Jurnal Computech & Bisnis, Vol. 14, No. 1, Juni 2020, 40-46
ISSN (print): 1978-9629, ISSN (online): 2442-4943

AUDIT KEAMANAN SISTEM INFORMASI MANAJEMEN AKADEMIK DAN KEMAHASISWAAN MENGGUNAKAN SNI ISO/IEC 27001:2013 (Studi Kasus STMIK Mardira Indonesia)

Heri Wahyudi[1], Arief Zulianto[2], Asep Maulana[3]
STMIK Mardira Indonesia[1], Universitas Langlangbuana[123]
herypoenya22@gmail.com[1], madzul@gmail.com[2], siapok@yahoo.com[3]

Abstract

Observation of SIMAK that in the process of operating the system is still experiencing obstacles such as data leakage which results in impaired agency performance, insufficient security and control to anticipate forms of fraud and illegal actions that result in large losses for information owners and uncontrolled access rights, so that a system the information used must have a guaranteed level of information security, including database security, hardware, software and human resources.

Based on observations in SIMAK, the authors conclude to audit SIMAK so that they are documented and obtain audit evidence and evaluate it objectively. From the results of comparisons with other methods, the authors chose the ISO 27001: 2013 SNI standard as a standard for auditing the security of an information system and used as a reference to produce documents (findings and recommendations) which are the results of the SIMAK information system security audit at STMIK Mardira Indonesia.

From the results of the study it was identified that the clause used was, Clause 5: Security Policy, the current SIMAK security policy is still not appropriate, Clause 7: Asset Management is still not appropriate to achieve and maintain appropriate protection of organizational assets due to the absence of a policy letter regarding asset management, Clause 9: Access Control so that there is no misuse of access rights and there are procedures for controlling access rights, Clause 15: Compliance has not been adjusted to the applicable academic regulations, and the time has been scheduled on the educational calendar is also the legal aspect of the software used.

Keyword ***:*** *IT services, SNI ISO/IEC 27001: 2013, SIMAK, Audit, Information security*

Abstrak

Pengamatan terhadap SIMAK bahwa dalam proses pengoperasian sistem masih mengalami hambatan seperti adanya kebocoran data yang mengakibatkan kinerja lembaga terganggu, belum cukup pengamanan dan pengendalian untuk mengantisipasi bentuk kecurangan dan tindakan ilegal yang mengakibatkan kerugian besar bagi para pemilik informasi serta hak akses tidak terkontrol, sehingga sebuah sistem informasi yang digunakan haruslah memiliki tingkat keamanan informasi yang terjamin, meliputi keamanan database, *hardware*, *software* dan sumber daya manusia.

Berdasarkan hasil pengamatan yang ada di SIMAK maka penulis menyimpulkan untuk mengaudit SIMAK supaya terdokumentasi dan memperoleh bukti audit serta mengevaluasinya secara objektif. Dari hasil perbandingan dengan metode lain maka penulis memilih standar SNI ISO/IEC 27001:2013 sebagai standar untuk mengaudit keamanan sebuah sistem informasi dan digunakan sebagai acuan untuk menghasilkan dokumen (temuan dan rekomendasi) yang merupakan hasil audit keamanan sistem informasi SIMAK di STMIK Mardira Indonesia. Dari hasil penelitian teridentifikasi bahwa klausul yang digunakan adalah, Klausul 5 : Kebijakan Keamanan (*Security Policy*) saat ini kebijakan keamanan SIMAK masih belum sesuai, Klausul 7 : Manajemen Aset (*Asset Management*) masih belum sesuai untuk mencapai dan memelihara perlindungan yang sesuai terhadap aset organisasi dikarenakan belum adanya surat kebijakan tentang pengelolaan aset, Klausul 9 : Kontrol Akses (*Access Control*) agar tidak terjadi penyalahgunaan hak akses serta adanya prosedur pengendalian hak akses, Klausul 15 : Kepatuhan (*Compliance*) belum disesuaikan dengan peraturan akademik yang berlaku, serta waktu yang telah dijadwalkan pada kalender pendidikan juga aspek legal *software* yang digunakan.

Kata Kunci **:** Layanan TI, SNI ISO/IEC 27001:2013, SIMAK, Audit, Keamanan informasi

PENDAHULUAN

Perguruan Tinggi mempunyai peranan yang sangat besar dalam pengembangan ilmu pengetahuan dan teknologi di masyarakat sehingga membutuhkan sumber informasi yang mutakhir dan terkini. Fungsi utama dari Perguruan Tinggi adalah sebagai penyelenggara pendidikan dan pelayanan akademik, maka seharusnya implementasi teknologi informasi perlu dikembangkan sehingga sasaran dari pelayanan akademik bisa tercapai dengan baik. Hal ini pun berlaku di STMIK Mardira Indonesia atau disingkat STMIK-MI pada pelayanan akademiknya.

