AUDIT KEAMANAN SISTEM INFORMASI AKADEMIK (SIAKAD) UNIVERSITAS LAMPUNG MENGGUNAKAN STANDAR ISO/IEC 27001

(Skripsi)

Oleh

DESTA RIANI

PROGRAM STUDI ILMU KOMPUTER
JURUSAN ILMU KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMPUNG

2018

ABSTRACT

SECURITY AUDIT OF ACADEMIC INFORMATION SYSTEM (SIAKAD) OF UNIVERSITY LAMPUNG USING ISO/IEC 27001 STANDARD

By

DESTA RIANI

The process of service control and poor business process control on information system assets are facilitating irresponsible parties to disrupt activities about organizational assets. The risk of information security is influenced by the high needs of the organization to obtain an information. The research was conducted to find out how far Siakad University of Lampung readiness level to meet an international security standard. This study focuses on Siakad's organizational compliance with security controls based on Annex A ISO 27001: 2013 and risk analysis of assets by determining the current condition (inherent risk). The research data was obtained based on interviews with related parties of Siakad management. The result of the research found that the value of Siakad University of Lampung security index based on ISO 27001 standard is currently worth 2.90. When it rounded into the maturity index, Siakad security is currently entering Level 3 or largely managed (defined).

Keywords : ISO 27001; Security Audits; Academic Information System.

ABSTRAK

AUDIT KEAMANAN SISTEM INFORMASI AKADEMIK (SIAKAD) UNIVERSITAS LAMPUNG MENGGUNAKAN STANDAR ISO/IEC 27001

Oleh

DESTA RIANI

Masih minimnya proses kendali pelayanan dan pengawasan bisnis proses pada aset sistem informasi memudahkan pihak yang tidak bertanggungjawab untuk mengganggu jalannya aktivitas terkait pada aset organisasi. Meningkatnya sifat bergantungan pada informasi sejalan dengan meningkatnya resiko yang terjadi, salah satu resiko yang mungkin terjadi yaitu resiko keamanan informasi. Penelitian ini dilakukan untuk mengetahui sejauh mana tingkat kesiapan Siakad Universitas Lampung untuk memenuhi sebuah standar keamanan. Penelitian ini berfokus pada kepatuhan organisasi pengelola Siakad terhadap kontrol keamanan berdasarkan lampiran A ISO 27001:2013 dan analisa resiko aset dengan menentukan kondisi resiko saat ini. Data dari penelitian didapatkan berdasarkan hasil wawancara oleh pihak terkait pengelola Siakad. Hasil penelitian menemukan bahwa nilai indeks keamanan Siakad Universitas Lampung menggunakan standar ISO 27001 saat ini bernilai 2.90. Jika dibulatkan ke dalam indeks maturity, keamanan Siakad saat ini telah memasuki Level 3 atau sebagian besar telah terkelola (*defined*).

Kata Kunci : Audit Keamanan, ISO 27001; Sistem Informasi Akademik.

AUDIT KEAMANAN SISTEM INFORMASI AKADEMIK (SIAKAD) UNIVERSITAS LAMPUNG MENGGUNAKAN STANDAR ISO/IEC 27001

Oleh
Desta Riani

Skripsi
Sebagai Salah Satu Syarat untuk Memperoleh Gelar
SARJANA KOMPUTER

Pada
Jurusan Ilmu Komputer
Fakultas Matematika Dan Ilmu Pengetahuan Alam

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMPUNG
2018

Judul Skripsi	:	**AUDIT KEAMANAN SISTEM INFORMASI AKADEMIK (SIAKAD) UNIVERSITAS LAMPUNG MENGGUNAKAN STANDAR ISO/IEC 27001**
Nama Mahasiswa	:	Desta Riani
Nomor Pokok Mahasiswa	:	1417051037
Jurusan	:	Ilmu Komputer
Fakultas	:	Matematika dan Ilmu Pengetahuan Alam

MENYETUJUI

1. Komisi Pembimbing

Dr. Ir. Kurnia Muludi, M.S.Sc.	**Rizky Prabowo, M.Kom.**
NIP 19640616 198902 1 001	NIK 231708880807101

2. Ketua Jurusan Ilmu Komputer

Dr. Ir. Kurnia Muludi, M.S.Sc.
NIP 19640616 198902 1 001

MENGESAHKAN

1. Tim Penguji

Ketua : **Dr. Ir. Kurnia Muludi, M.S.Sc.** .....

Sekretaris : **Rizky Prabowo, M.Kom.** .....

Penguji
Bukan Pembimbing : **Didik Kurniawan, S.Si., M.T.** .....

2. Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam

Prof. Warsito, S.Si., D.E.A., Ph.D.
NIP 19710212 199512 1 001

Tanggal Lulus Ujian Skripsi : **20 Juli 2018**

PERNYATAAN

Saya yang bertanda tangan di bawah ini, menyatakan bahwa skripsi saya yang berjudul **"Audit Keamanan Sistem Informasi Akademik (Siakad) Universitas Lampung menggunakan Standar ISO/IEC 27001"** Merupakan karya saya sendiri bukan hasil karya orang lain. Semua tulisan yang tertuang di skripsi ini telah mengikuti kaidah penulisan karya ilmiah Universitas Lampung. Apabila terbukti di kemudian hari bahwa skripsi saya merupakan hasil penjiplakan atau dibuat orang lain, maka saya bersedia menerima sanksi berupa pencabutan gelar yang telah saya terima.

Bandar Lampung, 25 Juli 2018

Desta Riani
NPM. 1417051037

RIWAYAT HIDUP

Penulis dilahirkan di Bandar Lampung Provinsi Lampung pada tanggal 31 Desember 1995, sebagai anak kedua dari dua bersaudara dengan ayah bernama Dasmir dan ibu bernama Yusriati. Penulis memiliki seorang kakak perempuan bernama Gustia Yolanda.

Penulis menyelesaikan Taman Kanak-Kanak (TK) pada tahun 2002 di TK Aisyah Bandar Lampung, Sekolah Dasar (SD) di SD Negeri 2 Sukajawa pada tahun 2008, Sekolah Menengah Pertama di SMP Negeri 9 Bandar Lampung pada tahun 2011, dan Sekolah Menengah Atas di SMA Negeri 1 Bandar Lampung pada tahun 2014.

Pada Tahun 2014, penulis terdaftar sebagai mahasiswa Jurusan Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung melalui jalur SNMPTN. Selama menjadi mahasiswa penulis aktif dalam Organisasi Himpunan Mahasiswa Jurusan Ilmu Komputer (Himakom) sebagai Sekretaris Bidang Internal. Pada bulan Juli-September 2017, penulis melakukan Kuliah Kerja Nyata selama 40 hari di Desa Ketapang, Kecamatan Ketapan, Kabupaten Lampung Selatan. Selama menjadi mahasiswa, penulis aktif mengikuti beberapa kegiatan, antara lain:

1. Anggota Abacus Himakom 2014-2015.
2. Anggota Bidang Internal Himakom 2015-2016.
3. Sekretaris Bidang Internal Himakom 2016-2017.

4. Melaksanakan Kerja Praktik di Divisi Pelayanan Kantor Pelayanan Pajak (KPP) Pratama Tanjung Karang Barat pada tanggal 16 Januari-24 Februari 2017.
5. Anggota Kehormatan (AK) Himakom 2017-2018.

PERSEMBAHAN

Puji dan syukur saya panjatkan kepada Allah SWT, atas segala berkat, rahmat, hidayah-Nya sehingga skripsi ini dapat terselesaikan.

Kupersembahkan karya kecilku ini untuk:

Orangtua yang telah mendidik, membesarkan, menjaga, melindungi, memberikan motivasi, dan doa yang selalu tulus dipanjatkan kepada Allah SWT demi kesuksesan anak-anaknya.

Keluarga dekat yang telah memberikan semangat dalam mengejar cita-cita.

Keluarga Ilmu Komputer 2014.

Terimakasih terhadap apapun yang telah kalian berikan.

MOTO

“Hal kecil di masa sekarang akan mempengaruhi masa yang akan datang.”

“Lakukan setiap pekerjaan dengan ikhlas, inshallah pekerjaan akan terasa ringan.”

“Lakukan hari ini atau tidak sama sekali.”

SANWACANA

Puji syukur penulis panjatkan kehadirat Allah SWT atas berkat, rahmat, hidayah, dan kesehatan yang diberikan sehingga penulis dapat menyelesaikan penelitian ini. Penelitian dilakukan sebagai syarat untuk memperoleh gelar Sarjana Ilmu Komputer Universitas Lampung. Judul penelitian ini adalah, "Audit Keamanan Sistem Informasi Akademik Universitas Lampung menggunakan Standar ISO/IEC 27001"

Dalam penyusunan skripsi ini, penulis banyak menghadapi kesulitan. Namun, berkat bantuan dan dorongan dari berbagai pihak, penulis dapat menyelesaikan skripsi ini. Oleh karena itu, penulis mengucapkan terimakasih kepada:

1. Mama dan kakak yang telah memberikan doa dan motivasi serta memfasilitasi kebutuhan untuk menyelesaikan skripsi ini.
2. Bapak Dr. Ir. Kurnia Muludi, M.S.Sc., selaku Ketua Jurusan Ilmu Komputer sekaligus sebagai pembimbing I penulis yang telah memberikan ide, masukan, dan dorongan sehingga skripsi ini dapat diselesaikan.
3. Bapak Rizky Prabowo, M. Kom., sebagai pembimbing II yang telah memberikan saran dan membimbing penulis dalam pembuatan skripsi ini.
4. Bapak Didik Kurniawan, S.Si.,M.T., sebagai Sekretaris Jurusan Ilmu Komputer sekaligus pembahas yang telah memberikan masukan-masukan dan saran yang bermanfaat dalam skripsi ini.

