

**AUDIT KEAMANAN SISTEM INFORMASI DI DINAS KOMUNIKASI
DAN INFORMATIKA PROVINSI LAMPUNG MENGGUNAKAN
STANDAR ISO/IEC 27001:2013**

(Skripsi)

**Oleh:
ANNISA MEYLIANA**



**FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMPUNG
BANDAR LAMPUNG
2019**

ABSTRACT

AUDIT KEAMANAN SISTEM INFORMASI DI DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI LAMPUNG MENGGUNAKAN STANDAR *ISO/IEC 27001:2013*

By

ANNISA MEYLIANA

Audit of Information security system in the Communication and Information department is needed to determine the extent of information system carried out. This reasearch uses the ISO/ IEC 27001: 2013. Data from this reasearch were obtained based on the result of interview, observation and questionnaire. The respondent conducted a self assessment, then the researcher observe. The results of this study indicate that the average maturity level of the respondent is at level 2 (repeatable) with a value of 2.13 and the average maturity level of the finding is level 2 (repeatable) with a value of 2.40. The difference between the respondent value and the value of the finding show in the sub domain of information security incident management. This difference occurs due to the absence of existing standard operating procedure and criteria. So overall, there is no policy for testing security in developing a system.

Keyword: Audit Keamanan, ISO 270012013, Maturity level

ABSTRAK
**AUDIT KEAMANAN SISTEM INFORMASI DI DINAS KOMUNIKASI
DAN INFORMATIKA PROVINSI LAMPUNG MENGGUNAKAN
STANDAR *ISO/IEC 27001:2013***

Oleh
ANNISA MEYLIANA

Audit sistem keamanan informasi di departemen Komunikasi dan Informasi diperlukan untuk menentukan sejauh mana sistem informasi dilakukan. Penelitian ini menggunakan *ISO/IEC 27001:2013*. Data dari penelitian ini diperoleh berdasarkan hasil wawancara, observasi dan kuesioner. Responden melakukan penilaian sendiri, kemudian peneliti mengamati. Hasil penelitian ini menunjukkan bahwa tingkat kematangan rata-rata responden berada pada level 2 (berulang) dengan nilai 2,13 dan tingkat kematangan rata-rata temuan adalah level 2 (berulang) dengan nilai 2,40. Perbedaan antara nilai responden dan nilai temuan ditunjukkan dalam sub domain manajemen insiden keamanan informasi. Perbedaan ini terjadi karena tidak adanya prosedur operasi standar dan kriteria yang ada. Jadi secara keseluruhan, belum ada kebijakan untuk pengujian keamanan dalam mengembangkan suatu sistem.

Kata Kunci: Audit Keamanan, *ISO 27001:2013*, Maturity level

**AUDIT KEAMANAN SISTEM INFORMASI DI DINAS KOMUNIKASI
DAN INFORMATIKA PROVINSI LAMPUNG MENGGUNAKAN
STANDAR *ISO/IEC 27001:2013***

Oleh
Annisa Meyliana

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
2019

Judul Skripsi : **AUDIT KEAMANAN SISTEM INFORMASI
DI DINAS KOMUNIKASI DAN
INFORMATIKA PROVINSI LAMPUNG
MENGUNAKAN STANDAR *ISO/IEC*
27001:2013**

Nama Mahasiswa : **Annisa Meyliana**

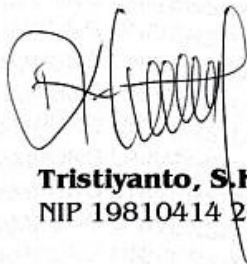
Nomor Pokok Mahasiswa : 1417051017

Jurusan : Ilmu Komputer

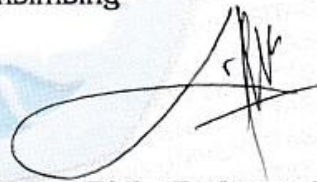
Fakultas : Matematika dan Ilmu Pengetahuan Alam