Teknologi informasi di STMIK Mardira Indonesia salahsatunya adalah Sistem Informasi Manajemen Akademik dan Kemahasiswaan (SIMAK) yang sudah berjalan dari tahun 2002 dan terus menerus mengalami perkembangan seiring dengan bertambahnya data yang di kelola dan fungsinya.

Sejak awal Sistem Informasi Manajemen Akademik dan Kemahasiswaan (SIMAK) di STMIK Mardira Indonesia sampai saat ini secara umum berjalan dengan baik, namun setelah penulis melakukan prapenelitian pada STMIK Mardira Indonesia, khususnya pengamatan terhadap SIMAK bahwa dalam proses pengoperasian sistem masih mengalami hambatan seperti SIMAK belum bisa di akses dari luar oleh Karyawan, Dosen, Mahasiswa, nilai mahasiswa sering berubah, belum terkoneksi dengan pddikti.ristekdikti.go.id, tidak adanya batasan waktu untuk pengisian nilai oleh dosen, tidak adanya ketentuan input nilai oleh dosen pengampu matakuliah, adanya kebocoran data yang mengakibatkan kinerja lembaga terganggu, belum cukup pengamanan dan pengendalian untuk mengantisipasi bentuk kecurangan dan tindakan ilegal yang mengakibatkan kerugian besar bagi para pemilik informasi. Sehingga sebuah sistem informasi yang digunakan haruslah memiliki keamanan agar dapat terjamin. Ketika membahas mengenai keamanan maka tidak akan pernah lepas dari yang namanya aspek keamanan. Menurut HARR dalam Simanungkalit keamanan informasi meliputi perlindungan terhadap tiga aspek, yaitu Kerahasiaan (*Confidentiality*), Integritas (*Integrity*) dan Ketersediaan (*Availability*). Salah satu contoh seperti Hak akses tidak terkontrol, nilai mahasiswa sering berubah.

Berdasarkan hasil pengamatan yang ada di SIMAK maka proses pengukuran kinerja yang ditempuh yaitu melalui audit. Agar audit keamanan sistem informasi dapat berjalan dengan baik diperlukan suatu standar untuk melakukannya. Secara formal tidak ada acuan baku mengenai standar apa yang akan digunakan atau dipilih oleh Perguruan Tinggi untuk melaksanakan audit keamanan sistem informasi sehingga dapat menggunakan standar sesuai dengan kebutuhan. Sehingga penulis menyimpulkan untuk mengaudit SIMAK Audit merupakan proses yang sistematis, mandiri, dan terdokumentasi untuk memperoleh bukti audit dan mengevaluasinya secara objektif sejauh mana kriteria audit terpenuhi.

Masalah yang terdapat pada lembaga pendidikan STMIK-MI adalah

1. Hak Akses tidak terkontrol
2. Belum bisa di akses dari luar kampus
3. Adanya kebocoran data
4. Belum terkoneksi dengan pddikti.ristekdikti.go.id

Metode yang digunakan yaitu metode kualitatif dengan pendekatan studi kasus. Berdasarkan Yin (1994), pendekatan studi kasus berguna ketika penelitian bertujuan untuk wawasan teoritis dan empiris yang diteliti. SIMAK dipilih sebagai kasus yang diteliti karena berdasarkan aktivitas utama STMIK Mardira Indonesia dan merupakan aset informasi yang dimiliki oleh lembaga yang menghadapi ancaman keamanan informasi atas kerahasiaan, integritas, dan ketersediaan.

Data Primer diperoleh melalui hasil wawancara dan tatap muka serta observasi langsung dengan responden. Wawancara dilakukan untuk menggali informasi mengenai aktifitas utama dalam kegiatan akademik di STMIK Mardira Indonesia.

KAJIAN PUSTAKA

Audit Sistem Informasi

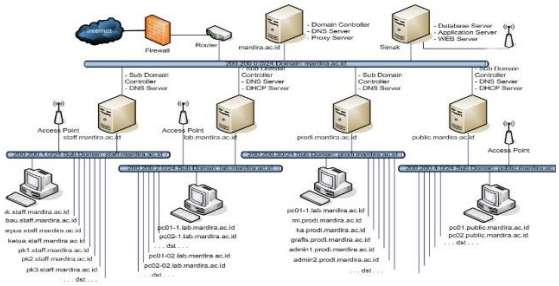
"Audit sistem informasi adalah proses pengumpulan dan penilaian bukti-bukti untuk menentukan apakah sistem komputer dapat mengamankan aset, memelihara integritas data, dapat mendorong pencapaian tujuan organisasi secara efektif dan menggunakan sumberdaya secara efisien." (*Weber*, 2017).