5. Bapak Dr. Eng, Helmy Fitriawan, S.T.,M.Sc selaku Kepala UPT. TIK Universitas Lampung yang telah membantu jalannya penelitian.
6. Bapak Gigih Forda Nama, M.T., sebagai Kepala Divisi Infrastruktur UPT. TIK Universitas Lampung yang telah memberikan data, dukungan, saran, dan masukan sehingga skripsi ini dapat terselesaikan.
7. Bapak Aristoteles, S.Si., M.Si., sebagai pembimbing akademik penulis yang telah memberikan saran, motivasi, dan bimbingan selama menjalani masa perkuliahan di Jurusan Ilmu Komputer.
8. Bapak Prof. Warsito, S.Si, D.E.A., Ph.D., selaku Dekan FMIPA Universitas Lampung.
9. Bapak dan Ibu Dosen Jurusan Ilmu Komputer yang telah memberikan ilmu pengetahuan yang bermanfaat bagi penulis.
10. Ibu Ade Nora Maela selaku staf administrasi di Jurusan Ilmu Komputer yang telah membantu segala urusan administrasi selama kuliah.
11. Seluruh staf UPT. TIK Universitas Lampung yang telah mendukung dan memberi semangat dalam penyelesaian skripsi ini.
12. Sahabat, rekan, rival, sekaligus kakak yang telah memberikan masukan, bimbingan, dan motivasi kepada penulis.
13. Rekan-rekan seperjuangan Arien, Annisa, Dwi, Eindita, Elfeny, Gisella, Hanifah, dan Sela yang telah memberikan penulis inspirasi dan keceriaan selama perkuliahan.
14. Teman-teman Ilmu Komputer 2014, yang telah berjuang bersama-sama dalam menjalankan studi di Jurusan Ilmu Komputer Universitas Lampung.

Penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan, akan tetapi sedikit harapan semoga skripsi ini bermanfaat bagi perkembangan ilmu pengetahuan terutama bagi rekan-rekan Ilmu Komputer.

Bandar Lampung, 25 Juli 2018

Desta Riani

DAFTAR ISI

Halaman

COVER ..... **i**
ABSTRAK ..... **ii**
DAFTAR ISI ..... **xv**
DAFTAR GAMBAR ..... **xviii**
DAFTAR TABEL ..... **xix**
I. PENDAHULUAN **1**
1.1 Latar Belakang 1
1.2 Rumusan Masalah 4
1.3 Batasan Masalah 5
1.4 Tujuan Penelitian 5
1.5 Manfaat 6
II. TINJAUAN PUSTAKA **7**
2.1 Penelitian Terdahulu 7
2.2 Keamanan Informasi 9
2.3 Keamanan Teknologi Informasi 12
2.4 Audit 13
2.5 Audit Internal 13
2.6 Audit Berbasis Resiko 14
2.7 Karakteristik Audit Teknologi Informasi (TI) 15
2.8 Sertifikasi Audit 16
2.9 ISO/IEC 27000 *Series* 18
2.10 ISO/IEC 27001 22
2.11 *Maturity Level* 24
III. METODOLOGI PENELITIAN **27**
3.1 Waktu dan Tempat 27
3.2 Data 27
3.3 Metode Penelitian 28

3.1.1 Identifikasi Masalah 29
3.1.2 Studi Literatur 29
3.1.3 Menentukan Ruang Lingkup dan Tujuan Audit 29
3.1.4 Identifikasi Proses Bisnis TI 30
3.1.5 Observasi dan Wawancara 30
3.1.6 Review Kelengkapan Dokumen 32
3.1.7 Analisis *Gap* 33
3.1.8 *Risk Assessment* 33
3.1.9 Menetapkan Kontrol 34
3.1.10 Melakukan Dokumentasi (Data dan Bukti) 36
3.1.11 Penyusunan Daftar Temuan dan Rekomendasi 36
3.2 *Audit Working Plan* 37
IV. HASIL DAN PEMBAHASAN 39
4.1 Identifikasi Proses Bisnis TI 39
4.1.1 Gambaran Umum Instansi/Organisasi 39
4.1.2 Visi dan Misi 40
4.1.3 Tujuan Universitas Lampung 41
4.1.4 Sasaran Strategis Universitas Lampung 42
4.1.5 Infrastruktur TIK Universitas Lampung 43
4.1.6 Sistem Informasi Universitas Lampung 44
4.1.7 Gambaran Umum Pengelolaan Siakad Universitas Lampung 46
4.2 Pemodelan ISMS (*Plan)* 47
4.2.1 Menentukan Ruang Lingkup 48
4.2.2 Gap Analisis 49
4.2.3 *Risk Assessment* 59
4.3 Analisa Resiko 64
4.3.1 Menentukan Kontrol 79
4.3.2 Kontrol Mitigasi Resiko 83
4.4 Analisis Penerapan Kontrol ISO 27001 88
4.5 Kebijakan dan Prosedur Keamanan Informasi 107
V. KESIMPULAN DAN SARAN 109
5.1 Kesimpulan 109
5.2 Saran 110

DAFTAR PUSTAKA 111
LAMPIRAN 113

DAFTAR GAMBAR

Halaman

Gambar 1. *Risk Management and Treatment Process* ISO 27001 24
Gambar 2. Metodologi Penelitian 28
Gambar 3. Struktur Organisasi Universitas Lampung 40
Gambar 4. Pengelola Siakad Universitas Lampung..... 47
Gambar 5. Proses ISMS *Plan* 47
Gambar 6. Proses Perencanaan ISMS 48
Gambar 7. Implementasi 114 Kontrol ISO 27001 Siakad Universitas Lampung. 57
Gambar 8. *Actual Condition* dan *Best Practice* pada Penerapan ISO 27001..... 58
Gambar 9. Proses *Risk Assessment* 59

DAFTAR TABEL

Halaman

Tabel 1. Penelitian terkait Keamanan Sistem Informasi 7
Tabel 2. Macam-macam sertifikasi dan standar..... 17
Tabel 3. Standar Seri ISO 27000..... 19
Tabel 4. Contoh penilaian *maturity level*. 25
Tabel 5. Skala Pembulatan Indeks 26
Tabel 6. Bagian Pengelola Siakad Universitas Lampung 31
Tabel 7. Penilaian Gap ISO 27001..... 33
Tabel 8. Domain dan Kontrol Objektif ISO 27001..... 35
Tabel 9. *Audit Working Plan*..... 37
Tabel 10. Internet Universitas Lampung sejak 1996-2015 43
Tabel 11. Sistem Informasi Universitas Lampung..... 45
Tabel 12. Perhitungan *Gap Assessment* untuk domain ISO 27001..... 50
Tabel 13. *Actual Condition* Penerapan ISMS Siakad Universitas Lampung..... 57
Tabel 14. Identifikasi Aset Sistem Informasi Akademik Universitas Lampung .. 60
Tabel 15. Identifikasi Kerawanan 61
Tabel 16. Identifikasi Ancaman 61
Tabel 17. Nilai Kecenderungan..... 62
Tabel 18. Nilai Dampak 63
Tabel 19. *Risk Matrixs* 63
Tabel 20. Langkah Pengendalian Resiko 64
Tabel 21. Prioritas Resiko 65
Tabel 22. Pengendalian Resiko (*Residual Risk*) 70
Tabel 23. Hasil Analisa Resiko..... 73
Tabel 24. Kontrol ISO 27001 untuk *Vulnerability Management*..... 79
Tabel 25. Kontrol ISO 27001 untuk *Threats Management* 80
Tabel 26. ISO 27001 untuk *Impacs* 82

Tabel 27. Sasaran kemanan informasi 84
Tabel 28. Upaya mitigasi resiko dari identifikasi aset 84
Tabel 29. Analisis *Existing Control* Siakad 88
Tabel 30. Dokumen terkait ISMS 114
Tabel 31. Dokumen terkait ISO/IEC 27001 114

BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi Informasi (TI) saat ini telah banyak diterapkan oleh hampir seluruh organisasi, baik dari pemerintahan, sektor industri perusahaan, bidang pendidikan, kesehatan, dan lainnya. TI masih dipercaya dalam membantu meningkatkan efisiensi dan efektifitas suatu organisasi dalam menciptakan layanan yang berkualitas dari proses bisnisnya. Masih minimnya proses kendali pelayanan dan pengawasan bisnis proses pada aset sistem informasi memudahkan pihak yang tidak bertanggungjawab untuk mengganggu jalannya aktivitas terkait pada aset organisasi. Meningkatnya sifat bergantungan pada informasi sejalan dengan meningkatnya resiko yang mungkin terjadi, salah satu resiko yang mungkin terjadi yaitu resiko keamanan informasi.

Penggunaan standar keamanan dan pelayanan dalam memandu jalannya proses bisnis dapat menjadi salah satu solusi dalam meminimalisir terjadinya gangguan yang tidak diinginkan. Akan tetapi, organisasi memiliki kesulitan tersendiri dalam memahami sudah sejauh mana standar tersebut dapat terimplementasikan, terlebih ketika organisasi mengimplementasikan lebih dari satu buah standar. Hal ini dimungkinkan terjadi karena ruang lingkup atau fokus cakupan standar dirasa kurang luas untuk memenuhi seluruh cakupan manajemen (Gehrmann, 2012).

Dengan memiliki kontrol terhadap akses informasi, organisasi dapat meminimalkan kerugian yang diakibatkan oleh hilangnya data yang disebabkan oleh penyalahgunaan akses.

Universitas Lampung merupakan perguruan tinggi negeri yang telah mengaplikasikan penggunaan teknologi informasi sebagai pendukung proses bisnisnya. Universitas Lampung memiliki Sistem Informasi Akademik (Siakad) yang mengintegrasikan proses bisnis yang terkait dalam kegiatan akademik dan administrasi mahasiswa. Pengelolaan Informasi yang tidak baik dapat berdampak pada rendahnya kualitas layanan dan rendahnya tingkat kepuasan mahasiswa, sehingga hal tersebut dapat mempengaruhi kepercayaan *user* terhadap institusi tersebut. Hal tersebut dapat diatasi dengan melakukan audit keamanan sistem informasi yang diterapkan sesuai dengan prosedur terhadap pelaksanaan Sistem Informasi Akademik Universitas Lampung dan standar yang digunakan yaitu ISO/IEC 27001.

