AUDIT KEAMANAN SISTEM INFORMASI AKADEMIK DENGAN KERANGKA KERJA ISO 27001 DI PROGRAM STUDI SISTEM INFORMASI UNIKOM

MARLIANA BUDHININGTIAS WINANTI, ISMAIL DZULHAN
Program Studi Sistem Informasi, Fakultas Teknik dan Ilmu Komputer
Universitas Komputer Indonesia

Academic Information Systems Prodi UNIKOM Information System is the primary system used in the Information Systems Prodi process data and information about lectures and students. But in this system still found a lack of control of physical and logical security.
To find out how your system security in organizations, information systems need security audit to determine whether security information is in accordance with the security procedures of management. Standardization used here is ISO 27001, this standards have been an international standards organization that is structured on the management of information security systems. Implementation of academic information system security audit is done by using the Audit Checklist ISO 27001: 2005.
Audit results found security controls are still less well as the roles and responsibilities of employee safety, physical protection from disasters and power failures, data validation, and data backup are less regular. So the academic information system security controls is still need to be repairs in accordance with the recommendation.

Keywords : Academic Information System, Information System Security Audit, ISO 27001

PENDAHULUAN

1. Latar Belakang Penelitian

Program studi Sistem Informasi UNIKOM didalam melakukan aktifitasnya sudah menggunakan Sistem Informasi Akademik, yaitu Sistem Informasi Akademik prodi SI (SIAKAD SI). Keamanan data atau kemanan informasi elektronik merupakan suatu hal penting bagi sebuah perusahaan yang menggunakan fasilitas Teknologi Informasi dan menempatkannya sebagai infrastruktur yang sangat penting. Sebab salah satu aset yang penting sebuah perusahaan adalah data atau informasi.

Keamanan pada sistem informasi akademik di prodi Sistem Informasi masih terbilang kurang terlindungi. Karena ditemukan pada area dan fisik yang masih kurang kontrol keamananya. Dan dari aplikasinya pun masih kurang aman, karena pernah dapat diakses oleh orang yang tidak bertanggung jawab. Karena masih kurang akan kontrol keamanan dari SIAKAD ini, penulis akan mengaudit keamanan sistem ini dari keamanan secara fisik juga keamanan logik.

Kelangsungan proses bisnis di sebuah perusahaan dapat dipertahankan dengan adanya keamanan data ataupun keamanan informasi baik secara langsung maupun secara tidak langsung. Dapat juga mengurangi resiko pada perusahaan, dan bahkan memberikan peluang bisnis semakin besar. Adanya ancaman juga resiko yang muncul akibat adanya kegiatan dalam pengelolaan dan pemeliharaan suatu data juga informasi yang menjadi alasan disusunnya standar sistem manajemen keamanan informasi yang salah satunya adalah ISO 27001.

Karena metode stadarisasi dari ISO 27001 merupakan standar organsisasi internasional yang terstruktur mengenai sistem manajemen keamanan informasi, maka dari itu penulis melakukan penelitian mengenai keamanan sistem informasi akademik pada Program Studi Sistem Informasi UNIKOM dengan menggunakan standar ISO 27001.

2. Identifikasi Masalah

a. Sistem informasi akademik membutuhkan pengembangan dari segi keamanan sistem, keamanan fisik dan keamanan area pengolahan informasi.
b. Pernah terjadi manipulasi data nilai pada Sistem Informasi Akademik Prodi Sistem Informasi UNIKOM.

3. Rumusan Masalah

a. Bagaimana sistem yang berjalan pada Sistem Informasi Akademik Prodi Sistem Informasi.
b. Bagaimana mengetahui kontrol sistem manajemen keamanan informasi pada SIAKAD Prodi Sistem Informasi.
c. Bagaimana rekomendasi agar SIAKAD ini memiliki kontrol keamanan yang baik dan benar.