Keamanan Sistem Informasi

"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).

Sistem Informasi Akademik

Sistem informasi akademik adalah sistem yang dirancang untuk melakukan pengolahan data akademik baik melalui software ataupun hardware sehingga proses kegiatan akademik dapat dikelola dengan baik sehingga menjadi informasi yang bermanfaat untuk manajemen perguruan tinggi dan pengambilan keputusan oleh eksekutif. Sistem ini bertujuan untuk dapat membantu pelaksanaan pendidikan, sehingga perguruan tinggi dapat memberikan layanan informasi yang baik dan efektif, melalui jaringan internet



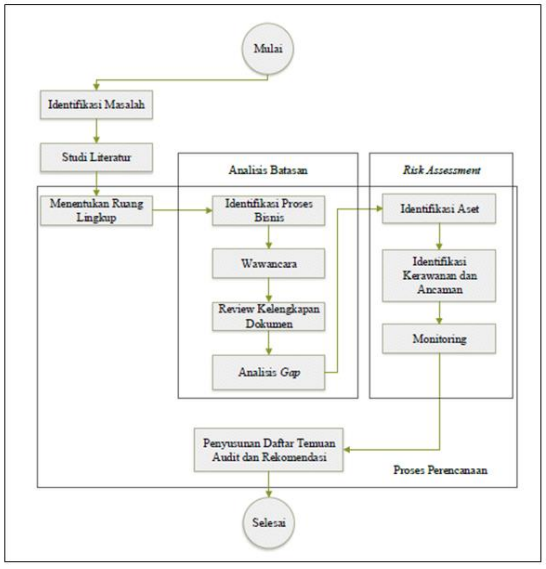
Gambar I.1 Arsitektur SIMAK

SNI ISO/IEC 27001:2013

Standar Nasional Indonesiaa (SNI) ISO/IEC 27001:2013 / *Information Security Management System Requirements* merupakan revisi dari standar sebelumnya yaitu ISO/IEC 27001:2005. ISO/IEC 27001:2013 tetap dapat diadopsi oleh semua organisasi, apapun jenis maupun ukurannya sebagaimana versi terdahulu. Berbeda dengan versi 2005 yang mengadopsi model PDCA (*Plan-Do-Check-Act*), versi 2013 tidak secara spesifik menyatakan penggunaan model manajemen tertentu. Namun demikian model PDCA tetap terlihat pada keseluruhan proses yang ada dalam SMKI yang diarahkan dalam ISO/IEC 27001:2013. SMKI SNI ISO/IEC 27001:2013 telah ditetapkan oleh Badan Standarisasi Nasional Nomor 61/KEP/BSN/4/2016 dan Peraturan Menteri KominfoNomor 4 tahun 2016 Pasal 7.

METODOLOGI PENELITIAN

Dalam melakukan Audit Keamanan Sistem Informasi Akademik STMIK Mardira Indonesia menggunakan Standar SNI ISO/IEC 27001, berikut ini adalah gambar alur metodologi penelitian dalam penyusunan audit:



Gambar I.2 Metodologi Penelitian

Analisis *gap* dilakukan berdasarkan *checklist* hasil wawancara, observasi dan pengumpulan dokumen organisasi baik itu kebijakan, prosedur, kontrol, dan dokumen-dokumen terkait keamanan informasi lainnya. Dokumen kemudian diteliti berdasarkan domain dan control objektif yang berasal dari *Assessment Checklist*. Tujuan dari penilaian *gap* adalah memeriksa sudah sejauh apa kontrol-kontrol SNI ISO/IEC 27001 diterapkan dan diimplementasikan dengan baik terhadap pihak terkait. Berikut ini adalah penilaian *gap* pada Annex SNI ISO/IEC 27001:

Tabel 1 Penilaian *Gap* SNI ISO/IEC 27001

Nilai	Keterangan
1	Kontrol persyaratan tidak diimplementasikan atau direncanakan (Pasif).
2	Kontrol direncanakan namun tidak dilaksanakan (Reaktif).
3	Kontrol diimplementasikan sebagian, sehingga efek secara penuh tidak ditimbulkan (Penerapan kerangka kerja dasar).
4	Kontrol persyaratan diimplementasikan, namun pengukuran, review, dan perbaikan tidak dilakukan (Terdefinisi dan konsisten).
5	Kontrol diimplementasikan dan pengukuran, review dan perbaikan, dilakukan secara berkala (Terkelola dan terstruktur).