Audit merupakan proses yang sitematis, mandiri, dan terdokumentasi untuk memperoleh bukti audit dan mengevaluasinya secara objektif sejauh mana kriteria audit terpernuhi. Dengan kata lain, pemeriksaan ini dilakukan berdasarkan standar yang digunakan berupa ISO/IEC 27001 maupun standar lain yang digunakan oleh institusi termasuk dokumen sistem manajemen mutu yang dimiliki, pencapaian sasaran mutu, meninjau keluhan *user*, dan lain-lain (Zuhrawaty, 2009).

Beberapa hal penting yang dapat dijadikan acuan mengapa standar ISO/IEC 27001 dipilih yaitu, standar ini sangat fleksibel karena sangat bergantung pada kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis, jumlah pegawai,

dan struktur organisasi. Selain itu, ISO/IEC 27001 menyediakan sertifikat implementasi Sistem Manajemen Keamanan Informasi yang telah diakui secara Internasional yang disebut dengan *Information Security Manajemen System* (ISMS) *certification* (Sarno dan Ifanno, 2009).

ISO/IEC 27001 menyatakan prasyarat utama yang harus dipenuhi menyangkut konteks organisasi, kepemimpinan, perencanaan, *support*, operasional, evaluasi kinerja, dan *improvement*. Selain itu, ISO 27001 telah menetapkan sasaran kontrol dan kontrol-kontrol keamanan informasi meliputi 14 area pengamanan yang akan dibahas dalam penelitian ini.

Studi yang dilakukan oleh Bahareh dan Hannes dalam mengevaluasi keefektifan ISO/IEC 27001:2013 berdasarkan *Annex* A mengklarifikasikan kontrol menjadi lima kategori, yaitu data, perangkat keras, perangkat lunak, sumber daya manusia, dan jaringan yang dapat membantu organisasi dalam mengevaluasi kinerja ISMS. Hasil yang didapatkan bahwa ISO 27001 menyajikan standar yang diperbaharui dan menyajikan panduan yang sesuai untuk mengevaluasi kinerja. Selain itu, audit dengan menggunakan standar ISO 27001 yang sebelumnya telah dilakukan oleh (Fine *et al*, 2012) mengenai Audit Keamanan Sistem Informasi pada PT. BPR Jatim menyimpulkan bahwa kontrol keamanan yang telah diterapkan dalam proses bisnis PT. BPR Jatim masih berada dalam *level* 2 *planned and tracked* sehingga diperlukan peningkatan kontrol keamanan yang telah direkomendasikan. Penelitian berbeda yang dilakukan oleh (Hsu *et al*, 2016) mengenai Dampak dari Sertifikat ISO 27001 pada kinerja perusahaan, penelitian mengambil sampel perusahaan dari Amerika dan negara-negara Eropa yang memiliki sertifikat ISO 27001. Penelitian ini menunjukkan bahwa tidak ditemukannya dampak yang signifikan terhadap

kinerja perusahaan dan pasar saham, namun dapat disimpulkan bahwa standarisasi keamanan informasi ISO/IEC 27001 merupakan kewajiban yang harus dipenuhi oleh instansi sehingga informasi dapat terjaga dengan baik, bukan merupakan keunggulan kompetitif melainkan kebutuhan suatu organisasi untuk menjaga keamanan suatu informasi.

Berdasarkan uraian diatas, penulis akan melakukan penelitian mengenai Audit Keamanan Sistem Informasi Akademik (Siakad) Universitas Lampung Menggunakan Standar ISO/IEC 27001. Dengan adanya penelitian ini diharapkan mampu memberikan rekomendasi terhadap peningkatan keamanan informasi pada Siakad Universitas Lampung.

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, adapun rumusan masalah yang dibahas pada penelitian ini adalah sebagai berikut:

1. Apakah kepatuhan organisasi terhadap capaian dan tindakan yang diterapkan telah memenuhi aspek keamanan informasi?
2. Apakah kebijakan dan prosedur yang ada telah memenuhi aspek keamanan informasi?
3. Apakah rekomendasi atau saran perbaikan terhadap kebijakan dan prosedur yang akan dibuat dapat meningkatkan keamanan informasi?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini adalah sebagai berikut:

1. *Framework* audit keamanan sistem informasi yang digunakan adalah standar ISO/IEC 27001.
2. Data audit sebagai acuan yang digunakan adalah hasil wawancara.
3. Audit menggunakan *checklist* yang terdapat dalam panduan ISO 27001:2013.
4. Identifikasi aset berasal dari hasil wawancara dan diskusi staff UPT TIK.
5. Output yang dihasilkan merupakan temuan dan rekomendasi hasil audit keamanan Siakad Universitas Lampung.

1.4 Tujuan Penelitian

Tujuan dari Audit Keamanan Sistem Informasi ini adalah sebagai berikut:

1. Mengetahui apakah kepatuhan organisasi terhadap tujuan dan prosedur telah memenuhi aspek keamanan informasi.
2. Mengetahui apakah kebijakan dan prosedur yang telah diterapkan telah memenuhi aspek keamanan informasi.
3. Mengetahui apakah rekomendasi atau perbaikan kebijakan dan prosedur dapat meningkatkan keamanan berdasarkan aspek keamanan informasi.

1.5 Manfaat

Adapun manfaat dari penelitian ini adalah sebagai berikut:

1. Menghasilkan dokumentasi hasil audit keamanan Siakad Universitas lampung berdasarkan dokumen temuan audit dan rekomendasi hasil Audit.
2. Memberikan rekomendasi kelengkapan mengenai kebijakan dan prosedur sehingga dapat meningkatkan aspek keamanan informasi.
3. Memperoleh data kondisi *existing* tentang ISMS di Siakad Universitas Lampung.

BAB II
TINJAUAN PUSTAKA

2.1 Penelitian Terdahulu

Terdapat beberapa penelitian mengenai Audit Keamanan Sistem Informasi, diantaranya adalah sebagai berikut:

Tabel 1. Penelitian terkait Keamanan Sistem Informasi

No.	Peneliti	Masalah	Metode	Hasil
1.	(Windirya, 2005)	Audit Keamanan Sistem Informasi pada Instalasi Sistem Informasi Manajemen RSUD Bangil sBerdasarkan ISO 27002	Metode yang digunakan yaitu 5 jenis klausul pada kerangka kerja ISO 27002:2005, yaitu Manajemen aset, Keamanan Sumber Daya Manusia, Keamanan Fisik dan Lingkungan, Kontrol Akses, dan Akusisi Sistem Informasi, Pengembangan dan Pemeiliharaan.	Hasil pemeriksaan kontrol keamanan audit diperoleh tingkat kematangan sistem sebesar 2,72.

Tabel 1. Penelitian terkait Keamanan Sistem Informasi (Lanjutan)

No.	Peneliti	Masalah	Metode	Hasil
2.	(Ikhsan *et al*, 2016)	Audit Keamanan Sistem Informasi Akademik Sekolah Tinggi Farmasi Bandung Berbasis Risiko dengan Menggunakan Standar ISO 27001	Standar yang digunakan yaitu ISO 27001:2009 menggunakan 4 klausal yang telah tersedia, yaitu A.9, A.11, A.12, dan A.13 berdasarkan tingginya *level* resiko.	Diperoleh nilai kematangan pada 4 klausal keamanan yang bernilai 2.5 yang berarti kontrol keamanan masih berada pada *level* 2.
3.	(Ciptaningrum *et al*, 2015)	Audit Keamanan Sistem Informasi Pada Kantor Pemerintah Kota Yogyakarta Menggunakan COBIT 5	Framework yang digunakan adalah COBIT 5 menggunakan domain EDM 03, APO 12, APO 13, BAI 06, DSS 05 untuk keamanan sistem informasi	Terdapat empat domain yang berada pada *level* P (*Partially Achieved*), yaitu proses EDM03, APO12, APO13, dan BAI06. Sedangkan DSS05 berada pada *level* L (*Largely Achieved*).

2.2 Keamanan Informasi

Keamanan informasi merupakan salah satu hal penting yang harus diperhatikan oleh perusahaan ataupun organisasi, adanya kebocoran informasi dan kegagalan sistem dapat menyebabkan kerugian baik di sisi finansial maupun produktifitas perusahaan. Keamanan informasi meliputi suatu mekanisme untuk mengontrol akses dan penggunaan *database* pada *level* obyek bagi pengguna, dimana pengguna tersebut memiliki akses terhadap informasi tertentu. Perngaturan utama mengenai keamanan informasi akan ditentukan berdasarkan seberapa jauh tingkat keamanan yang akan dibangun untuk informasi *database*. Tingkat keamanan informasi juga sangat bergantung pada tingkat sensitifitas informasi dalam *database*. Biasanya informasi yang tidak terlalu sensitif memiliki sistem keamanan yang tidak ketat, sedangkan informasi yang sangat sensitif perlu pengaturan keamanan yang ketat dalam akses informasi tersebut (Mufadhol, 2009).

Ancaman-ancaman (*Threats*) keamanan informasi dapat meliputi orang, organisasi, mekanisme, atau peristiwa yang memiliki potensi yang dapat membahayakan sumber daya informasi perusahaan, ancaman dapat bersifat internal mauput eksternal serta disengaja maupun tidak disengaja (McLeod dan Schell, 2007).

Keamanan infromasi adalah salah satu upaya untuk mengamankan aset informasi yang dimiliki (Syafrizal, 2007). Sedangkan informasi sendiri merupakan suatu aset penting yang harus dilindungi keamanannya. Keamanan secara umum diartikan sebagai ‘*quality or state of being secure-to be free from danger’*. Untuk menjadi aman adalah dengan cara dilindungi dari musuh dan bahaya (Whitmann dan Mattord, 2016).

Menurut (Hidayat, 2011) terdapat beberapa strategi yang dapat dilakukan untuk mengamankan informasi diantaranya adalah sebagai berikut :

1. *Physical security*

   Strategi yang memfokuskan pada hal-hal fisik seperti mengamankan dan memberikan perlindungan kepada karyawan, aset-aset fisik seperti hardware, perlindungan tempat kerja dan aktivitas-aktivitas yang dapat menyebabkan kerugian pada suatu organisasi.

2. *Personal security*

   Strategi yang memfokuskan pada keadaan individu seperti memberikan *awareness* terhadap pentingnya keamanan informasi.

3. *Operation security*

   Strategi yang memfokuskan pada kelancaran perusahaan dalam melakukan kegiatan operasionalnya tanpa gangguan dari pihak luar.