TINJAUAN PUSTAKA

1. Sistem Informasi

"Sistem Informasi adalah suatu kombinasi teratur dari people (orang), hardware (perangkat keras), software (perangkat lunak), computer network and data communications (jaringan komunikasi), dan database (basis data) yang mengumpulkan, mengubah, dan menyebarkan informasi di dalam suatu bentuk organisasi." (O'Brien, 2005)

"Sistem Informasi adalah suatu sistem di dalam suatu organisasi yang mempertemukan kebutuhan pengolahan transaksi harian, mendukung operasional, bersifat manajerial dan kegiatan strategi dari suatu organisasi dan menyediakan pihak luar tertentu dengan laporan-laporan yang diperlukan." (Jogiyanto, 2010)

Kelompok kegiatan operasi yang tetap yang pada dasarnya terbentuk dari suatu sistem informasi, yaitu:

a. Data dikumpukan
b. Data dikelompokkan
c. Data dilakukan penghitungan
d. Menganalisa
e. Laporan disajikan

2. Audit Sistem Informasi

"Audit sistem informasi adalah proses pengumpulan dan penilaian bukti-bukti untuk menentukan apakah sistem komputer dapat mengamankan aset, memelihara integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumberdaya secara efisien." (Weber, 20017)

Tujuan dari Audit Sistem Informasi ini di kelompokkan ke dalam dua aspek utama yaitu *Conformance* (kesesuaian) dan *Performance* (kinerja).

3. Keamanan Sistem Informasi

Sebuah informasi dinilai sangat penting sehingga dalam beberapa hal sebuah informasi hanya diinginkan dapat diakses oleh orang-orang tertentu saja. Karena jika informasi berada pada orang yang tidak tepat akan dapat menimbulkan adanya kerugian yang sangat besar bagi para pemilik informasi. Sehingga sebuah sistem informasi yang digunakan haruslah memiliki kemanan agar dapat terjamin.

"Menurut G. J. Simons, keamanan informasi adalah bagaimana kita dapat mencegah penipuan (*cheating*) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik." (Chazar, 2015)

Tiga tujuan akan tercapai dari adanya keamanan sistem yaitu kerahasiaan, ketersediaan dan integritas.

Dua area besar yang masuk dalam cakupan kemanan informasi yaitu adanya keamanan informasi secara fisik dan adanya keamanan informasi secara logika.

4. ISO 27001

"ISO 27001 adalah suatu standar sistem manajemen keamanan informasi (*ISMS, Information Security Management System*) yang diterbitkan oleh ISO dan IEC pada Oktober 2005. Standar yang berasal dari BS 7799-2 ini ditujukan untuk digunakan bersama dengan ISO/IEC 27002, yang memberikan daftar tujuan pengendalian keamanan spesifik."

"Tujuan utama dari ISO/IEC 27001:2005 adalah untuk membantu membangun, mengembangkan, mempertahankan dan terus meningkatkan sistem informasi manajemen yang efektif. Ini mempekerjakan prinsip dan kontrol untuk mengatur keamanan sistem informasi dan jaringan." (Chazar, 2015)

METODOLOGI PENELITIAN

Pada penelitian ini dilakukan beberapa tahapan, yaitu :

a. Studi Kepustakaan dan Penentuan Ruang Lingkup

Mencari data dan mengumpulkan data, sumber informasi dari buku, literature dan artikel yang terkait dengan objek penelitian.

b. Pengumpulan Data

Pengumpulan data didapat dari observasi langsung dan wawancara kepada pihak yang kompeten terhadap objek penelitian.

c. Pelaksanaan Audit

Pelaksanaan audit yaitu melakukan *audit check list* terhadap sistem yang sedang berjalan berdasarkan klausul *Audit Check List* ISO 27001:2005

d. Penentuan Hasil Audit

Menentukan hasil dari *Audit Check List* dan juga hasil observasi yang telah dilakukan sehingga akan terlihat temuan-temuan yang harus diperthaankan dan yang harus diperbaiki

e. Penyusunan rekomendasi (Ermana dkk, 2012)

Berdasarkan hasil analisis data dan penjelasan kondisi sistem informasi yang sedang berjalan ini makan disusun rekomendasi untuk keamanan sistem informasi yang menjadi objek penelitian.

1. Metode standarisasi ISO 27001

"ISO 27001 merupakan stadarisasi internasional mengenai sistem manajemen kemanan informasi. Standar ISO 27001 berisi persyaratan yang harus dipenuhi oleh suatu organisasi dalam mengembangkan keamanan informasi. Standar ini merupakan standar manajemen berbasis risiko dan dirancang untuk menjamin agar kontrol keamanan mampu melindungi asset informasi dari berbagai risiko." (Chazar, 2015)

Berdasarkan ISO/IEC 27001:2005, pelaksanaan audit keamanan sistem ini dengan menggunakan Audit Check List ISO/IEC 27001 mengenai kontrol keamanan dari segi keamanan dari SDM, keamanan fisik serta kemanan dari segi lingkungan, manajemen komunikasi dan operasional, kontrol terhadap akses, pengembangan dan pemeliharaan sebuah sistem, manajemen terhadap insiden dalam sebuah sistem informasi.