Kontrol ini didapatkan berdasarkan hasil identifikasi kerawanan dan ancaman sehingga didapatkan rekomendasi yang akan menutupi celah-celah keamanan informasi yang ada.

Tabel 2 Domain dan Kontrol Objektif SNI ISO/IEC 27001

No.	Domain ISO 27001	KontrolObjektif ISO 27001
A.5	*Information Security Policies*	A.5.1 *Information Security Policy Document* A.5.2 *Review of Information Security policy*
A.8	*Asset management*	A.8.1 *Responsibility for assets* A.8.2 *Information Classification* A.8.3 *Media handling*
A.9	*Acces Control*	A.9.1 *Business requirements of access control* A.9.2 *User access management* A.9.3 *User responsibilities* A.9.4 *System and application access control*
A.15	*Compliance*	*15.1: Compliance with Legal Requirements*
		15.2: compliance with security policies, standards and technical compliance

Dalam melakukan audit, *audit working plan* sangat dibutuhkan dalam melakukan *Monitoring* terhadap proses audit, mulai dari proses awal hingga proses pelaporan audit. Berikut ini adalah perencanaan Audit Keamanan Sistem Informasi Akademik STMIK Mardira Indonesia:

Tabel 3 *Audit Working Plan*

No	Kegiatan	Bulan															
		Oktober				November				Desember				Januari			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Studi Literatur																
2	Menentukan Ruang Lingkup																
3	Identifikasi Proses Bisnis TI																
4	Observasi dan Wawancara																
5	Pengecekan kelengkapan dokumen																
6	Analisis GAP																
7	Risk Asessment																
8	Identifikasi Asset																
9	Identifikasi Kerawanan																
10	Menetapkan Kontrol																
11	Menyusun hasil temuan																
12	Analisis dan rekomendasi																
13	Penyusunan Laporan																

HASIL DAN PEMBAHASAN

Berdasarkan kesadaran akan pentingnya ketersampaian informasi kepada semua civitas akademika, maka setiap informasi yang berkaitan dengan proses pendidikan disediakan secara internal. Ketua STMIK Mardira Indonesia

menugaskan kepada bagian PUSKOMTEK untuk mengelola sejumlah halaman web yang digunakan untuk berbagai data pendidikan dan penyebaran informasi pendidikan. Halaman web yang dikelola, yaitu situs yang digunakan untuk pengadministrasian proses pendidikan dan penampilan informasi yang sifatnya terbatas, sehingga hanya dapat diakses oleh pengguna yang terotorisasi. Berdasarkan *scope* akses dari pengguna, maka tingkat akses yang didefinisikan untuk situs ini adalah: STMIK MARDIRA INDONESIA, program studi, dan individu. Yang termasuk ke dalam kelompok situs ini secara garis besar adalah:

a. Situs administrasi proses pendidikan yang digunakan untuk pengadministrasian proses pendidikan yang dilakukan oleh program studi, termasuk tempat untuk melihat paket kerja yang sedang berjalan. Untuk transaksi data pendidikan yang mengandung aspek legal, seperti transaksi nilai, harus selalu mendapat persetujuan dari Ketua Program Studi masing-masing.
b. Sistem perwalian yang digunakan untuk membantu pengadministrasian proses perwalian dan pengisian rencana studi di awal semester.
c. Situs portofolio, yang digunakan untuk pengadministrasian portofolio kegiatan belajar mengajar setiap semester oleh masing-masing staf pengajar.
d. Situs pendaftaran mahasiswa baru, yang digunakan oleh calon mahasiswa baru untuk mengisikan datanya, dan juga digunakan oleh staff program studi untuk mempersiapkan berbagai data yang diperlukan serta memantau proses yang dilakukan oleh calon mahasiswa baru.

Berikut daftar situs administrasi pendidikan seperti terlihat pada tabel 4.1. Daftar Situs Sistem Informasi Akademik dan Kemahasiswaan (SIMAK):