MENYETUJUI

1. Komisi Pembimbing



Tristiyanto, S.Kom., M.I.S., Ph.D.
NIP 19810414 200501 1 001



Rizky Prabowo, M.Kom.
NIK 231708880807101

2. Ketua Jurusan Ilmu Komputer



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

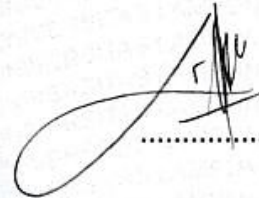
MENGESAHKAN

1. Tim Penguji

Ketua : **Tristiyanto, S.Kom., M.I.S., Ph.D.**



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



Penguji
Bukan Pembimbing : **Dr. Ir. Kurnia Muludi, M.S.Sc.**

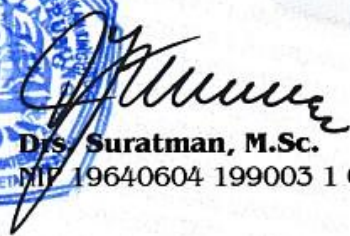


2. Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam



Drs. Suratman, M.Sc.

NIP. 19640604 199003 1 002



Tanggal Lulus Ujian Skripsi : 12 Maret 2019

PERNYATAAN

Saya yang bertanda tangan di bawah ini, menyatakan bahwa skripsi saya yang berjudul **“Audit Keamanan Sistem Informasi Di Dinas Komunikasi Dan Informatika Provinsi Lampung Menggunakan Standar *ISO/IEC 27001:2013*”** 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, 12 Maret 2019



Annisa Meyliana
NPM. 1417051017

RIWAYAT HIDUP



Penulis dilahirkan di Bandar Lampung Provinsi Lampung pada tanggal 22 Mei 1996, sebagai anak keempat dari empat bersaudara dengan ayah bernama Drs Amir dan ibu bernama Gustina. Penulis memiliki seorang kakak laki-laki bernama Nico, Adhy dan Adit.

Penulis menyelesaikan Taman Kanak-Kanak (TK) di TK Kartika II-26 Bandar Lampung pada tahun 2002, Sekolah Dasar (SD) di SD Kartika II-5 Bandar Lampung pada tahun 2008, Sekolah Menengah Pertama (SMP) di SMP Negeri 18 Bandar Lampung pada tahun 2011, dan Sekolah Menengah Atas (SMA) di SMA Negeri 10 Bandar Lampung pada tahun 2014.

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

1. Anggota Abacus Himakom 2014-2015.
2. Anggota Bidang Internal Himakom 2015-2016.
3. Melaksanakan Kerja Praktik di Dinas Sosial Provinsi Lampung, Bandar Lampung pada tanggal 16 Januari-24 Februari 2017.
4. 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

“Sekecil apapun kalian membantu meringankan beban orang lain dengan ikhlas lillah itaala, pasti akan selalu dibalas dengan Allah SWT lebih dari yang kalian bayangkan (sangka).”

“Tetaplah menjadi diri sendiri dan terimalah dirimu apa adanya.”

“Jadikan Allah SWT, Al-Qur'an, dan Orang tua sebagai pedoman hidupmu.”

SANWACANA

Alhamdulillah, puji syukur kehadirat Allah SWT, atas berkat karunia-Nya sehingga penulis dapat menyelesaikan skripsi di Jurusan Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung. Skripsi ini diselesaikan dengan judul penelitian “Audit Keamanan Sistem Informasi Di Dinas Komunikasi Dan Informatika Provinsi Lampung Menggunakan Standar *ISO/IEC 27001:2013*”. Dalam penyusunan skripsi ini, penulis mendapat bantuan, dukungan dan dorongan dari berbagai pihak. Terima kasih penulis sampaikan kepada semua pihak yang telah membantu dan berperan besar dalam menyusun skripsi ini, antara lain.