4. *Communication security*

   Streategi yang memfokuskan pada pengamanan media komunikasi dan teknologi komunikasi untuk memenuhi fungsi komunikasi dalam organisasi.

5. *Network security*

   Strategi yang memfokuskan pada pengamanan jaringan dan kemampuan jaringan dalam memenuhi fungsi jaringan dalam organisasi.

Menurut (Syafrizal, 2007), Keamanan Informasi terdiri dari tiga prinsip yaitu *Confidentiality, Integrity* dan *Availability*. Pada awalnya prisnip keamanan infomasi hanya CIA, seiring berjalannya waktu prinsip keamanan informasi menjadi CIA’s+ yaitu:

1. *Confidentiality* (Kerahasiaan)

   Adalah prinsip yang menjamin, memastikan dan menjaga kerahasiaan informasi, bahwa informasi hanya dapat diakses dan digunakan oleh orang yang mempunyai wewenang sekaligus menjamin informasi yang dikirim, diterima dan disimpan serta terjamin kerahasiaannya.

2. *Integrity* (Integritas)

   Adalah prinsip yang menjamin informasi tidak dirubah, dimanipulasi, dimodifikasi maupun dihilangkan tanpa izin dari pihak berwenang, serta menjaga keakuratan dan kesempurnaan infotmasi dan prosesnya.

3. *Availability* (Ketersediaan)

   Adalah prinsip yang menjamin bahwa informasi akan tersedia ketika dibutuhkan, serta memastikan pihak yang berwenang dapat menggunakan informasi yang dibutuhkan tanpa ada gangguan dari pihak lain.

4. *Privacy* (Privasi)

   Adalah prinsip yang menjamin bahwa informasi yang dikumpulkan, digunakan, dan disimpan oleh organisasi yang digunakan hanya untuk tujuan tertentu oleh pelmilik informasi pada saat informasi dikumpulkan.

5. *Identification* (Identifikasi)

   Adalah prinsip yang menjamin bahwa informasi memiliki karakteristik identifikasi ketika informasi dapat mengenali penggunanya. Identifikasi adalah langkah pertama dalam memperoleh akses ke informasi yang diamankan, dan berfungsi sebagai dasar untuk otentifikasi dan otorisasi.

6. *Authentification* (Otentifikasi)

Adalah suatu prinsip yang menjamin bahwa saat otentifikasi terjadi ketika sistem dapat membuktikan bahwa pengguna memiliki hak klaim.

7. *Authorization* (Otorisasi)

   Adalah prinsip yang menjamin bahwa pengguna telah mendapatkan otorisasi sehingga dapat mengakses, meng-*update* atau penghapus informasi.

8. *Accountability* (Akuntabilitas)

   Adalah prinsip informasi yang dikatakan eksis ketika sistem dapat menyajikan semua aktifitas terhadap informasi dan siapa yang melakukan aktifitas itu (Whitmann dan Mattord, 2016).

Masing-masing komponen diatas berkontribusi dalam program keamanan informasi secara keseluruhan. Keamanan informasi adalah perlindungan informasi, termasuk system dan perangkat yang digunakan, menyimpan, dan mengirimkannya. Keamanan informasi melindungin informasi dari berbagai ancaman untuk menjamin kelangsungan usaha, meminimalisasi kerusakan akibat terjadinya ancaman, mempercepat kembalinya investasi dan peluang usaha.

2.3 Keamanan Teknologi Informasi

Menurut (Swastika dan Putra, 2016) bahwa aset Teknologi Informasi dinyatakan aman jika kerugian yang diperkirakan akan terjadi akibat ancaman-ancaman dalam jangka waktu tertentu, masih dalam Batasan yang dapat diterima. Ancaman tersebut dapat berupa ancaman:

a. Fisik – ancaman personil, perangkat keras (*mainframe, mini, micro komputer, peripherals, storage, media*), fasilitas, dokumentasi, dan persediaan.
b. *Logical* – mengancam data/informasi dan perangkat lunak (sistem dan aplikasi).

2.4 Audit

Audit memiliki pengertian yaitu proses atau aktivitas yang sistematik, independen dan terdokumentasi untuk menemukan suatu bukti-bukti (audit *evidence*) dan dievaluasi secara obyektif untuk menentukan apakah telah memenuhi kriteria pemeriksaan (audit) yang ditetapkan ICASA (Sarno dan Ifanno, 2009).

Tujuan audit sistem informasi yaitu untuk mengetahui sudah sejauh mana sistem mempertahankan informasi dan integritas data, sudah sejauh mana sistem telah efektif membantu pencapaian organisasi dan sudah sejauh mana optimalisasi penggunaan sumber daya secara optimal (Swastika dan Putra, 2016).

Tujuan lain dengan dilakukannya audit keamanan sistem informasi menurut (Sarno dan Ifanno, 2009) yaitu dapat menjaga aspek kerahasiaan (*Confidentiality*), keutuhan (*Integrity*) dan ketersediaan (*Availability*) dari informasi.

2.5 Audit Internal

Audit internal memiliki peran utama yang bertanggung jawab dalam identifikasi dan investigasi kecurangan. Oleh karena itu, dibutuhkan tim yang memiliki

keahlian cukup mengenai skema skema kecurangan, teknik investigasi, ketentuan perundang-undangan dan hukum yang berlaku, serta pengetahuan dan keahlian lain yang dibutuhkan dalam investigasi. Tenaga staf yang diperlukan dapat diperoleh dari dalam (*in-house*), *outsourcing*, atau kombinasi dari keduanya. Dalam beberapa kasus, audit internal juga dapat menggunakan staf nonaudit dari unit lain di dalam organisasi untuk membantu penugasan. Hal ini sering terjadi bila keahlian yang diperlukan beragam dan tim harus dibentuk dengan segera. Dalam hal organisasi membutuhkan ahli eksternal, perlu menetapkan syarat-syarat yang harus dipenuhi lembaga penyedia sumber daya eksternal terutama dalam hal kompetensi dan ketersediaan sumber daya.

Dalam hal di mana tanggung jawab utama untuk fungsi investigasi tidak ditugaskan kepada aktivitas audit anternal, aktivitas audit internal masih dapat diminta untuk membantu penugasan investigasi dalam mengumpulkan informasi dan membuat rekomendasi untuk perbaikan pengendalian internal.

Menurut (Tugiman, 2011) *Internal auditing* atau pemeriksaan internal adalah suatu fungsi penilaian yang independen dalam suatu organisasi untuk menguji dan mengevaluasi kegiatan organisasi yang dilaksanakan.

2.6 Audit Berbasis Resiko

Semua organisasi memiliki beberapa risiko, potensi kerugian, kerusakan, cedera, atau hasil yang tidak diinginkan lainnya yang diakibatkan oleh keputusan atau tindakan. Munculnya resiko dikarenakan masa depan tidak dapat diprediksi dengan pasti, rencana atau strategi organisasi mengenai kejadian masa depan

mencerminkan asumsi, perhitungan, atau perkiraan tentang apa yang akan terjadi, namun selalu ada kemungkinan bahwa hasil yang didapatkan kurang menguntungkan daripada yang direncanakan organisasi (Gantz, 2014).

Hal yang sebelumnya harus dilakukan auditor sebelum melakukan audit yaitu perlunya memahami aspek-aspek yang harus dilakukan dalam melakukan Audit Berbasis Resiko (ABR). Dalam menerapkan ABR, auditor perlu mengidentifikasi wilayah/area yang Memiliki risiko yang menghambat pencapaian tujuan manajemen. Wilayah/area yang memiliki tingkat risiko yang tinggi tersebut akan memerlukan pengujian yang lebih mendalam. Auditor dapat mengalokasikan sumber daya auditnya berdasarkan hasil identifikasi atas kemungkinan dan dampak terjadinya risiko. Wilayah berisiko rendah menjadi prioritas akhir alokasi sumber daya audit. Oleh karena itu, dalam ABR, auditor harus melakukan analisis dan penaksiran risiko yang dihadapi auditi. Audit dengan pendekatan berbasis risiko banyak dipakai oleh para praktisi audit di dunia. Mereka berpendapat bahwa makin besar suatu perusahaan berkembang maka lebih besar juga risiko yang akan datang. Risiko selalu ada pada tiap proses yang dijalankan karena itu penting sekali pendekatan yang berbasiskan risiko dilakukan, jadi sudah biasa jika misalnya penilaian dan mitigasi risiko dilakukan sebagai bagian integral dari audit (Syafrizal, 2008).

2.7 Karakteristik Audit Teknologi Informasi (TI)

Audit TI memiliki karakteristik yang harus ditekankan kepada setiap auditor. Definisi, standar, metodologi, dan panduan menyepakati karakteristik utama yang terkait dengan audit TI yaitu berasal dari *Generally Accepted Auditing Standards*

(GAAS), standar internasional, dan kode praktik. Karakteristik ini mencakup kebutuhan auditor untuk mengerti jenis-jenis audit yang akan mereka lakukan. Memahami prinsip umum, prosedur, standar, dan tujuan merupakan jenis-jenis audit dan berlaku dalam konteks audit TI. Bergantung pada kompleksitas dan karakteristik khusus dari kontrol TI atau lingkungan operasi yang menjalani audit, auditor mungkin memerlukan pengetahuan atau keahlian khusus untuk dapat memeriksa kontrol yang termasuk dalam lingkup audit TI secara benar dan efektif. Kode etik, praktik, dan perilaku etis adalah kemampuan umum yang diterapkan pada setiap domain audit dengan menekankan prinsip dan tujuan seperti integritas, objektivitas, kompetensi, kerahasiaan, dan kepatuhan terhadap standar dan panduan yang sesuai.

Auditor independence merupakan prinsip yang berlaku untuk audit internal dan eksternal, dengan kata lain auditor adalah individu yang melakukan audit dapat membuktikan bahwa organisasi yang mereka wakili tidak memiliki kepentingan finansial dan bebas dari benturan kepentingan mengenai organisasi yang mereka audit sehingga tetap objektif serta tidak memihak. *Auditor independence* diamanatkan dalam *Sarbanes-Oxley Act* dan diberlakukan oleh *Securities and Exchange Commission* (SEC) secara legal memerlukan independensi untuk audit perusahaan publik (Gantz, 2014).