Tabel 4 Daftar situs SIMAK

NO	Nama Situs	Layanan	Pengguna Layanan	Kontrol Keamanan
1	Penerimaan mahasiswa Baru (PMB)	Pendaftaran Mahasiswa Baru Yang diakses dengan jaringan internal	Calon mahasiswa	Login calon mahasiswa yang sudah teregistrasi
2	Kelas	Pembukaan kelas mata kuliah dan pengisian dosen pengajar secara jaringan internal	Staff Prodi	Login Staff Prodi yang sudah terdaftar
3	Daftar Wali	Pengisian dosen wali mahasiswa secara jaringan internal	Staff Prodi	Login Staff Prodi yang sudah terdaftar
4	Rencana Studi dan Perwalian	Daftar ulang mahasiswa lama, pengambilan matakuliah dan perwalian secara jaringan lan	Mahasiswa, KA Prodi, Wakil Ketua I Bidang Akademik	Login masing-masing mahasiswa persetujuan KA Prodi atau Wakil Ketua I
5	Kehadiran Mahasiswa	Pengisian kehadiran mahasiswa dan topic perkuliahan secara jaringan LAN	Dosen	Login masing-masing dosen
6	Portofolio Dosen	Pengisian Portofolio masing-masing Dosen	Dosen dan ketua kelompok keahlian	Login dosen verifikasi ketua kelompok keahlian masing-masing
7	Evaluasi Perkuliahan	Pengisian kuesioner evaluasi perkuliah oleh mahasiswa	Mahasiswa	Login mahasiswa
8	Nilai	Pengisian daftar nilai akhir	Dosen	Login dosen persetujuan KA Prodi
9	Status Mahasiswa	Penayangan status akademik mahasiswa	Mahasiswa. Dosem. Staff prodi	Display data
10	Penjurusan	Pilih program studi dan penjurusan	Mahasiswa, Staff Prodi	Login mahasiswa display pemilihan
11	*Early Warning*	Penayangan mahasiswa yang memiliki kasus akademik	Staff Prodi	Display data
12	Wisuda	Proses pendaftaran wisuda secara jaringan Lan	Staff Prodi dan mahasiswa	Login staff tata usaha dan staff prodi

13	Drop Out/Pengunduran Diri	Proses dropout atau pengunduran diri	Ketua STMIK Mardira Indonesia	Login Admin
14	Mahasiswa Non reguler	Pendaftaran dan administrasi akademik mahasiswa non reguler	BAAK, Mahasiswa non reguler	Login staff Tatausaha, puslia dan BAAK

Dari identifikasi keamanan informasi klausul yang digunakan untuk audit keamanan informasi ini adalah:

1. *Annex* 5 : Kebijakan Keamanan (*Security Policy*)

Tabel 5 Kebijakan Keamanan

***Annex* : 5 Kebijakan Keamanan**		
Kategori Keamanan Utama : 5.1 Kebijakan Keamanan Informasi		
Kontrol Objektif : memberikan arahan kepada manajemen organisasi dan dukungan untuk keamanan Informasi dalam hubungannya dengan persyaratan bisnis organisasi, hukum dan aturan yang sedang berlaku		
5.1.1	Dokumen Kebijakan Keamanan Informasi	**Kontrol:** Dokumen Kebijakan Keamanan Informasi harus disetujui oleh pihak manajemen, dipublikasikan dan dikomunikasikan kepada seluruh pegawai dan pihak-pihak lain yang relevan
5.1.2	Tinjauan Ulang kebijakan Keamanan Informasi	**Kontrol:** Kebijakan Keamanan Informasi harus ditinjau ulang secara berkala, jika terjadi perubahan harus dipastikan hal tersebut merupakan pengembangan dari kebijakan sebelumnya sehingga menjadi lebih sesuai, menccukupi kebutuhan organisasi dan lebih efektif dalam pelaksanaannya

2. *Annex* 7 : Manajemen Aset (*Asset Management*) Tabel

Tabel 6 Manajemen Aset

Annex : 7 Manajemen Aset		
Kategori Keamanan Utama : 7.1 Tanggung Jawab Terhadap Aset **Objektif kontrol :** untuk memenuhi perlindungan dan pemeliharaan terhadap aset organisasi		
7.1.1	Inventarisasi terhadap aset	**Kontrol :** Seluruh aset organisasi harus diinventarisasi dan dipelihara
7.1.2	Kepemilikan aset	**Kontrol :** Seluruh informasi dan aset yang berhubungan dengan fasilitas pemrosesan Informasi harus ditentukan kepemilikannya sesuai ketentuan organisasi
7.1.3	Aturan penggunaan aset	**Kontrol :** Aturan-aturan penggunaan aset yang berhubungan dengan fasilitas pemrosesan informasi harus diidentifikasi dan diimlementasikan
Kategori Keamanan Utama : 7.2 klasifikasi Informasi **Objektif kontrol :** untuk memastikan bahwa aset dalam organisasi mendapatkan keamanan yang memadai		
7.2.1	Aturan Klasifikasi	**Kontrol :** Aset harus diklasifikasikan menurut nilai, kepentingan dan tingkat kritikalnya terhadap organisasi
7.2.2	Penanganan dan pelabelan aset	**Kontrol :** Suatu prosedur yang cukup memadai harus dibuat untuk pelabelan dan penanganan aset sesuai dengan klasifikasi yang telah ditentukan oleh organisasi