2. Ruang lingkup audit

Ruang lingkup audit ini adalah menganalisis keamanan sistem dari beberapa aspek dan jenis.

a. Fisik dan Logik

Dari aspek keamanan fisikal yang diaudit dalam penelitian ini meliputi:

- Keamanan peralatan (komputer) *user*
- Keamanan peralatan (komputer) *server*
- Keamanan dari gangguan listrik
- Keamanan instalasi kabel

Sedangkan dari aspek keamanan logik yang diaudit dalam penelitian ini meliputi:

- Keamanan jaringan komputer user dan *server*
- Keamanan *source code* aplikasi
- Kontrol terhadap data yang di proses

b. Sumber Daya Manusia

Kontrol keamanan yang diaudit dari sumber daya manusia meliputi;

- Identifikasi *user*
- Hak akses
- Peran dan tanggung jawab *user*
- Keamanan aset perusahaan
- Keamanan terhadap pihak ketiga seperti teknisi dari luar organisasi

c. Lingkungan

Kontrol keamanan yang diaudit dari lingkungan pengolahan informasi meliputi:

- keamanan area dari ancaman bencana
- keamanan ruang *server*
- keamanan ruang pengolahan informasi (*user room*)
- keamanan dari ancaman orang yang tidak berwenang
- keamanan dari ancaman binatang atau tumbuhan yang membahayakan

HASIL PENELITIAN DAN PEMBAHASAN

1. Menentukan Ruang Lingkup

Program Studi Sistem Informasi UNIKOM tentu memahami pentingnya keamanan sistem informasi bagi kesuksesan organisasi ini. Dengan keamanan sistem informasi yang baik tentunya akan menjaga keaslian dan kerahasian data dan informasi yang diproses dalam sistem informasi akademik di Program Studi Sistem Informasi UNIKOM ini.

Untuk mengetahui apakah keamanan sistem informasi akademik di Program Studi Sistem Informasi UNIKOM ini, maka bagi SI dilakukan audit keamanan untuk mengukur tingkat keamanan dari SI akademik Prodi Sistem Informasi. Dengan begitu organisasi dapat meningkatkan kinerja dan keamanan dari sistem informasi akademik ini dengan optimal.

Standar yang digunakan sebagai pandunan dalam audit ini ada dengan menggunakan *framework* ISO 27001:2005.

2. Penyusunan Audit

Berdasarkan *framework* ISO 27001:2005 pertanyaan diambil dari klausul *Audit Check List* ISO 27001:2005 yang terlihat pada tabel 1.

Tabel 1. Klausul *Audit Check List ISO 27001:2005*

No.	*Check List*
1	*Asset Management*
2	*Human Resource Security*
3	*Physical and Environmental security*
4	*Operations Management*
5	*Access Control*
6	*Information systems acquisition, development and maintenance*
7	*Information Security Incident Management*

[Sumber: *Audit Check List ISO 27001:2005*]

3. Pelaksanaan Audit

Pelaksanaan audit yang dilakukan dengan mengadakan wawancara kepada pegawai sekretariat program studi menghasilkan beberapa dokumen wawancara, dilengkapi dengan bukti-bukti audit, dan beberapa temuan audit juga nilai tingkat kematangan pada setiap kontrol keamanan yang ada.

Hasil dari wawancara audit sistem informasi, maka didapat pertanyaan-pertanyaan dalam bentuk *Audit CheckList* yang berdasarkan klausul *Audit Check List ISO 27001:2005.*

Berikut adalah contoh kerangka kerja dari Audit Check List ISO 27001:2005 pada audit keamanan sistem informasi akademik Program Studi Sistem Informasi UNIKOM yang terlihat pada Tabel 2.