2.8 Sertifikasi Audit

Audit sertifikasi adalah evaluasi formal terhadap satu atau lebih aspek kemampuan operasional organisasi terhadap persyaratan eksplisit yang terkait dengan standar atau metodologi yang ditetapkan secara eksternal. Pencapaian sertifikasi

memberikan dukungan eksternal bahwa sebuah organisasi memenuhi kriteria yang ditentukan untuk standar tertentu. Berhasil mencapai sertifikasi bukanlah indikasi bahwa sebuah organisasi berkinerja secara optimal atau dengan cara yang lebih unggul dari organisasi lain. Sebagai gantinya, sertifikasi merupakan bentuk jaminan independen bahwa sebuah organisasi memenuhi setidaknya seperangkat persyaratan minimum (Gantz, 2014).

Menurut (Gantz, 2014) terdapat beberapa tipe sertifikasi dan standar dalam audit, diantaranya adalah sebagai berikut :

Tabel 2. Macam-macam sertifikasi dan standar

Fokus Sertifikasi	**Serifikasi**
Quality Management	ISO 9001
	ISO 14001
Information Security Management	ISO/IEC 27001
	Cybertrust
Service management	CMII *for Services*
	ISO/IEC 20000
Service organization controls	SSAE 16
	ISAE 3402
	SOC 2 *and* 3
Process improvement	CMMI
	ISO/IEC 15504
	Six Sigma
Products or technologies	*Common criteria*
	CESG *assisted products scheme* (United Kingdom)
	FIPS (United States)

2.9 ISO/IEC 27000 *Series*

International Organization for Standardization (ISO) dan *International Electrotechnical Commission* (IEC) bersama-sama menerbitkan seperangkat standar yang menggambarkan *Information Security Management System* (ISMS) organisasi dan kontrol keamanan yang dimiliki oleh sebuah sistem. Dalam konteks ISMS, kata sistem menunjukkan serangkaian proses dan aktivitas eksplisit, standar, dan berulang untuk pengelolaan keamanan. ISO seri 27000 awalnya dibuat pada tahun 1995 sebagai British Standard 17799, kerangka kerja ini direvisi pada tahun 1998 dan diadopsi oleh *International Standar Organisation* pada tahun 1999 sebagai ISO 17799. Setelah kembali direvisi secara signifikan pada tahun 2005, standar 17799 diubah secara resmi menjadi dua standar ISO/IEC yang terkait, yaitu 27001 dan 27002. Kemudian standar ini menjadi landasan pengelolaan keamanan informasi yang lebih luas yang dikenal sebagai seri 27000. ISO/IEC 27001 menentukan persyaratan untuk sistem manajemen keamanan informasi, sementara ISO/IEC 27002 menyediakan kerangka kontrol keamanan (ISO/IEC 27001:2013, 2017).

ISO / IEC 27002 menentukan hirarki kontrol keamanan yang terdiri dari 11 klausul keamanan utama, 39 kategori keamanan, dan 133 kontrol keamanan yang berbeda. Sedangkan ISO/IEC 27007 memberikan panduan untuk auditor yang mengevaluasi ISMS dari organisasi berdasarkan ISO/IEC 27001. ISO menerbitkan dua standar yang terpisah namun secara substansial serupa mengenai manajemen risiko, yaitu ISO/IEC 27005, yang secara eksplisit menangani manajemen risiko keamanan informasi (Gantz, 2014).

ISO mengelompokkan semua standar keamanan informasi ke dalam satu struktur penomoran, seperti pada serial ISO 27000. Adapun daftar standar di seri ISO 27000 ini adalah sebagai berikut:

Tabel 3. Standar Seri ISO 27000

ISO 27000 *Serials*	***Standarization***
ISO/IEC 27000	*Information security management systems* (o*verview and vocabulary*).
ISO/IEC 27001	*Information technology, Security Techniques,* dan *Information security management systems* (ISMS).
ISO/IEC 27002	*Code of practice for information security management.*
ISO/IEC 27003	*Information security management system implementation guidance.*
ISO/IEC 27004	*Information security management* (*Monitoring, measurement, analysis and evaluation*).
ISO/IEC 27005	*Information security risk management.*
ISO/IEC 27006	*Requirements for bodies providing audit and certification of information security management systems.*
ISO/IEC 27007	*Guidelines for information security management systems auditing (focused on auditing the management system).*
ISO/IEC TR 27008	*Guidance for auditors on ISMS controls (focused on auditing the information security controls).*
ISO/IEC 27009	*Essentially an internal document for the committee developing sector/industry-specific variants or implementation guidelines for the* ISO27k *standards.*
ISO/IEC 27010	*Information security management for inter-sector and inter-organizational communications.*
ISO/IEC 27011	*Information security management guidelines for telecommunications organizations based on* ISO/IEC 27002.

Tabel 3. Standar Seri ISO 27000 (Lanjutan)

ISO 27000 *Serials*	***Standarization***
ISO/IEC 27013	*Guideline on the integrated implementation of* ISO/IEC 27001 *and* ISO/IEC 20000-1 *(derived from ITIL).*
ISO/IEC 27014	*Information security governance.*
ISO/IEC TR 27015	*Information security management guidelines for financial services.*
ISO/IEC TR 27016	*Information security economics.*
ISO/IEC 27017	*Code of practice for information security controls based on* ISO/IEC 27002 *for cloud services.*
ISO/IEC 27018	*Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.*
ISO/IEC TR 27019	*Information security for process control in the energy industry.*
ISO/IEC 27031	*Guidelines for information and communication technology readiness for business continuity*
ISO/IEC 27032	*Guideline for cybersecurity*
ISO/IEC 27033-1	*Network security - Part 1: Overview and concepts*
ISO/IEC 27033-2	*Network security - Part 2: Guidelines for the design and implementation of network security.*
ISO/IEC 27033-3	*Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues.*
ISO/IEC 27033-4	*Network security - Part 4: Securing communications between networks using security gateways.*
ISO/IEC 27033-5	*Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs).*

Tabel 3. Standar Seri ISO 27000 (Lanjutan)

ISO 27000 *Serials*	***Standarization***
ISO/IEC 27033-6	*Network security - Part 6: Securing wireless IP network access.*
ISO/IEC 27034-1	*Application security - Part 1: Guideline for application security*
ISO/IEC 27034-2	*Application security - Part 2: Organization normative framework.*
ISO/IEC 27034-6	*Application security - Part 6: Case studies.*
ISO/IEC 27035-1	*Information security incident management - Part 1: Principles of incident management*
ISO/IEC 27035-2	*Information security incident management - Part 2: Guidelines to plan and prepare for incident response.*
ISO/IEC 27036-1	*Information security for supplier relationships - Part 1: Overview and concepts.*
ISO/IEC 27036-2	*Information security for supplier relationships - Part 2: Requirements.*
ISO/IEC 27036-4	*Information security for supplier relationships - Part 4: Guidelines for security of cloud services.*
ISO/IEC 27037	*Guidelines for identification, collection, acquisition and preservation of digital evidence.*
ISO/IEC 27038	*Document redaction*
ISO/IEC 27039	*Intrusion prevention*
ISO/IEC 27040	*Storage security*
ISO/IEC 27041	*Investigation assurance*
ISO/IEC 27042	*Analyzing digital evidence*
ISO/IEC 27043	*Incident investigation*
ISO/IEC 27050-1	*Electronic discovery - Part 1: Overview and concepts.*

Tabel 3. Standar Seri ISO 27000 (Lanjutan)

ISO 27000 *Serials*	***Standarization***
ISO 27799	*Information security management in health using* ISO/IEC 27002 (*guides health industry organizations on how to protect personal health information using* ISO/IEC 27002).

2.10 ISO/IEC 27001

ISO 27001 adalah standar yang menjelaskan bagaimana mengelola keamanan informasi dalam suatu organisasi. Standar ini terdiri dari 10 klausul dan 114 kontrol keamanan generik yang dikelompokkan menjadi 14 bagian (*Annex* A), dengan tujuan membantu organisasi untuk mendefinisikan, menerapkan, mengoperasikan, mengendalikan, dan meningkatkan keamanan informasi berdasarkan pendekatan manajemen risiko.