1. Kedua orangtua tercinta, mama dan papa yang selalu mendoakan dan tidak pernah henti-hentinya selalu memberikan rasa hangatnya kasih sayang, selalu mendukung, membimbing, menghargai setiap proses penulis selama ini.
2. Kakak-kakakku tersayang Susan, Nico, Adhy dan Adit yang selalu memberi doa, menghibur, menghargai, menyayangi dan usil yang tiada henti dari kecil hingga tulisan ini dibuat hal tersebut masih hangat terasa.
3. Bapak Tristiyanto, S.Kom., M.I.S., Ph.D selaku pembimbing utama saya dalam penelitian ini, yang telah memberikan ide, semangat, motivasi, nasihat, serta keikhlasan beliau yang luar biasa dalam membantu saya menyelesaikan skripsi ini.
4. Bapak Rizky Prabowo, M.Kom selaku pembimbing kedua yang telah memberikan ide, kritik, dan nasihat selama penulis melakukan penelitian sehingga penulis dapat menyelesaikan skripsi ini.

5. Bapak Dr. Ir. Kurnia Muludi, M.S.Sc selaku pembahas yang telah memberikan banyak masukan, ide, kritik, serta saran yang bermanfaat dalam perbaikan dalam proses menyelesaikan skripsi ini.
6. Bapak Drs Suratman, M.Sc. sebagai Dekan FMIPA Universitas Lampung.
7. Bapak Dr. Ir. Kurnia Muludi, M.S.Sc., selaku Ketua Jurusan Ilmu Komputer FMIPA Universitas Lampung.
8. Bapak Didik Kurniawan, S.Si., M.T. sebagai Sekretaris Jurusan Ilmu Komputer FMIPA Universitas Lampung sekaligus Pembimbing Akademik yang telah membimbing, memotivasi, dan mendukung penulis sehingga penulis memiliki target dalam setiap menyelesaikan sesuatu.
9. Ibu Anie Rose Irawati, ST, M.Cs sebagai pembimbing akademik penulis yangtelah memberikan saran, motivasi, dan bimbingan selama menjalani masa perkuliahan di Jurusan Ilmu Komputer.
10. Seluruh Bapak dan Ibu Dosen Jurusan Ilmu Komputer yang telah memberikan Ilmu dan pelajaran hidup selama penulis menjadi mahasiswa.
11. Bapak Budi Marta, Bapak Irsan Murhan dan Bapak Hamami selaku pembimbing saat penelitian skripsi yang membimbing, menasihati, mengajarkan arti kedisiplinan, memberikan motivasi selama penulis melakukan penelitian di Kominfo
12. Sahabat, rekan, rival, sekaligus kakak yang telah memberikan semangat dan motivasi kepada penulis.
13. Ibu Nora dan Ibu Wiwik yang telah membantu dalam segala urusan administrasi di Jurusan Ilmu Komputer dan memberikan saya semangat dalam mengejar gelar sarjana Ilmu Komputer.
14. UKHTI (Danis Sela, Arien Ferlina, Desta Riani, Dwi Tia, Elfeny Nandia, Eindita Septiara, Gisella Roliani, dan Hanifah Atiya) yang senantiasa memberikan dukungan moril, selalu menemani, dan memberi keceriaan selama perkuliahan ini.

15. Terspesial untuk Danis Sela Valena yang selalu mengerti, menghibur, membantu dalam hal apapun dan memberi semangat untuk penulis.
16. Teman-teman maba (Caroline, Frandhika, Yusikania, Ferly, Adit, Dicky, Malik) yang telah berjuang bersama-sama dalam menajalankan studi dan skripsi di Ilmu Komputer.
17. 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.

