatis bila melebihi batasan waktu yang telah ditetapkan - Menampilkan informasi tanggal dan waktu log-on berhasil terakhir - Melakukan pencatatan oleh sistem dan

Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
				menyimpannya dalam histori. - Membuat pencatatan rincian seluruh kegagalan log-on sejak log-on terakhir yang berhasil. Pencatatan tersebut dilakukan oleh sistem dan disimpan dalam history.
		9.5.2 Identifikasi dan otentifikasi user	Belum terdapat prosedur yang telah terdokumentasi. Otentikasi ditujukan dengan IP ataupun UserID	- Organisasi harus menerapkan metode identifikasi dan otentikasi (authentication) sesuai tingkat pentingnya aplikasi misalnya penggunaan one-factor authentication untuk palikasi biasa serta penggunaan two-facttor authentication untuk palikasi yang bersifat kritikal atau sensitif.
		9.5.3 Sistem manajemen password	- Terdapat kondisi perubahan password pengguna tapi tidak ada layanan perubahan password secara berkala - Aplikasi menyimpan password dalam bentuk enkripsi menggunakan algoritma enkripsi one-way	- Sistem manajeen password dan perangkat yang dimiliki organisasi sedapat mungkin membantu pelaksanaan pengamanan password, sebagai contoh : ✓ Memaksa user untuk mengubah passwordnya setelah jangka waktu tertentu dan menolak bila user memasukan password yang sama dengan yang digunakan sebelumnya saat mengganti password ✓ Menyimpan password secara aman (ter-enkripsi) ✓ Memutuskan hubungan atau akses user jika tidak terdapat respon selama jangka waktu tertentu (session time-out) - Organisasi harus menyediakan dan menlakukann kajian ulang atas jejak log baik ditingkat jaringan, sistem, maupun aplikasi serta menetapkan jenis log (misalnya administrator log, user log, system log) informasi yang harus dimasukan kedalam log.
		9.5.4 Penggunaan utilitas sistem	- Tidak ada control pemisah system fasilitas dan prinati lunak aplikasi - Belum ada control otorisasi dan pembatasan durasi wktu penggunaan system fasilitas. - Belum ada proses pencatatan penggunaan fasilitas sistem - Tida terdapat dokumentasi penetapan tingkatan pada	- Pemisahaan harus menerapkan kontrol pemisah sistem fasilitas dan piranti lunak aplikasi - Organisasi harus menerapkan kontrol pembatasan ketersediaan sistem yaitu durasi waktu yang diijinkan - Organisasi harus menyediakan dan melakukan kaji ulang atas jejak log baik ditingkat jaringan, sistem maupun aplikasi serta menetapkan jenis log

Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
			otoritas fasilitas sistem.	(misalnya : administrator log, user log, system log), informasi yang harus dimasukan ke dalam log - Tigkatan otorisasi fasilitas sistem harus ditetapkan dan didokumentasikan. - Organisasi harus memiliki prosedur formal (tertulis dan telah disetujui oleh manajemen) tentang pengadministrasian pengguna yang meliputi pendaftaran, perubahan, dan penghapusan pengguna.
		9.5.5 Sesi time-out	- Terdapat fasilitas time-out biasanya layar akan mati jika 10 menit tidak terjadi aktifitas apapun, namun tidak semua computer didalam organisasi telah disetting seperti itu. - Time-our delay belum menggambarkan resiko keamanan wilayah, karena time-out delay telah di default semua.	- Melakukan pemetaan terhadap kepentingan fungsi setiap aset komputer - Melakukan setting time-out yang telah disesuikan dengan pemetaan fungsi setiap aset computer - Time-out delay untuk computer yang memiliki fungsi sangat penting memiliki alokasi waktu time-out yang minimum - Terminal yang tidak aktif pada lokasi yang beresiko tinggi, seperti wilayah public atau wilayah eksternal diluar manajemen keamanan organisasi, atau yang melayani system beresiko tinggi, harus dimatikan setelah periode waktu tanpa aktifitas yang ditentukan untuk mencegah akses tanpa otorisasi. - Format terbatas dari fasilitas time-out terminal dapat disediakan untuk sebagian PC yang mati layarnya dan mencegah akses pihak tanpa otorisasi tetapi tidak menutup aplikasi jaringan
		9.5.6 Batasan waktu koneksi	Belum ada system pengamanan tambahan untuk aplikasi yang beresiko tinggi berupa pelarangan terhadap waktu koneksi	- Pelarangan terhadap waktu koneksi harus menyertakan system pengamanan tambahan untuk palikasi yang beresiko tinggi - Organisasi harus menerapkan pembatasan periode selama koneksi terminal membolehkan layanan computer mengurangi terbukanya peluang akses tanpa ijin
	9.6 Kontrol akses	9.6.1 Pembatasan akses informasi	Logical access terhadap software dan informai tidak dapat diakses oleh pengguna kecuali terdapat otorisasi. Terdapat peraturannya namun secara informal	- Mendesain kebijakan mengenai kewajiban merahasiakan logical access

Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
	informasi dan aplikasi			- Membuat prosedur untuk kebijakan akses untuk penggunaan aplikasi secara tertulis yang didalamnya terdapat pengertian, kebijakan, dan tujuan - Menerapkan sangsi terhadap pelanggaran kebijakan - Mendokumentasikan kebijakan mengenai logical access dengan persetujuan manajemen - Melakukan distribusi informasi atau pengumuman mengenai kebijakan itu - Mengadakan pelatihan mengenai logical access - Melakukan pemantauan dan evaluasi
		9.6.2 Isolasi sistem yang sensitif	Sensifitas system aplikasi telah didindentifikasi, namun belum terdokumentasi	- Isolasi system sensitive dimana sensivitas system aplikasi harus diindentifikasi secara eskplisit dan didokumentasian oleh pemilik aplikasi - Aplikasi sensitive dijalankan pada lingkungan bersama, system aplikasi yang akan dibagi resourcesnya harus diidentifikasi dan disetujui oleh pemilik aplikasi sensitive.
	9.7 Komputasi bergerak dan bekerja dari lain tempat/tele working	9.7.1 Komunikasi dan terkomputerisasi yang bergerak	Belum ada prosedur penggunaan software berbahaya, namun pastinya pegawai telah dihimbau untuk yang tidak berkepentingan dengan proses bisnis yang ada menggunakan software berbahaya pada terminal perusahaan	- Mendesain kebijakan mengenai komputasi bergerak dan software lain. - Menetapkan sangsi terhadap pelanggaran kebijakan - Mendokumentasikan kebijakan mengenai komputasi bergerak dan software berbahaya atas persetujuan manajemen - Melakukan distribusi informasi atau pengumuman kebijakan tersebut - Pengawasan terhadap peralatan komputasi bergerak (notebook, laptop, dan telepon genggam) harus dikunci secara fisik atau penggunaan kunci khusus untuk mengamankan peralatan.

2. Hasil Temuan Dan Rekomendasi Klausul 11 : Keamanan Fisik dan Lingkungan

Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
11 Keamanan Fisik dan Lingkungan	11.1 Wilayah aman	11.1.1 Pembatas keamanan fisik	- Belum ada pintu dan tangga darurat - Belum terpasang tanda bahaya	- Menyediakan adanya pintu darurat - Memasang alat pengamanan didalam ruangan (misalnya:alarm, pengukur suhu, dan kelembaban udara, dan CCTV)
		11.1.2 Kontrol masuk fisik	- Belum ada control keamanan berupa log dating dan perginya pengunjung - Tidak terdapat dokumen tertulis mengenai prosedur darurat - Belum ada intruder detection system - Personil diwajibkan untuk memakai tanda pengenal yang jelas. Namun, pada pelaksanaanya masih ditemukan beberapa personil tidak menggunakan tanda pengenal. - Belumada sangsi tegas yang tetapkan jika personil tidak memamkai tanda pengenal, selain itu aturan tentang kewajiban untuk emmakai tanda pengenal belum didokumentasikan. - Belum dilakukan pengkajian ulang dan pembaharuan hak akses secara berkala - Pembaharuan secara berkala untuk hak akses tidak diwajibkan	- Melakukan pencatatan terhadap seluruh kedatangan dan kepergian pengunjung dengan menambhakan buku tamu - Menambah pengendali akses masuk (misalnya : penggunaan access control card, PIN, biometric, dan alaram) - Melakukan observasi atau pemetaan terhadap proses kerja yang sudah berjalan atau akan berjalan - Melakukan benchmarking bile diperlukan dengan organisasi sejenis - Mendesain prosedur sesuai dengan hasil observasi dan hasil referensi untuk menambah ketajaman desain prosedur - Melakukan review prosedur agar prosedur yang sudah dibuat bisa berjalan tanpa hambatan - Mempertegas kebijakan mengenai kewajiban pemakaian tanda pengenal baik untuk tamu dan karyawan - Menetapkan sangsi atas pelanggaran kebijakan tersebut, emndokumentasikan kebijakan mengenai pemakaian tanda pengenal sesuai dengan persetujuan manajemen, dan mengumumkannya. - Organisasi harus memiliki prosedur formal (tertulis dan telah disetujui oleh manajemen) tentang pengadministrasian user yang meliputi pendaftaran, perubahan, dan penghapusan user - Organisasi harus melakukan pemeriksaan berkala terhadap hak akses user untuk memastikan bahwa hak akses yang diberikan sesuai dengan wewenang yang diberikan

Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
		11.1.3 Keamanan kantor, ruang dan fasilitasnya	- Tidak ada standard peraturan tertentu untuk pemilihan dan desain wilayah - Tidak menggunakan standard kesehatan dan keselamatan tertentu untuk pemilihan dan desain wilayah	- Mempelajari beberapa standard tentang pemilihan dan desain wilayah, termasuk standard kesehatan dan keseluruhan - Ruang fasilitas pemrosesan informasi tidak boleh berada dibawah kamar mandi atau tempat penyimpanan air. - Ruang server harus tertutup dan dinding ruangan harus terbuat dari material yang tidak bias dilihat dari luar - Menerapkan standard tersebut sebagai acuan pemilihan dan desain wilayah untuk perbaikan dan peningkatan.
		11.1.4 Perlindungan terhadap serangan dari luar dan ancaman lingkungan sekitar	- Untuk makan dan minum selain dirungan server belum ada larangan - Belum menggunakan metode perlindungan khusus, seperti membrane keyboard	- Menerapkan pemeliharaan kebersihan ruangan dan peralatan 9misalnya dari debu rokok, makanan atau minuman, barang mudah terbakar) - Memeprtimbangkan penggunaan metode perlindungan khusus - Mengkaji ulang manfaat penggunaan membrane keyboard - Menganggarkan pembelian membrane keyboard - Menambah pengendali akses masuk (misalnya penggunaan access control card, PIN, biometrics) - Menambah kelengkapan alat pengamanan didalam ruangan (misalnya alarm, pendeteksi dan pemadam api, pengukur suhu dan kelembaban udara, CCTV) - Alarm kebakaran harus dipastikan kapasitas dan ketersediannya dalam mendukung operasionak fasilitas pemrosesan informasi.
		11.1.5 Bekerja di wilayah aman	Belum ada panduan tambahan untuk meningkatkan keamanaan pada wilayah aman Belaum ada larangan untuk penggunaan peralatan fotografi, video, audio, dan peralatan perekam lainnya.	- Mencari informasi panduan tambahan yang dapat meningkatkan keamanan pada wilayah aman. - Mempertimbangkan panduan tersebut - Menerapkan pada wilayah aman organisasi dan mendokumentasikannya - Mempertimbangkan resiko yang mungkin muncul akibat penyalahgunaan peralatan tersebut, misalnya data organisasi yang terancam tersebar diluar tanpa

Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
				diketahui pelakunya - Menambahkan peraturan untuk larangan penggunaan peralatan tersebut diwilayah organisasi, kecuali jika ada ijin khusus. - Mensosialisasikan peraturan baru tersebut kepada seluruh pegawai - Mengntrol apakah kebijakan baru telah terlaksana dengan baik
		11.1.6 Akses publik, area pengiriman dan penurunan barang	Lokasi tempat menaikan dan menurunkan barang diletakan jauh dari area pemrosesan informasi dan telah dilakukan pengontrolan	Lokasi pemrosesan informasi harus berada dilinngkungan yang aksesnya terbatas untuk publik (restriced area) mudah diawasi, dan lokasinya tidak boleh dicantumkan dipapan petunjuk.
	11.2 Keamanan peralatan	11.2.1 Penempatan peralatan dan perlindunganya	Peralatan sistem informasi telah ditempatkan dan dilindungi dengan baik	- Mencari tambahan info bagaimana penempatan dan perlindungan yang baik untuk peralatan pemrosesan informasi - Menerapkan dan mendokumentasikan penempatan tersebut sebagai suatu standard yang baik dan mensosialisasikan pada seluruh pegawai
		11.2.2 Utilitas pendukung	- Terdapat UPS dan Genset. Namun, belum dilakukan pemeriksaan UPS dan Genset secara berkala - Tidak terdapat tombol listrik darurat didekat pintu darurat - Tidak ada penangkal petir pada gedung - Tidak ada filter penangkal petir yang dipasang disemua saluran komunikasi	- Melakukan penjadwalan pemeriksaan UPS dan genset. UPS kapasitas 15 menit kepada semua perangkat computer. Kapasitas Genset harus cukup untuk seluruh perangkat computer dan fasilitas pendukungnya. - Melakukan pencatatan berkala terhadap pemeriksaan yang telah dilakukan - Menganggarkan untuk memiliki penangkal petir sendiri pada gedung termasuk filter penangkal petir yang dipasang disemua saluran komunikasi demi keamanan dan kenyamanan bersama
		11.2.3 Keamanan pengkabelan	- Kabel jaringan, kabel listrik, dan kabbel komunikasi masih tampak berada diluar dan belum mendapat perlindungan yang memadai - Belum menggunakan pipa pengaman untuk pengabelan	- Saluran listrik dan saluran komunikasi kefasilitas pemrosesan informasi harus dipasang dibawah tanah atau perlindungan alternative yang memadai - Menerapkan perlindungan pengkabelan jaringan terhadap penyadapan dengan menggunakan pipa

Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
			jaringan - Kabel listrik belum dipisahkan dari kabel komunikasi	pengaman - Kabel lsitrik harus dipisahkan dari kabel komunikasi untuk mencegah gangguan (interferensi)
		11.2.4 Pemeliharaan peralatan	- Jadwal service belum dilakukan secara ruitn dan belum terdokumentasi - Belum melakukan pencatatan dari semua dugaan atau kerusakan aktual yang terjadi - Belum dilakukan pencatatan dari semua tindakan pemeliharaan - Terdapat asuransi yang telah diimplementasikan namun belum keseluruhan, misalnya saja peralatan pemrosesan sistem informasi belum diasuransikan	- Menjadwalkan secara rutin jjadwal service untuk pemeliharaan yang intensif dan mendokumentasikan - Melakukan pencatatan terhadap semua dugaan atau kerusakan actual yang terjadi serta tindakan pemeliharaan yang dilakukan - Menkaji ulang catatan kerusakan actual dan catatan pemeliharaan - Mengumpulkan data dan fakta terhadap dugaan atau kerusakan actual yang terjadi - Mengkalsifikasikan data - Melakukan evaluasi dan pengolahan data - Mendokumentasikan dengan persetujuan pempinan terkait - Melaksanakan servis sesuai jadwal servis yang ditetapkan - Penggunaan TI dapat menimbulkan terjadinya resiko operasional yang disebabkan oleh antara lain ketidak cukupan atau ketidaksesuaian peeliharaan sistem atau komputer dan perlengkapannya - Mengkaji ulang manfaat asuransi bagi keamanan aset informasi - Mendata aset informasi yang penting dan sensitive - Membuat rencana anggaran untuk mengasuransikan aset informasi yang bersifat sensitif dan penting - Penggunaan fasilitas ruangan atau gedung mengandung resiko terjadi kebakaran. Resiko ini ditangani dengan memindahkan resiko ke perusahaan asuransi yaitu dengan mengasuransikan fasilitas ruangan atau gedung
		11.2.5 Keamanan peralatan di luar	Terdapat perlindungan organisasi untuk emlindungi peralatan yang ditempatkan diluar tempat yang diisyaratkan	- Tidak ada

Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
		tempat kerja yang tidak diisyaratkan		
		11.2.6 Keamanan pembuangan atau pemanfaatan kembali peralatan	- Belum ada dokumentasi prosedur pembungan media simpan - Belum ada kajian resiko terhadap media penyimpanan	- Mendesain prosedur sesuai dengan hasil observasi dan hasil referensi termasuk prosedur pencatatan untuk menambah ketajaman dari desain prosedur - Melakukan review prosedur yang sudah dibuat bias berjalan tanpa hambatan - Mendokumentasikan prosedur pembuangan media dan melakukan pencatatan setiap pembuangan media yang dilakukan termasuk personil yang bertugas dalam pembuangan media tersebut. - Melakukan identifikasi dan analisis resiko terhadap media simpan rusak - Mengkomunikasikan resiko terhadap media simpan rusak - Mendokumentasikan kajian resiko yang telah dilakukan
		11.2.7 Hak pemindahan peralatan	- Belum dilakukan pencatatan terhadap peminjaman yang dilakukan oleh bagian lain - Belum dilakukan pemeriksaan berkala penndeteksi pemindahaan tanpa ijin ataupun kebijakan pemeriksaan mendadak - Tidak ada kebijakan pemeriksaan mendadak	- Mendesai perosedur sesuai dengan hasil observasi dan hasil referensi termasuk prosedur pencatatan untuk menambah ketajaman dari desain prosedur - Melakukan review prosedur agar prosedur yang sudah dibuat bias berjalan tanpa hambatan - Melakukan peminjaman ulang terhadap peminjaman dan kepmilikan aset - Melakukan penjadwalan terhadap pemeriksaan pemindahaan aset - Sesekali dilakukan pemerisakaan mendadak untuk emnghindari rekayasa atau manipulasi data - Memberi pemeritahuan terhadap pegawai tentang berlakunya kebijakan pemeriksaan mendadak - Mendokumentasikan hasil pemeriksaan

3. Hasil Temuan Dan RekomendasiKlausul 14 : Akuisisi Sistem Informasi, Pembangunan, dan Pemeliharaan

Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
14 Akuisisi Sistem Informasi, Pembangunan, dan Pemeliharaan	14.1 Persyaratan keamanan untuk sistem informasi	14.1.1 Analisa dan spesifikasi persyaratan keamanan	Untuk mengatasi penyusupan terhadap jaringan belum ada pemberitahuan yang signifikan kepada penanggungjawab sistem	✓ Membuat aplikasi pemberitahuan jika terjadi penyusupan ✓ Periksa aplikasi sistem informasi akademik secara berkala untuk mendeteksi celah keamanan yang terjadi
	14.2 Pemrosesan yang benar dalam aplikasi	14.2.1 Validasi data input	- Metode penginputan UserID masih menggunakan single character - Tidak ada proses log dari pengguna - Belum dibedakan antara numeric, dan integer, serta spesial karakter dalam proses input	Pada bagian input data gunakan pemberitahuan atau komentar untuk masing-masing kolom dan bedakan masing-masing karakter untuk menghindari kesalahan input.
		14.2.2 Kontrol untuk pemrosesan internal	- Penerapan kebijaksanaan-kebijaksanaan, metode-metode dan prosedur-prosedur didalam sistem belum terdokumentasi. - Sesuatu yang dirancang untuk menemukan kesalahan atau penyimpangan	- Menyusun sistem pengendalian intern dimaksudkan untuk mencegah hal-hal yang tidak baik yang mengganggu masukan, proses dan hasil dari sistem supaya sistem dapat beroperasi seperti yang diharapkan - Periksa aplikasi untuk mencegah salah dalam pemasukan data
		14.2.4 Validasi data output	Jenis keluaran yang dihasilkan dari proses transaksi, antara lain: laporan nilai, transaksi keuangan, laporan operasional, dokumen pengiriman, dan neraca saldo belum terdokumentasi	- Menyusun dokumentasi dan pelatihan dalam proses transaksi - Menyusun laporan perkembangan penggunaan aplikasi
	14.5 Keamanan dalam pembangunan dan proses-proses pendukung	14.5.1 Prosedur tambahan kontrol	Tidak ada kontrol tambahan	- Melakukan review dan observasi dilapangan terhadap hal-hal tersebut - Mendokumentasikan kebijakan-kebijakan tersebut - Melakukan distribusi informasi atau kebijakan tersebut - Membuat kontrol tambahan dalam jaringan untuk mengetahui penggunaan aplikasi
		14.5.3 Pembatasan perubahan paket software	- Telah digunakan authentication system terhadap modul-modul yang tersedia - Mendokumentasikan perubahan modul-modul yang digunakan	- Dokumentasikan secara tertulis yang diketahui oleh pimpinan organisasi - Batasi perubahan dari penyedia jasa aplikasi - Lakukan sosialisasi jika terjadi perubahan