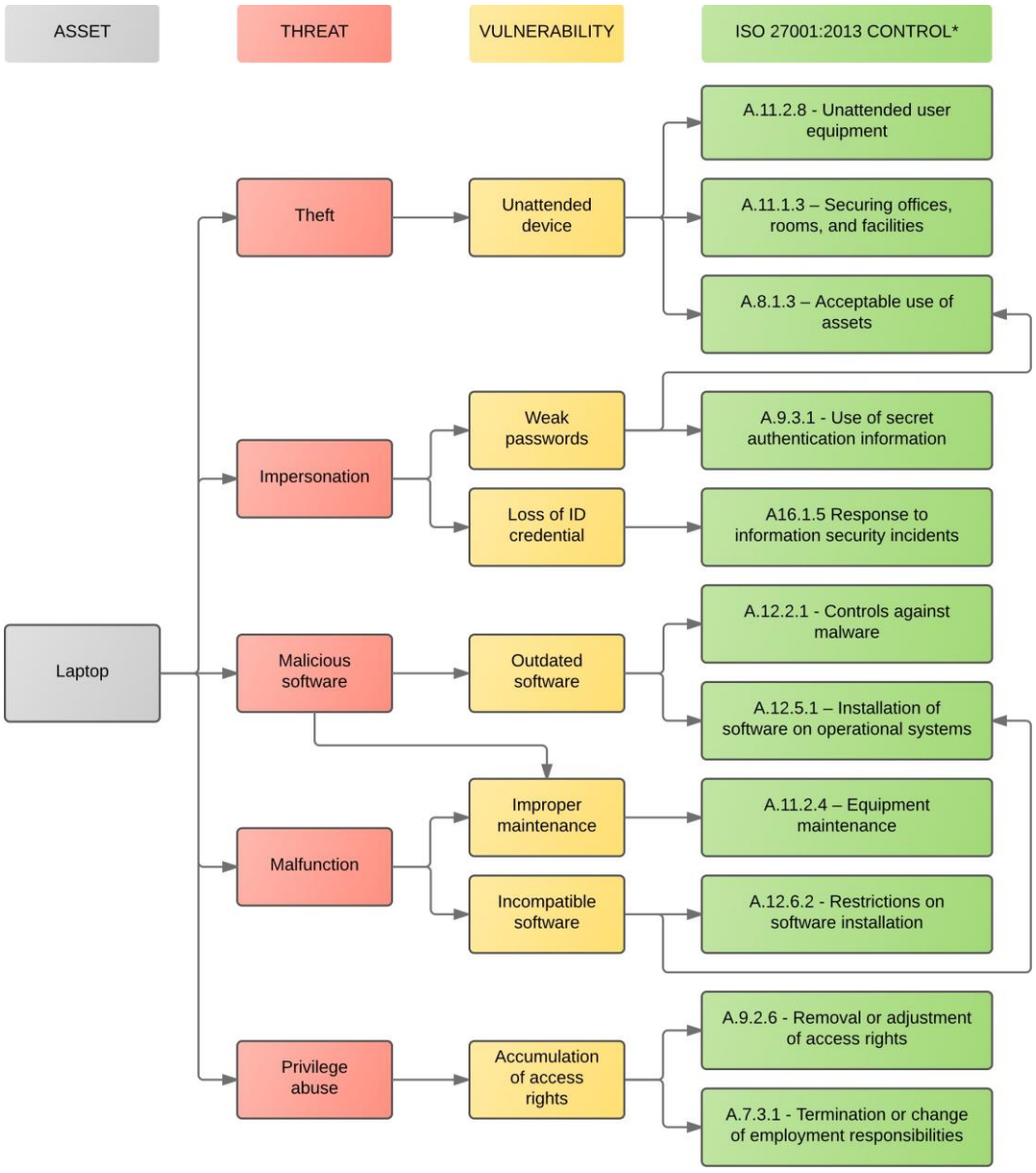
ISO 27001: 2013 *Annex* A mencakup kontrol yang terkait dengan struktur organisasi (fisik dan logis), sumber daya manusia, teknologi informasi, dan manajemen pemasok dan lainnya. Pengadopsiannya direkomendasikan untuk organisasi yang informasinya merupakan salah satu aset bisnis yang paling penting, atau perusahaan yang bisnis utamanya terkait langsung dengan informasi (misalnya, organisasi penelitian dan pengembangan, pengolah kartu kredit, bank, penyedia konten, jaringan sosial, dll).

Seperti standar pengelolaan ISO lainnya (misalnya, ISO 9001 untuk manajemen mutu, dan ISO 14001 untuk pengelolaan lingkungan), ISO 27001 dirancang agar sesuai dengan organisasi dari berbagai ukuran dan industri. Demikian pula, ISO

27001 juga tidak menawarkan rincian tentang bagaimana penerapannya, hanya persyaratan yang harus dipenuhi. Untuk membantu implementasi, ISO telah merilis beberapa standar dalam rangkaian ISO 27000, seperti ISO 27002 (pedoman untuk semua kontrol), ISO 27017 (panduan untuk keamanan informasi pada *cloud environments*), dan ISO 27031 (pedoman untuk kesiapan teknologi informasi untuk kelangsungan bisnis).

Dengan menerapkan ISO 27001, sebuah organisasi dapat mengurangi risiko yang berkaitan dengan kerahasiaan, ketersediaan, dan integritas informasi; mencapai kepatuhan terhadap hukum, peraturan, dan kontrak yang menuntut perlindungan informasi sensitif; mengurangi biaya bisnis karena adanya suatu insiden; dan sistem yang telah diakui karena telah memenuhi standar yang telah ditetapkan secara internasional (ISO 27001 Academy, 2017).

Menurut (Ikhsan *et al*, 2009) 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 menyatakan persyaratan utama yang harus dipenuhi menyangkut Sistem manajemen keamanan informasi (kerangka kerja, proses dan dokumentasi), Tanggung jawab manajemen, Audit internal SMKI, Manajemen tinjau ulang SMKI dan Peningkatan berkelanjutan.



Gambar 1. *Risk Management and Treatment Process* ISO 27001
(Sumber: ISO 27001, 2017)

2.11 *Maturity Level*

Maturity model adalah suatu model yang digunakan untuk menilai kematangan semua proses berdasarkan masing-masing tingkatan. Kerangka ini berfungsi

sebagai alat penilaian yang memungkinkan organisasi memahami dan meningkatkan kemampuan TI mereka dalam enam tingkat kematangan, yaitu tidak ada (*non-existent*), permulaan dasar (*initial*), dasar perencanaan (*basic*), menengah (*intermediate*), lanjutan (*advanced*), dan optimalisasi (*optimizing*). Area yang menjadi focus utama yaitu gambaran tingkat kematangan dengan skor penggambungan yang dapat menjadi tolak ukur dalam penilaian kematangan. Penilaian kematangan ini didapatkan berdasarkan hasil penilaian survei dan wawancara dengan pemangku kepentingan di dalam organisasi (Carcary, 2012).

Tabel 4. Contoh penilaian *maturity level*.

Maturity Level	***Practice***
5	Telah mengimplementasikan kebijakan resiko dengan baik, telah diperluas, melakukan review secara berkala, perencanaan yang terdefinisi dengan baik, serta adanya pembaharuan yang terdokumentasi.
4	Mengembangkan kebijakan dengan peninjauan secara teratur melalui proses kerjasama dengan pihak ketiga.
3	Menerapkan kebijakan *Risk Management* yang terperinci serta adanya penyelarasan yang berkaitan dengan strategi perusahaan.
2	Membangun prosedur yang telah diikuti oleh setiap pemangku kepentingan. Tidak ada pelatihan dan komunikasi dari prosedur-prosedur tersebut.
1	Membangun kebijakan manajemen resiko awal dan dilakukan penilaian terhadapnya sesuai kebutuhan.
0	Tidak ada praktik formal pada *level* ini.

Menurut (Sarno dan Ifanno, 2009) dalam hubungannya dengan SMKI, resiko adalah dampak yang ditimbulkan atas terjadinya sesuatu yang mengancam keamanan informasi di organisasi, yang dimaksud adalah ancaman terhadap aspek

keamanan informasi yaitu CIA (*Confidentiality, Integrity, Availability*). Sehingga setiap pernyataan akan diberikan bobot yang sesuai dengan nilai resiko yang akan terjadi apabila tidak diterapkan. Bobot yang dihasilkan dari penilaian indeks kematangan kemudian akan dipetakan menjadi beberapa *level* dengan skala pembulatan masing-masing. Berikut ini adalah skala pembulatan dari indeks maturity:

Tabel 5. Skala Pembulatan Indeks

Maturity Indeks	***Maturity Level***
4.51 – 5.00	5 – Dioptimalisasi (*Optimised*)
3.51 – 4.50	4 – Diatur (*Managed and Measurable*)
2.51 – 3.50	3 – Ditetapkan (*Defined*)
1.51 – 2.50	2 – Dapat diulang (*Repeatable but Intuitive*)
0.51 – 1.50	1 – Inisialisasi (*Initial/Ad Hoc*)
0.00 – 0.50	0 – Tidak ada (*Non-Existent*)

BAB III

METODOLOGI PENELITIAN

3.1 Waktu dan Tempat

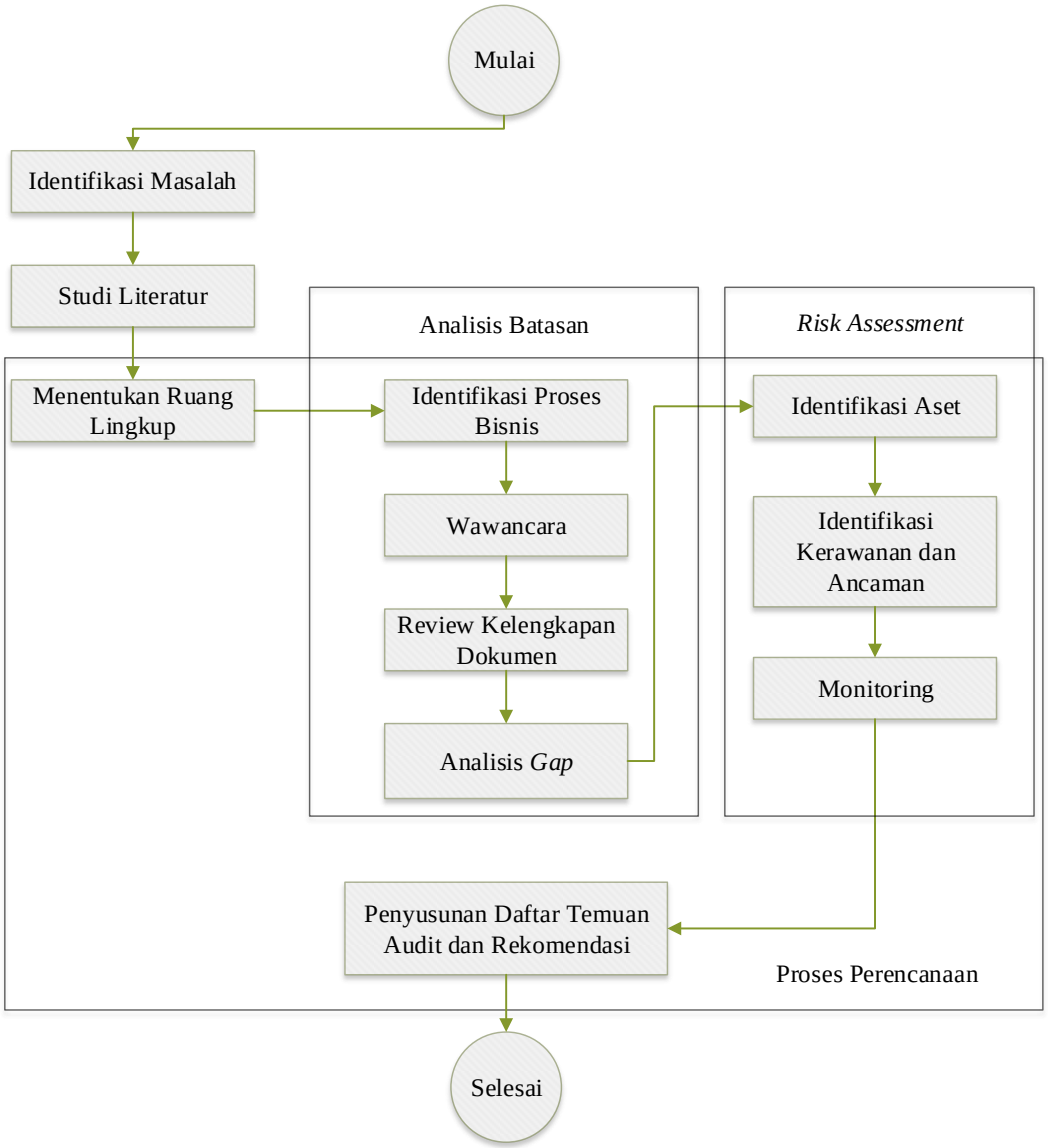
Penelitian ini dilakukan di Universitas Lampung pada bagian divisi infrastruktur dan divisi pengelola siakad Unit Pelaksana Teknis (UPT) Teknologi dan Komunikasi Universitas Lampung. Penelitian ini dimulai pada tanggal 01 Januari 2018 sampai 31 Maret 2018.