Tabel 2. Kerangka Kerja Perhitungan *Audit Check List*

Audit area, objective and question		Results
Section	*Audit Question*	Findings
1 *Asset Management*		
1.1 *Responsibility for assets*		
1.1.1 *Inventory of Assets*	Apakah semua aset diidentifikasi dan diinventarisasi atau dipertahankan dengan semua aset penting.	ADA
1.1.2 *Ownership of Assets*	Apakah setiap aset diidentifikasi memiliki pemilik, didefinisikan dan disepakati klasifikasi keamanan, dan akses pembatasan yang berkala.	ADA
1.2 Information Classification		
1.2.1 *Classification guidelines*	Apakah informasi yang diklasifikasikan dalam hal nilai, persyaratan hukum, kepekaan dan kekritisan terhadap organisasi.	ADA

2. Human resources security		
2.1 *Prior to employment*		
2.1.1 *Roles and responsibilities*	Apakah peran dan tanggung jawab keamanan karyawan dan pengguna pihak ketiga didefinisikan sesuai dengan kebijakan keamanan informasi organisasi.	ADA
	Apakah peran dan tanggung jawab yang didefinisikan dan dikomunikasikan dengan jelas kepada calon karyawan sebelum proses kerja	TIDAK
2.1.2 *Screening*	Apakah pemeriksaan verifikasi latar belakang untuk semua calon tenaga kerja dan pengguna sudah dilakukan sesuai peraturan yang relevan.	ADA
2.2 *During Employment*		
2.2.1 *Management Responsibilities*	Apakah manajemen membutuhkan karyawan dan pengguna untuk menerapkan keamanan agar dapat sesuai dengan kebijakan organisasi serta prosedur yang ada di organisasi.	YA
2.2.2 *Infromation security awareness, education and training*	Apakah semua karyawan dalam organisasi dan pengguna pihak ketiga, menerima pelatihan kesadaran keamanan yang sesuai dengan fungsi pekerjaan mereka.	TIDAK
2.2.3 *Disciplinary process*	Apakah ada proses disipliner formal untuk karyawan yang telah melakukan pelanggaran keamanan.	ADA
2.3 *Termination or change of employment*		
2.3.1 *Termination responsibilities*	Apakah tanggung jawab untuk melakukan pemutusan hubungan kerja, atau perubahan pekerjaan, didefinisikan secara jelas dan ditetapkan.	YA
2.3.2 *Return of assets*	Apakah ada proses di tempat yang menjamin para karyawan dan pengguna menyerahkan semua aset organisasi yang mereka miliki pada saat pemutusan hubungan kerja terjadi/dalam sebuah perjanjian.	YA
2.3.3 *Removal of access rights*	Apakah hak akses dari semua karyawan dan pengguna, untuk informasi fasilitas pengolahan, akan dilakukan penghapusan saat pemutusan hubungan kerja terjadi	YA
3. Physical and Enviornmental security		
3.1 *Secure Areas*		
3.1.1 *Physical security perimeter*	Apakah fasilitas keamanan fisik telah dilaksanakan untuk melindungi layanan pemrosesan informasi.	TIDAK
3.1.2 *Physical entry controls*	Apakah kontrol masuk berada di tempat untuk memungkinkan personil hanya berwenang dalam berbagai bidang dalam organisasi.	YA
3.1.3 *Securing offices, rooms and facilities*	Apakah kamar, yang memiliki layanan pemrosesan informasi, terkunci atau memiliki lemari dikunci atau brankas.	YA