3. *Annex* 9 : Kontrol Akses (*Access Control*)

Tabel 7 Kontrol Akses

***Annex* : 9 Kontrol Akses**		
Kategori Keamanan Utama : 9.1 Persyaratan Bisnis untuk Akses Kontrol **Objektif kontrol :** untuk mengontrol akses informasi		
9.1.1	Kebijakan Akses kontrol	**Kontrol :** Suatu kebijakan kontrol akses harus dibuat, didokumentasi dan dikaji ulang berdasarkan kebutuhan bisnis dan keamanan akses
Kategori Keamanan Utama : 9.2 Manajemen Akses *User* **Objektif kontrol :** untuk memastikan pengguna yang mempunyai hak akses ke sistem informasi dan yang tidak mempunyai akses		
9.2.1	Registrasi pengguna	**Kontrol :** Harus ada prosedur formal untuk registrasi dan penghapusan user atau pengguna untuk pemberian dan pencabutan akses keseluruhan sistem informasi dan layanannya
9.2.2	Manajemen hak istimewa atau khusus	**Kontrol :** Alokasi penggunaan hak akses istimewa atau khusus harus dibatasi dan diatur
9.2.3	Manajemen *password user*	**Kontrol :** Pembuatan dan penggunaan *password* harus diatur melalaui proses manajemen yang formal
9.2.4	Tinjauan terhadap hak akses user	**Kontrol :** Manajemen harus melakukan tinjauan ulang terhadap hak akses user secara berkala melalui proses yang formal.
Kategori Keamanan Utama : 9.3 Tanggung Jawab Pengguna *(User)* **Objektif kontrol :** untuk mencegah akses user tanpa hak atau pencurian informasi dan fasilitas pemrosesan		
9.3.1	Pengguna *password*	**Kontrol :** Pengguna seharusnya mengikuti praktek keamanan yang baik dalam pemilihan dan penggunaan *password*
9.3.2	Kebijakan *clear desk* dan *clear screen*	**Kontrol :** Kebijakan *clear desk* untuk kertas dan media penyimpanan bergerak atau *portable* dan kebijakan *clear screen* untuk fasilitas pemrosesan informasi harus dijalankan
Kategori Keamanan Utama : 9.4 : Kontrol Akses Sistem Operasi **Objektif kontrol :** untuk mencegah akses tanpa hak ke sistem operasi		
9.4.1	Prosedur *Log-On* yang aman	**Kontrol :** Akses terhadap sistem operasi seharusnya dikontrol dengan prosedur log-on yang aman
9.4.2	Identifikasi dan autentikasi pengguna	**Kontrol :** Seluruh pengguna harus mempunyai ID yang unik untuk penggunaan pribadi dan teknik autentikasi yang tepat harus dipilih untuk memastikan identitas pengguna
9.4.3	Sistem manajemen password	**Kontrol :** Sistem yang digunakan untuk mengelola password harus interaktif dan harus dipastikan password nya berkualitas
9.4.4	Sesi **time-out**	**Kontrol :** Sesi yang tidak aktif seharusnya dimatikan setelah periode tidak aktif yang terdefinisi
9.4.5	Batasan waktu koneksi	**Kontrol :** Batasan dalam waktu koneksi seharusnya digunakan untuk penyediaan keamanan tambahan untuk aplikasi yang tingkat risikonya tinggi.
Kategori Keamanan Utama : 11.5 : Kontrol Akses Informasi dan Aplikasi **Objektif kontrol :** untuk mencegah akses tanpa hak terhadap informasi yang terdapat di dalam aplikasi		
9.5.1	Pembatasan akses informasi	**Kontrol :** Akses terhadap informasi dan sistem aplikasi oleh pengguna harus dibatasi sesuai dengan kebijakan yang ditentukan
9.5.2	Pengisolasian sistem yang sensitif	**Kontrol :** Sistem yang sensitif seharusnya memiliki lingkungan komputer tertentu (terisolir)

4. *Annex* 15 : Kepatuhan (*Compliance*)

Tabel 8 Kepatuhan (*Compliance*)