3.2 Data

Data yang digunakan dalam penelitian ini berupa informasi mengenai kepatuhan dalam pelaksanaan keamanan pada sistem informasi akademik. Data tersebut berupa hasil observasi, pengisian kuisioner, dan wawancara di beberapa unit kerja yang mengelola pelaksanaan Siakad, diantaranya BAK dan UPT TIK Universitas Lampung. Pengambilan data dilakukan terpusat yaitu pada UPT TIK Universitas Lampung sebagai penyedia *hardware* dan kelola aset.

3.3 Metode Penelitian

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



Gambar 2. Metodologi Penelitian

3.1.1 Identifikasi Masalah

Langkah awal dalam penelitian ini adalah identifikasi masalah. Masalah yang dihadapi yaitu keamanan sistem informasi, dimana keamanan sangat dibutuhkan oleh organisasi sehingga diperlukan suatu audit keamanan menggunakan *framework* tertentu. Pada penelitian ini, *framework* yang digunakan dalam Audit Keamanan Sistem Informasi Akademik Universitas Lampung adalah ISO/IEC 27001:2013 yaitu mengenai *Information Security Management System* (ISMS).

3.1.2 Studi Literatur

Setelah memilih masalah dan metode yang digunakan dalam penyelesaian masalah. Studi literatur didapatkan dari berbagai teori yang berhubungan dengan topik penelitian antara lain jurnal, buku, *web*, dan standar-standar *checklist* yang dijadikan acuan dalam penelitian ini, serta dokumen-dokumen organisasi seperti kebijakan dan prosedur keamanan informasi.

3.1.3 Menentukan Ruang Lingkup dan Tujuan Audit

Ruang lingkup dari penelitian ini adalah Sistem Informasi Akademik Universitas Lampung. Penelitian ini bertujuan untuk mengetahui kepatuhan organisasi terhadap prosedur yang terdapat pada *checklist* ISO 27001:2013. Ruang lingkup audit keamanan sistem informasi ini tidak hanya pada sistem informasi yang ada pada organisasi, tetapi berdasarkan manajemen keamanan dalam mendeteksi kelemahan dalam informasi yang kemungkinan berasal dari faktor di luar sistem atau manajemen proses bisnis yang kurang baik.

3.1.4 Identifikasi Proses Bisnis TI

Pada tahapan perencanaan audit, proses pertama yang dilakukan adalah melakukan pemahaman proses bisnis dan TI perusahaan yang diaudit (*auditee*). Pemahaman dilakukan dengan cara mempelajari dokumen-dokumen yang terkait dengan perusahaan. Dokumen tersebut berupa profil perusahaan, *standard operating procedure*, kebijakan, standar, prosedur, portopolio, arsitektur, infrastruktur, dan aplikasi sistem informasi. Langkah selanjutnya adalah mencari informasi apakah sebelumnya perusahaan telah melaksanakan proses audit. Apabila pernah dilakukan audit, maka auditor perlu mengetahui dan memeriksa laporan audit sebelum itu.

Dalam menggali pengetahuan mengenai *auditee*, langkah yang harus dilakukan adalah memeriksa dokumen-dokumen yang terkait dalam proses audit, wawancara manajemen dan *staff*, serta melakukan observasi terkait kegiatan operasional dan teknologi sistem informasi yang digunakan. Keluaran yang dihasilkan dari proses ini adalah berupa profil perusahaan, visi, misi perusahaan, struktur organisasi, serta gambaran umum teknologi informasi.

3.1.5 Observasi dan Wawancara

Observasi dimulai dengan mengidentifikasi dan membuat pemetaan sehingga didapatkan gambaran umum tentang sasaran penelitian. Pada penelitian ini dilakukan observasi mengenai kondisi *existing* pengelolaan keamanan bagi sistem. Sehingga nantinya hasil observasi digunakan dalam penentuan kontrol objektif yang sesuai.

Wawancara merupakan metode yang dapat dilakukan untuk mendapatkan data *primer*. Untuk tahapan audit, data yang didapatkan berasal dari hasil wawancara responden yang dikumpulkan untuk kelengkapan temuan audit.

Adapun bagian-bagian dalam civitas Universitas Lampung yang bertanggungjawab dalam pengelolaan Sistem Informasi Akademik berdasarkan domain ISO 27001:2013 adalah sebagai berikut:

Tabel 6. Bagian Pengelola Siakad Universitas Lampung

Domain ISO 27001	**Pengelola**
A.5 *Information Security Policies*	BAK
	UPT TIK
A.6 *Organization of information security*	WR I (Bidang Akademik)
	WR II (Bidang Administrasi Umum dan Keuangan)
	WR IV (Bidang Perencanaan, Kerja sama, dan Teknologi Informasi dan Komunikasi)
	BAK
	UPT TIK
A.7 *Human resource security*	WR II (Bidang Administrasi Umum dan Keuangan)
	UPT TIK
	BAK
A.8 *Asset management*	WR IV (Bidang Perencanaan, Kerja sama, dan Teknologi Informasi dan Komunikasi)
	WR II (Bidang Administrasi Umum dan Keuangan)
	UPT TIK
A.9 *Acces Control*	UPT TIK
A.10 *Cryptography*	UPT TIK
A.11 *Physical and environmental security*	WR II (Bidang Administrasi Umum dan Keuangan)

Tabel 7. Bagian Pengelola Siakad Universitas Lampung (Lanjutan)

Domain ISO 27001	**Pengelola**
	UPT TIK
A.12 *Operations Security*	UPT TIK
A.13 *Communication security*	WR IV (Bidang Perencanaan, Kerja sama, dan Teknologi Informasi dan Komunikasi)
	UPT TIK
A.14 *System acquisition, development and maintenance*	UPT TIK
A.15 *Supplier relationships*	WR II (Bidang Administrasi Umum dan Keuangan)
	UPT TIK
A.16 *Information security incident management*	BAK
	UPT TIK
A.17 *Information security aspects of business continuity management*	WR IV (Bidang Perencanaan, Kerja sama, dan Teknologi Informasi dan Komunikasi)
	BAK
	UPT TIK
A.18 *Compliance*	WR IV (Bidang Perencanaan, Kerja sama, dan Teknologi Informasi dan Komunikasi)
	BAK
	UPT TIK

3.1.6 Review Kelengkapan Dokumen

Kegiatan ini berfokus pada melakukan pemeriksaan mengenai kelengkapan dokumen-dokumen terkait kebijakan, prosedur, instruksi, serta dokumentasi mengenai keamanan informasi. Review kelengkapan akan memberikan gambaran mengenai kebijakan/prosedur/instruksi/dokumentasi yang sudah diterapkan dan daftar rekomendasi penerapan kebijakan berdasarkan standar keamanan informasi.

3.1.7 Analisis *Gap*

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 kontrol objektif yang berasal dari *Assessment Checklist Annex* A: 2013. Tujuan dari penilaian *gap* adalah memeriksa sudah sejauh apa kontrol-kontrol ISO 27001 diterapkan dan diimplementasikan dengan baik terhadap pihak terkait. Berikut ini adalah penilaian *gap* pada klausul ISO 27001:

Tabel 7. Penilaian *Gap* ISO 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).

3.1.8 *Risk Assessment*

Setelah melakukan gap analisis, dilakukan *risk assessment* yang bertujuan untuk melakukan penilaian resiko yang mungkin timbul dari tahap sebelum itu. Resiko tersebut muncul dan berkemungkinan untuk mengancam keamanan informasi dan pengelolaannya. Dalam *risk assessment*, akan dilakukan identifikasi aset, identifikasi kerawanan dan ancaman, menentukan prioritas resiko yang akan

dikendalikan, menentukan kontrol apa saja yang dapat dilakukan untuk mengendalikan resiko, dan mengawasi resiko.

Adapun analisis yang akan dilakukan mengacu pada ISO 27001 berisi identifikasi kelengkapan aset, ketersediaan informasi yang digunakan apakah telah sesuai dengan permintaan lembaga yang berwenang, kerahasiaan menyangkut apakah informasi dapat diproses oleh pihak yang tidak berwenang, keamanan informasi mengenai kerahasiaan, integritas dan ketersediaan informasi, pelanggaran terhadap kebijakan keamanan informasi, adanya serangkaian kejadian keamanan informasi yang tidak diinginkan. Selain itu, dilakukan analisis ISMS (mencakup struktur, kebijakan, kegiatan perencanaan, tanggung jawab, praktek, prosedur, proses dan sumber daya organisasi), integritas, resiko *residu*, keputusan dalam menerima resiko, analisis resiko, *risk assessment*, evaluasi resiko, manajemen resiko, perlakuan resiko, dan pernyataan pemberlakuan yang terdokumentasi.

3.1.9 Menetapkan Kontrol

Proses selanjutnya yang akan dilakukan yaitu menentukan kontrol. Kontrol yang dipilih berdasarkan kontrol objektif dari ISO/IEC 27001. Kontrol ini didapatkan berdasarkan hasil identifikasi kerawanan dan ancaman sehingga didapatkan rekomendasi yang akan menutupi celah-celah keamanan informasi yang ada.