3.1.4 *Protecting against external and enviornmental threats*	Apakah perlindungan fisik terhadap kerusakan akibat kebakaran, banjir, gempa bumi, ledakan, kerusuhan sipil dan bentuk-bentuk bencana alam atau buatan manusia harus dirancang dan diterapkan.	TIDAK
	Apakah ada potensi ancaman dari area lingkungan terdekat.	ADA
3.1.5 *Public access delivery and loading areas*	Apakah orang yang tidak berwenang dapat memasuki tempat pengolahan informasi yang terisolasi, untuk menghindari akses yang tidak sah.	YA
3.2 *Equipment Security*		
3.2.1 *Equipment siting and protection*	Apakah peralatan dilindungi untuk mengurangi risiko dari ancaman lingkungan dan bahaya, serta kesempatan untuk pengaksesan yang tidak sah.	TIDAK
3.2.2 *Supporting utilities*	Apakah peralatan yang ada dilindungi dari gangguan listrik dan gangguan lain yang disebabkan oleh kegagalan dalam mendukung penggunaan	TIDAK
	Apakah menggunakan pasokan listrik, seperti pakan ganda, Uninterruptible Power Supply (ups), generator cadangan, dll	TIDAK
3.2.3*Equipment Maintenance*	Apakah peralatan dipelihara dengan benar untuk memastikan ketersediaan dan integritas yang terus menerus.	TIDAK
	Apakah pemeliharaan dilakukan hanya oleh pihak yang berwenang.	YA
	Apakah peralatan diasuransikan dan memenuhi persyaratan asuransi	TIDAK
3.2.4 *Removal of property*	Apakah peralatan, informasi dan perangkat lunak tidak diambil tanpa izin sebelumnya.	YA
4. Communication and Operations Management		
4.1 *Operational procedures and responsibilities*		
4.1.1 *Change Management*	Apakah semua perubahan pada fasilitas pengolahan informasi dan sistem dikendalikan.	YA
4.1.2 *Segregation of duties*	Apakah tugas dan bidang tanggung jawab dibedakan, untuk mengurangi peluang adanya modifikasi yang tidak sah atau penyalahgunaan informasi juga jasa.	YA
4.2. *System planning and acceptance*		
4.2.1 *Capacity Management*	Apakah ada pemantauan ruang hard disk, RAM dan CPU pada server kritis.	ADA
4.3. *Backup*		
4.3.1 *Information backup*	Apakah back-up informasi dan perangkat lunak diambil dan diuji secara teratur.	TIDAK

4.4. *Network Security Management*		
4.4.1 *Network Controls*	Apakah jaringan tersebut cukup dikelola dan dikendalikan, untuk melindungi dari ancaman, dan untuk menjaga keamanan untuk sistem dan aplikasi yang menggunakan jaringan, termasuk informasi dalam perjalanan.	YA
	Apakah kontrol dilaksanakan untuk menjamin keamanan informasi dalam jaringan, dan perlindungan layanan terhubung dari ancaman, seperti akses yang tidak sah.	YA
4.4.2 *Security of network services*	Apakah operator jaringan mengelola layanan jaringan dengan aman dan diawasi	YA
4.5. *Monitoring*		
4.5.1 *Monitoring system use*	apakah prosedur yang dikembangkan menggunakan monitoring system untuk memfasilitasi pengolahan informasi.	YA
	apakah hasil dari monitoring ditnjua secara rutin	YA
	apakah diperlukan pengawasan untuk pengolahan informasi individu	YA
4.5.2 *Protection of log information*	apakah fasilitas dan informasi logging dilindungi terhadap gangguan dan akses yang tidak sah	YA
4.5.3 *Administrator and operator log*	apakah aktivitas loggin ditinjau atau diulas secara rutin	TIDAK
4.5.4 *Fault logging*	apakah kesalahan dalam loggin akan dianalisa dan di tindak secara tepat	YA
4.5.5 *Clock Synchronisation*	apakah jam pada sistem komputer sinkron dengan jam dari sumber waktu yang akurat (greenwich)	YA
5. *Access Control*		
5.1. *User Access Management*		
5.1.1 *User Registration*	apakah ada prosedur pedaftaran dan penghapusan user untuk memberikan akses ke semua sistem informasi dan pelayanan	YA
5.1.2 *Privilege Management*	Apakah alokasi dan penggunaan hak istimewa dalam lingkungan sistem informasi dibatasi dan dikendalikan	YA
5.1.3 *User Password Management*	penglokasian password harus dikontrol melalui proses manajemen	YA
5.1.4 *Review of user access rights*	apakah ada prsoses untuk meninjau hak akses user secara berkala.	YA