Kategori Keamanan Utama : 15.1 : Kepatuhan terhadap Persyaratan Legal **Objektif kontrol :** untuk mencegah pelanggaran terhadap hukum, perundangan, peraturan atau kewajiban kontrak dan suatu persyaratan keamanan		
15.1.1	Identifikasi perundangan yang dapat diaplikasikan	**Kontrol :** Seluruh perundangan yang relevan, peraturan harus didefinisikan, didokumentasi, dan dipelihara kesesuaiannya untuk setiap sistem informasi di dalam organisasi
15.1.2	Hak kekayaan intelektual	**Kontrol :** Prosedur-prosedur yang tepat harus diimplementasikan untuk memastikan kesesuaiannya dengan perundangan, Peraturan dalam penggunaan material yang dimungkinkan memiliki hak kekayaan intelektual dan atau penggunaan software yang legal
15.1.3	Perlindungan dokumen organisasi	**Kontrol :** Dokumen penting harus dilindungi dari kehilangan,kerusakan,pemalsuan dalam hubungannya terhadap perundangan dan peraturan
15.1.4	Perlindungan data dan kerahasiaan informasi personal	**Kontrol :** Proteksi data dan privasi seharusnya dipastikan sesuai dengan perundangan, regulasi yang berlaku.
15.1.5	Pencegahan penyalagunaan fasilitas pemrosesan informasi	**Kontrol :** Pengguna harus dicegah untuk menggunakan fasilitas pemrosesan informasi untuk kepentingan atau tujuan diluar haknya
Kategori Keamanan Utama : 15.2 : kepatuhan dengan kebijakan keamanan, standard dan kepatuhan teknik **Objektif kontrol :** untuk memastikan kepatuhan terhadap sistem didalam kebijakan keaman organisasi dan standar		
15.2.1	Kepatuhan dengan kebijakan keamanan dan standar	**Kontrol :** Manajer harus memastikan seluruh prosedur keamanan di dalam area tanggung jawab dilakukan dengan benar untuk mencapai kepatuhan dengan standar yang ditetapkan
15.2.2	Pemeriksaan kepatuhan teknik	**Kontrol :** Sistem informasi harus diperiksa secara berkala agar memenuhi kepatuhan keamanan standar yang diimplementasikan
Kategori Keamanan Utama : 15.3 : Audit sistem Informasi dan pertimbangan **Objektif kontrol :** untuk memaksimalkan keefektifitasan dan meminimisasi interferensi dari atau ke dalam proses audit sistem informasi		
15.3.1	Kontrol audit sistem informasi	**Kontrol :** Kebutuhan audit dan aktivitas yang melibatkan pengecekan terhadap sistem operasional seharusnya direncanakan dan disetujui untuk memininalkan risiko gangguan terhadap proses bisnis
15.3.2	Perlindungan terhadap perangkat audit sistem informasi	**Kontrol :** Akses ke perangkat audit sistem informasi harus dilindungi untuk mencegah kemungkinan penyalagunaan atau kompromi

KESIMPULAN

1. Dari hasil penelitian teridentifikasi bahwa klausul yang digunakan adalah, *annex* 5 : Kebijakan Keamanan (*Security Policy*), *annex* 7 : Manajemen Aset (*Asset Management*), *annex* 9 : Kontrol Akses (*Access Control*) dan *annex* 15 : Kepatuhan (*Compliance*).
2. Pada *annex* 5 tentang *Security policy* (Kebijakan Keamanan) saat ini kebijakan keamanan SIMAK pada STMIK Mardira Indonesia masih belum sesuai.
3. Pada *annex* 7 *Asset Management* (Manajemen Aset) berarti saat ini kebijakan manajemen aset SIMAK pada STMIK Mardira Indonesia masih belum sesuai dikarenakan belum adanya surat kebijakan tentang pengelolaan aset, untuk mencapai dan memelihara perlindungan yang sesuai terhadap aset organisasi.
4. Pada *annex* 11 bahwa perlu membangun kebijakan yang ditetapkan dan tidak terjadi penyalahgunaan hak akses serta adanya prosedur pengendalian hak akses dan mencegah adanya akses secara tidak berwenang terhadap informasi dan fasilitas sistem informasi.
5. Pada *annex* 15 tentang *Compliance* (Kepatuhan) bahwa kegiatan yang dilakukan dalam sistem informasi akademik belum disesuaikan dengan peraturan akademik yang berlaku, serta waktu yang telah dijadwalkan pada kalender pendidikan.

REFERENSI

[1] J. Long "List of ITIL Processes," *SpringerBriefs in Computer Science*, 2012.

[2] R. Rizaldi, "Audit Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 5 (Studi Kasus: Pt.indocom Tambak Udang Lampung)," Jan. 2019.

[3] Priandono, Anjar. "Comparison between COBIT, ITIL and ISO27001."

[4] IT Governance Institute, "COBIT 4.1," Illinois : IT Governance Institute, 2007.

[5] Sarno, Riyanarto. "Audit Sistem & Teknologi Informasi," Surabaya : itspress, 2009.