Terdapat 14 domain dan 34 kontrol objektif didalam standarisasi ISO 27001:2013 berdasarkan lampiran A (*Annex* A), adapun domain dan kontrol objektif tersebut adalah sebagai berikut:

Tabel 8. Domain dan Kontrol Objektif ISO 27001

No.	Domain ISO 27001	Kontrol Objektif ISO 27001
A.5	*Information Security Policies*	A.5.1 *Manajemen direction for information security*
A.6	*Organization of information security*	A.6.1 *Internal organization*
		A.6.2 *Mobile device and Teleworking*
A.7	*Human resource security*	A.7.1 *Screening*
		A.7.2 *During employment*
		A.7.3 *Termination and change of employment*
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.10	*Cryptography*	A.10.1 *Criptographic controls*
A.11	*Physical and environmental security*	A.11.1 *Secure areas*
		A.11.2 *Equipment*
A.12	*Operations Security*	A.12.1 *Operational procedures and responsibilities*
		A.12.2 *Protection from malware*
		A.12.3 *Backup*
		A.12.4 *Logging and monitoring*
		A.12.5 *Control of operational software*
		A.12.6 *Technical vulnerability management*
		A.12.7 *Information systems audit considerations*
A.13	*Communication security*	A.13.1 *Network secutiry management*
		A.13.2 *Information transfer*
A.14	*System acquisition, development and maintenance*	A.14.1 *Security reqirements of information system*

Tabel 9. Domain dan Kontrol Objektif ISO 27001 (Lanjutan)

No.	Domain ISO 27001	Kontrol Objektif ISO 27001
		A.14.2 *Security in development and support processes*
		A.14.3 *Test data*
A.15	*Supplier relationships*	A.15.1 *Information security in supplier relationship*
		A.15.2 *Supplier service delivery management*
A.16	*Information security incident management*	A.16.1 *Management of information security incidents and improvement*
A.17	*Information security aspects of business continuity management*	A.17.1 *Information security continuity*
A.18	*Compiliance*	A.18.1 *Compiliance with legal and contractual requirements*
		A.18.2 *Information security reviews*

(Sumber: ISO 27001:2013 *Checklist*)

3.1.10 Melakukan Dokumentasi (Data dan Bukti)

Setelah menetapkan kontrol objektif atas dasar identifikasi ancaman (*threats*) serta dampak yang terjadi. Selanjutnya dibuat kebijakan, prosedur, instruksi, dokumentasi dan rekomendasi berdasarkan subkontrol yang terdapat dalam ISO/IEC 27001:2013 *checklist*. Pada langkah ini dilakukan penyususunan dokumen berupa data maupun bukti-bukti atas temuan atau fakta yang ada.

3.1.11 Penyusunan Daftar Temuan dan Rekomendasi

Pada proses temuan dan rekomendasi yang dilakukan adalah memeriksa data profil, kebijakan, standar, prosedur, dan portofolio, mengobservasi *standar operating procedure* serta melakukan wawancara. Seluruh proses tersebut menghasilkan

bukti (data temuan audit) yang terkait dengan sistem yang sedang berlangsung, selain itu analisa sebab dan akibat temuan, serta rekomendasi untuk organisasi agar melakukan penetapan kontrol keamanan yang lebih baik dan sesuai dengan standar ISO 27001.

3.2 *Audit Working Plan*

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 Univeristas Lampung:

Tabel 9. *Audit Working Plan*

No.	Kegiatan	Bulan																			
		Desember				Januari				Februari				Maret				April			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	Studi Literatur																				
2	Penentuan Ruang Lingkup																				
3	Identifikasi Proses Bisnis TI																				
4	Observasi dan Wawancara																				
5	*Review* Kelengkapan Dokumen																				
6	Analisis *Gap*																				
7	*Risk Assessment*																				
8	Identifikasi Aset																				
9	Identifikasi Kerawanan																				

	dan Ancaman																				

Tabel 9. *Audit Working Plan* (Lanjutan)

No.	Kegiatan	Bulan																			
		Desember				Januari				Februari				Maret				April			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
10	Menetapkan Kontrol																				
11	Penyusunan daftar Temuan																				
12	Analisis Rekomendasi																				
13	Penyusunan Laporan Akhir																				

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berikut ini adalah kesimpulan yang didapat berdasarkan hasil penelitian yang telah dilakukan, yaitu:

1. Dari gap analisis yang ada, dapat disimpulkan bahwa Sistem Informasi Akademik (Siakad) Universitas lampung belum memenuhi standar keamanan ISO 27001. Saat ini sistem memiliki indeks penilaian sebesar 2.90. Jika indeks dibulatkan ke dalam penilaian maturity, keamanan Siakad Universitas Lampung berada pada *level* 3 (*defined*) sesuai standar ISO/IEC 27001:2013.
2. Kebijakan, prosedur, instruksi, dan dokumentasi yang telah diterapkan dalam pelaksanaan manajemen siakad saat ini belum memenuhi aspek keamanan informasi. Siakad Universitas Lampung menerapkan 8 kebijakan/prosedur diantara 32 kebijakan/prosedur yang seharusnya diterapkan.
3. Rekomendasi yang diberikan dapat meningkatkan keamanan sistem. Terdapat 9 pengelompokkan rekomendasi pengendalian keamanan aset berdasarkan domain yang ada dan 12 kelengkapan kebijakan keamanan sesuai standar ISO 27001.

5.2 Saran

Berdasarkan hasil penelitian, berikut ini adalah saran yang dapat dilakukan untuk penelitian selanjutnya:

1. Penelitian saat ini berfokus pada kepatuhan penerapan keamanan Siakad Universitas Lampung, namun tidak melakukan audit pemeriksaan dokumen terkait. Sehingga diharapkan untuk penelitian kedepannya dapat dilakukan audit kelayakan dokumen Siakad sesuai standar keamanan sistem informasi.
2. Diharapkan untuk penelitian berikutnya dapat melakukan pengukuran terhadap ketercapaian sasaran keamanan informasi yang mencakup metode pengukuran, frekuensi pengukuran, dan hasil pengukuran.

DAFTAR PUSTAKA

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

Ciptaningrum, D., Nugroho, E., dan Adhipta, D. 2015. Audit Keamanan Sistem Informasi Pada Kantor Pemerintah Kota Yogyakarta Menggunakan Cobit 5. *Sentika*, *2015*(Sentika), 6.

Fine, E., Haryanto, T., dan Adrian, M. I. (2012). Audit Keamanan Sistem Informasi Berdasarkan Standar Iso 27001 Pada Pt. Bpr Jatim. *Stikom*, 1–8. Retrieved from http://jurnal.stikom.edu/indeks.php/jsika/article/viewFile/77/71

Gantz, S. D. 2014. The Basics of IT Audit. *The Basics of IT Audit*. https://doi.org/10.1016/B978-0-12-417159-6.00005-5

Gehrmann, M. 2012. *Combining* ITIL, COBIT *and* ISO / IEC 27002 *for structuring comprehensive information technology for management in organizations. Navus - Revista de Gestao e Tecnologia.*, *2*, 66–77. https://doi.org/10.1109/AMS.2008.145

Hidayat, M. N. 2011. Kajian tata kelola keamanan informasi berdasarkan i*nformationc security management system* (ISMS) ISO 27001:2005 untuk outsourching teknologi informasi pada PT.Kereta Api Indonesia (Persero), (Program Studi Magister Teknologi Informasi Fasilkom UI).

Hsu, C., Wang, T., dan Lu, A. 2016. *The impact of ISO 27001 certification on firm* performance. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2016–March*, 4842–4848. https://doi.org/10.1109/HICSS.2016.600

IAS. 2013. ISO 27001 : 2013 *Compliance Checklist* Iso 27001 : 2013 *Compliance Checklist*.

Ikhsan, M., Darwiyanto, E., Dwi, D., dan Suwawi, J. (2016). *Security Audit of Academic Information System Bandung College of Pharmacy Based on Risk Using Standard* ISO 27001, *3*(3), 5221–5229.

ISO/IEC 27001:2013. 2017. ISN.

ISO 27001 Academy. 2017. *How to integrate* ISO 27001 , COBIT *and* NIST. *Advisera Expert*, 1–14.

Kominfo. 2017. Panduan Penerapan SMKI. Jakarta: Kementrian Informasi dan Komunikasi.

McLeod, R., dan Schell, G. P. 2007. *Sistem Informasi Manajemen* (13th ed.). Jakarta: Salemba Empat.

Mufadhol. 2009. Kerahasiaan dan Keutuhan Keamanan Data dalam Menjaga Integritas dan Keberadaan Informasi Data (Vol. 6). Jurnal Transformatika.

Ruslam, R. Z. 2013. Audit Kepatuhan Keamanan Informasi Dengan Menggunakan Framework ISO 27001/ISMS Pada PT.XYZ.

Sarno, R., dan Ifanno, I. (2009). *Sistem Manajemen Keamanan Informasi*. Surabaya: IT Press.

Swastika, I. P. A., dan Putra, I. G. L. A. 2016. *Audit Sistem Informasi dan Tata Kelola Informasi*. Yogyakarta: Penerbit Andi.

Syafrizal, M. 2007. ISO 17799: Standar Sistem Manajemen Keamanan Sistem Informasi, Seminar Nasional Teknologi 2007 (STN 2007).

Syafrizal, M. 2008. *Information Security Management System (ISMS) Menggunakan Standar* ISO/IEC 27001:2005.

Tugiman, H. 2011. *Pandangan Baru Internal Auditing*. Yogyakarta: Kanisius.

Whitmann, M. E., dan Mattord, H. J. 2016. *Manajemen of Information Sequrity* (5th ed.). Boston: Course Technology.

Windirya, D. R. 2005. Audit Keamanan Sistem Informasi pada Instalasi Sistem Informasi Manajemen RSUD Bangil Berdasarkan ISO 27002, 1–8.

Zuhrawaty. 2009. *Sistem Manajemen Mutu Berdasarkan Prasyarat ISO 19011:2002*. Jogyakarta: Med Press.