5.2. *User Responsibilities*		
5.2.1 *Password use*	apakah ada latihan keamanan khusus untuk pengguna dalam memilih dan mengamankan password	YA
5.2.2 *Unattended user equipment*	apakah user disadarkan akan persyaratan dan prosedur keamanan informasi.	YA
5.3. *Network Access Control*		
5.3.1 *User authentication for external connections*	apakah mekanisme authentication yang tepat digunakan untuk mengontrol pengguna jarak jauh (diluar area LAN)	YA
5.4. *Operating system access control*		
5.4.1 *User Identification and authentication*	apakah ID pengguna tersedia untuk semua user seperti operator, administrator, dan semua staff sampai teknisi	YA
5.4.2 *Password Management system*	apakah ada sistem untuk mengatur password user seperti akuntabilitas password, perubahan password dll.	YA
6. *Information systems acquisition, development and maintenance*		
6.1. *Correct processing in applications*		
6.1.1 *Input data validation*	apakah ada validasi dari setiap data yang diinput kedalam sistem	YA
6.1.2 *Control of internal processing*	apakah ada pemeriksaan validasi dari data yang diunput ke dalam sistem untuk mendeteksi informasi *corrupt* baik dari kesalahan proses atau kesengajaan.	TIDAK
6.1.3 *Output data validation*	apakah output data dari sistem divalidasi dan terjamin bahwa informasi yang disimpan dan dikeluarkan benar dan sesuai.	YA
6.2. *Security of system files*		
6.2.1 *Control of operational software*	apakah ada prosedur dalam mengendalikan instalasi software dalam sistem operasi.	YA
6.2.2 *Access control to program source code*	apakah ada kontrol keamanan untuk membatasi akses ke sumber program (*source code*)	YA
7. *Information Security Incident Management*		
7.1. *Reporting information security events and weaknesses*		
7.1.1 *Reporting information security events*	apakah kejadian keamanan informasi dilaporkan ke manajemen dengan tepat dan cepat	TIDAK
	apakah prosedur pelaporan insiden keamanan informasi dikembangkan dan diimplementasikan	YA

7.2. *Management of information security incidents and improvements*		
7.2.1 *Responsibilities and procedures*	apakah monitoring sistem digunakan untuk mendeteksi insiden keamanan informasi	YA
	Apakah tujuan dari pengelolaan insiden keamanan informasi disepakati dengan manajemen.	YA
7.2.2 *Collection of evidence*	apakah tindak lanjut terhadap orang atau organisasi yang terlibat dalam insiden keamanan sistem melibatkan tindakan hukum (baik perdata atau pidana)	YA
	apakah bukti yang berkaitan dengan insiden itu dikumpulkan , disimpan, dan disajikan agar sesuai dengan aturan bukti yang ditetapkan dalam hukum yang terkait	YA

[Sumber: Hasil Penelitian 2014]

4. Penentuan dan Penyusunan Hasil Audit Sistem Informasi

Setelah seluruh perhitungan selesai maka didapat hasil dari klausul *Audit Check List* yang dapat dilihat pada tabel dibawah ini.

Berdasarkan hasil *Audit Check List* dan wawancara didapatkan temuan-temuan mengenai keamanan informasi pada SIAKAD Prodi Sistem Informasi UNIKOM. Dari hasil temuan tersebut direkomendasikan sebagai evaluasi terhadap keamanan informasi pada SIAKAD Prodi Sistem Informasi UNIKOM.

Berikut adalah hasil evaluasi dan temuan yang masih perlu perbaikan sistem beserta rekomendasi yang diusulkan yang terlihat pada Tabel 3.

Tabel 3. Temuan yang perlu perbaikan beserta Rekomendasi

klausul	Temuan	Rekomendasi
Human Resource Security	Peran dan tanggung jawab tidak didefinisikan dan dikomunikasikan dengan jelas kepada calon karyawan sebelum proses kerja	Menjelaskan kepada calon karyawan mengenai tanggung jawab atas keamanan informasi di organisasi
Human Resource Security	Semua karyawan dan pihak ketiga belum mendapatkan pelatihan mengenai kesadaran keamanan informasi yang sesuai dengan *jobdesk* mereka	Memberikan pelatihan kepasa seluruh karyawan dan pihak ketiga kesadaran keamanan informasi yang sesuai dengan *jobdesk* mereka
Physical and Enviornmental security	fasilitas keamanan fisik tidak dilaksanakan dalam melindungi layanan pemrosesan informasi.	Mengevaluasi fasilitas keamanan fisik dalam melindungi layanan pemrosesan informasi.
Physical and Enviornmental security	Perlindungan fisik terhadap kerusakan akibat kebakaran, banjir, gempa bumi, ledakan, kerusuhan sipil dan bentuk-bentuk bencana alam atau buatan manusia tidak diterapkan	Menerepkan fasilitas perlindungan fisik terhadap kerusakan akibat kebakaran, banjir, gempa bumi, ledakan, kerusuhan sipil dan bentuk-bentuk bencana alam atau buatan manusia
Physical and Enviornmental security	Peralatan tidak dilindungi dari ancaman pada lingkungan dan dari bahaya, serta adanya kesempatan untuk akses yang tidak sah.	Melindungi peralatan dari akses yang tidak sah