[6] Sarno, R. "Iffano, Sistem Manajemen Keamanan Informasi," Surabaya, 2009.

[7] Hutahaean, Jeperson. "Konsep Sistem Informasi," Yogyakarta: Deepublish, 2014.

[8] Jogiyanto, H.M 2005. "Analisis dan Desain Sistem Informasi," Edisi ketiga, Cetakan pertama, Andi Offset, Yogyakarta.

[9] Catur Daya Solusi, "Upgrading ISO 27001:2005 ke ISO 27001:2013," 9 Maret 2015. [Online]. Available: http://caturdayasolusi.com/upgrading-iso-270012005-ke-iso-270012013/.[7] A. M. Wibowo, ISO 27001 Informations Security Management Systems, 2005.

[10] IAS. 2013. ISO 27001 : 2013 Compliance Checklist ISO 27001 : 2013 Compliance Checklist.

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

[12] Carcary, M. 2012. IT Risk Management : A Capability Maturity Model Perspective. Electronic Journal Information Systems Evaluation, 16(3), 3–13. Retrieved from www.ejise.com

[13] Ikhsan, M., & Suwawi, D. D. J. (2016). Audit Keamanan Sistem Informasi Akademik Sekolah Tinggi Farmasi Bandung Berbasis Risiko Dengan Menggunakan Standar Iso 27001. *eProceedings of Engineering*, *3*(3). Farmasi Bandung Berbasis Risiko Dengan Menggunakan Standar Iso 27001:2009

[14] Bless, Y. C., Sasmita, G. M. A., & Cahyawan, A. K. A. (2014). Audit

Keamanan SIMAK Berdasarkan ISO 27002 (Studi Kasus: FE UNUD). *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*.

[15] Winanti, M. B., & Dzulhan, I. (2018). Audit Keamanan Sistem Informasi Akademik Dengan Kerangka Kerja ISO 27001 Di Program Studi Sistem Informasi Unikom. *Majalah Ilmiah Unikom*, *16*(2), 1-12.

[16] Afandi, H., & Darmawan, A. (2017). Audit Kemanan Informasi Menggunakan Iso 27002 Pada Data Center Pt. Gigipatra Multimedia. *Jurnal Teknologi Informasi Magister*, *1*(02), 175-191.

[17] Satyareni, D. H., & Mahanani, F. (2014, June). Audit Sistem Informasi Akademik Perguruan Tinggi (PT) XYZ Menggunakan Kerangka Kerja COBIT 4.1. In *Seminar Nasional Aplikasi Teknologi Informasi (SNATI)* (Vol. 1, No. 1).

[18] Azizah, N. (2017). Audit Sistem Informasi Menggunakan Framework COBIT 4.1 Pada E-Learning UNISNU Jepara. *Simetris: Jurnal Teknik Mesin, Elektro dan Ilmu Komputer*, *8*(1), 377-382.

[19] Fitrianah, D., & Sucahyo, Y. G. (2008). Audit Sistem Informasi/Teknologi Informasi dengan kerangka kerja COBIT untuk evaluasi manajemen teknologi informasi di Universitas XYZ. *Jurnal Sistem Informasi*, *4*(1), 37-46.

[20] Purba, A. D., Purnawan, I. K. A., & Pratama, I. P. A. E. (2018). Audit Keamanan TI Menggunakan Standar ISO/IEC 27002 dengan COBIT 5. *Jurnal Ilmiah Merpati (Menara Penelitian Akademika Teknologi Informasi)*, 148-158.

[21] Sukmajaya, I. B., & Andry, J. F. (2017, November). Audit Sistem Informasi Pada Aplikasi Accurate Menggunakan Model Cobit Framework 4.1 (Studi Kasus: Pt. Setia Jaya Teknologi). In *Prosiding Seminar Nasional Teknoka* (Vol. 2, pp. I42-I51).

[22] Ramdhany, T., & Asikin, M. D. (2018). AUDIT SISTEM INFORMASI APLIKASI STARCLICK MENGGUNAKAN FRAMEWORK COBIT 4.1 DOMAIN DELIVER AND SUPPORT DI PT. TELEKOMUNIKASI REGIONAL III JAWA BARAT. *Jurnal Komputer Bisnis*, *11*(1), 33-39.

[23] Gunawan, R., & Tjahjadi, D. (2018). AUDIT SISTEM INFORMASI AKADEMIK BERBASIS WEB MENGGUNAKAN FRAMEWORK COBIT 5.0 PADA DOMAIN APO13 DAN DSS05 (Studi Kasus: SIAT STMIK ROSMA KARAWANG). Jurnal Interkom, 13(3).