Klausul	Objektif Kontrol	Kontrol Keamanan	Temuan	Rekomendasi
		14.5.4 Kelemahan informasi	- Untuk akses masuk ke halaman sistem, tidak menggunakan koneksi yang aman - Banyak celah keamanan informasi pada aplikasi - Mudah dirubah oleh pegawai tanpa ada informasi penggunaan yang sesuai dengan prosedur	- Gunakan virtual private network untuk masuk halaman sistem - Batasi penggunaan jaringan di area umum untuk mengakses sistem - Gunakan log file sebagai monitoring sistem yang berjalan
	14.6 Manajemen teknik kelemahan (Vurnerability)	14.6.1 Kontrol terhadap kelemahan secara teknis (Vurnerability	- Perubahan data transaksi yang dilakukan oleh pegawai yang tidak berkepentingan - Sistem terinfeksi virus - Patch sudah kadaluarsa	- Membuat halaman yang aman dengan menggunakan protokol https - Update patch pada aplikasi yang terbuka - Tutup port yang berpotensi disusupi - Dokumentasikan setiap perubahaan pada file transaksi dan lakukan pembersihan secara berkala

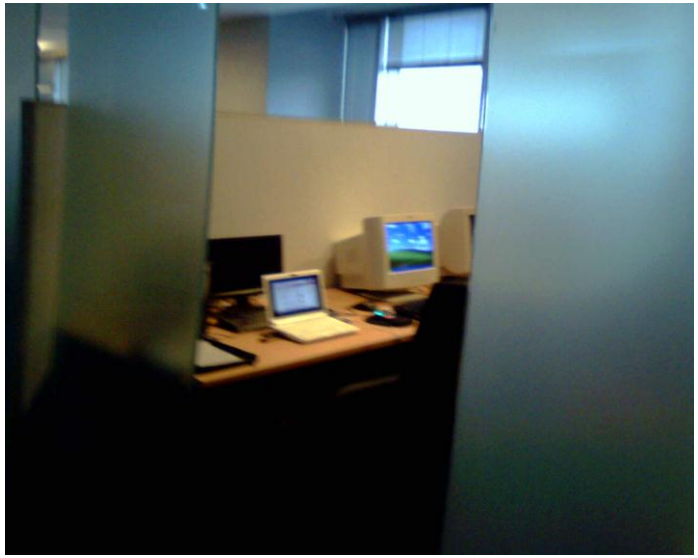
LAMPIRAN D

1. Ruang control dan pemasangan akses keamanan



2. Ruang Staff PUSKOM


3. Ruang Server Sistem Akademik



LAMPIRAN E

Sertifikat Publikasi International IJCSIS

International Journal of Computer Science and Information Security

ISSN 1947 5500

IJCSIS January 2018 Volume 16 No. 1

This Research Publication Certificate

is presented to distinguished authors

Endang Kurniawan & Imam Riadi

for peer-reviewed published paper entitled

" Security Level Analysis of Academic Information Systems Based on Standard ISO 27002: 2013 using SSE-CMM "

Professor Ying Yang

Professor Yong Li

Dr. Jorge A. Ruiz-Vanoye

IJCSIS Editorial Board
International Journal of Computer Science and Information Security,
IJCSIS ISSN 1947-5500, Pittsburgh, PA, USA
Email: ijcsiseditor@gmail.com
http://sites.google.com/site/ijcsis/
https://google.academia.edu/JournalofComputerScience

29 January 2018