klausul	Temuan	Rekomendasi
Physical and Enviornmental security	Peralatan minim perlindungan dari gangguan listrik	Merancang intalasi listrik yang baik di dalam area pengolahan informasi SIAKAD Prodi SI
Physical and Enviornmental security	Tidak adanya asuransi terhadap peralatan	Membeli peralatan yang memiliki asuransi pemakaian
Communication and Operations Management	Backup informasi dan *software* tidak diuji secara teratur	Melakukan backup secara teratur dan terawasi
Information systems acquisition, development and maintenance	Tidak ada validasi data yang diinput keadalam sistem	Harus disisipkan validasi terhadap data yang diinput dalam aplikasi
Information Security Incident Management	Insiden keamanan informasi tidak dilaporakan dengan cepat dan tepat kepada manajemen	Memberi ketegasan kepada semua pihak yang mengetahui insiden keamanan informasi untuk melaporkan secara tanggap ke manajemen
Temuan dalam Observasi	*User* dapat *login tanpa* perlu menggunakan user yang disediakan *database* tapi dapat diakses menggunakan *basic* dari *SQL Injection* dalam arti lain siapapun dapat masuk kedalam aplikasi tanpa perlu *login.*	Menginstal aplikasi SQL Injection Patch untuk menutup lubang keamanan dalam aplikasi
Temuan dalam Observasi	Terdapatnya virus pada server	Perbaikan *Firewall* pada server agar tidak mudah dimasuki aplikasi yang tidak dikenal (seperti virus)
Temuan dalam Observasi	Server menggunakan aplikasi SQL Server 2005 yang rentan diakses oleh Hacker karena SQL Server menggunakan versi lama.	Menginstal *SQL Server* 2005 *Patch* dan *Windows Server* 2002 *Patch* untuk menutup lubang keamanan pada server SIAKAD Program Studi Sistem Informasi UNIKOM.

[Sumber: Hasil Penelitian 2014]

KESIMPULAN DAN SARAN

Kesimpulan dan saran yang dapat diambil dari hasil penelitian yang dilakukan adalah :

1. Kesimpulan

Berdasarkan hasil audit keamanan sistem informasi akademik program studi Sitem Informasi UNIKOM, penulis mendapat kesimpulan yaitu:

a. Pelaksanaan Audit keamanan sistem informasi akademik program studi Sistem Informasi UNIKOM dilakukan pembuatan pertanyaan berdasarkan *Audit CheckList ISO 27001:2005* terhadap keamanan sistem informasi yang terkait dalam organisasi.
b. Hasil temuan yang didapat masih ada beberapa kekurangan dalam kontrol keamanan seperti peran dan tanggung jawab keamanan, perlindungan fisik dari bencana dan gangguan listrik, kurangnya validasi data, dan *backup* data yang kurang teratur.

2. Saran

Adapun saran yang diberikan demi peningkatan keamanan sistem informasi lebih lanjut:

a. Kontrol keamanan sistem informasi masih perlu dimanajemen kembali agar semua aktifitas pengolahan informasi dapat berjalan dengan lancar tanpa ada gangguan dari orang atau organisasi yang tidak berwenang.
b. Mengimplementasikan rekomendasi-rekomendasi terkait berdasarkan hasil temuan dari *Audit Check List* maupun hasil Audit observasi langsung.
c. Dikarenakan ISO belum memiliki metode penilaian khusus maka untuk itu dalam pengembangan penelitian berikutnya dapat menggunakan metode audit lain untuk perbandingan.

DAFTAR PUSTAKA

O'Brien, James A. 2005. *Introduction to Information System. (12th Edition)*. McGraw-Hill. New York.

Jogiyanto, 2010. Analisis dan Desain Sistem Informasi, Edisi IV, Andi Offset,

Yogyakarta.

Ron Weber. 2007. *Information System Control and Audit*. The University of Queensland, Prentice Hall Inc.

Chalifa Chazar. 2015. Standar Manajemen Keamanan Sistem Informasi Berbasis ISO/ IEC 27001:2005. Jurnal Informasi Volume VII No.2/November/2015.

Fine Ermana, Haryanto Tanuwijaya, Ignatius Adrian Mastan. 2012. Audit Keamanan Sistem Informasi Berdasarkan Standar Iso 27001 Pada PT. BPR JATIM. Jurnal JSIKA Vol.1 No.1 2012.