Penulis

Annisa Meyliana

DAFTAR ISI

	Halaman
DAFTAR ISI	i
DAFTAR GAMBAR	iii
DAFTAR TABEL	iv
I. PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Rumusan Masalah	3
1.3 Batasan Masalah.....	4
1.4 Tujuan Penelitian.....	4
1.5 Manfaat Penelitian.....	4
II. TINJAUAN PUSTAKA	6
2.1 Penelitian Terdahulu.....	6
2.2 Pengertian Audit.....	7
2.3 Audit Internal	7
2.4 Audit Sistem Informasi	8
2.5 Karakteristik Audit Teknologi Informasi (TI).....	8
2.6 Keamanan Informasi	10
2.7 Keamanan Teknologi Informasi	13
2.8 Tujuan Audit Keamanan	14
2.9 Tahapan Audit	14
2.10 ISO.....	15
2.11 ISO/IEC 27001	15
2.12 ISO 27001:2013	16
2.13 Analisis SWOT (<i>Strength, Weakness, Opportunity, Threat</i>)	17
2.14 <i>Maturity Level</i>	18
2.15 Lampiran A (Annex A)	20
III. METODOLOGI PENELITIAN	24
3.1 Sumber Data	24
a. Data Primer.....	24
b. Data Sekunder	24
3.2 Tempat dan Waktu Penelitian	25
3.3 Gambaran Umum Perusahaan	25

3.3.1	Profil Perusahaan	25
3.3.2	Jenis Produk atau Jasa.....	27
3.3.3	Bagan Struktur Organisasi Instansi.....	28
3.3.4	<i>Job Description</i>	28
3.3.5	Peralatan, <i>Software</i> dan Aplikasi Pendukung.....	35
3.3.6	Proses Produksi Instansi	35
3.3.7	Identifikasi Proses Bisnis.....	36
3.3.8	Produk yang Sudah Dihasilkan.....	36
3.3.9	Mitra Perusahaan dan Klien.....	37
3.4	Kerangka Penelitian	37
3.5	Perencanaan.....	38
3.6	Studi Literatur.....	38
3.7	Metode Pengumpulan Data	38
3.8	Pelaksanaan/Analisis Audit.....	39
3.9	Rekomendasi	40
3.10	Pelaporan Hasil Audit	40
IV.	HASIL DAN PEMBAHASAN	41
4.1	Data Penelitian	41
4.2	Analisis SWOT (<i>Strength, Weakness, Opportunity, Threat</i>)	41
4.2.1	<i>Strength</i>	41
4.2.2	<i>Weakness</i>	42
4.2.3	<i>Opportunity</i>	42
4.2.4	<i>Threat</i>	43
4.3	Penentuan <i>Maturity Level</i>	43
4.4	<i>Gap</i> Analisis	43
4.5	Pengolahan Data Responden.....	44
4.6	Hasil Keseluruhan <i>Maturity Level</i>	56
4.7	Hasil Temuan	59
4.8	Rekomendasi Hasil Audit.....	85
V.	KESIMPULAN DAN SARAN	87
5.1	Kesimpulan.....	87
5.2	Saran.....	88
	DAFTAR PUSTAKA	89

DAFTAR GAMBAR

	Halaman
Gambar 1. <i>Maturity Level</i>	18
Gambar 2. Dinas Komunikasi dan Informatika Provinsi Lampung.....	26
Gambar 3. Struktur Organisasi Dinas Komunikasi dan Informatika	28
Gambar 4. Tahapan Metode Penelitian.....	37
Gambar 5. Grafik Pencapaian <i>Maturity Level</i>	58

DAFTAR TABEL

	Halaman
Tabel 1. Penelitian terkait Keamanan Sistem Informasi.....	6
Tabel 2. Skala Pembulatan Indeks	20
Tabel 3. Klausul ISO 27001:2013.....	21
Tabel 4. Perhitungan <i>gap</i> analisis untuk domain ISO 27001:2013.....	44
Tabel 5. Pengolahan Data Responden <i>Information security policies</i>	48
Tabel 6. Pengolahan Data Responden <i>Organization of information security</i>	49
Tabel 7. Pengolahan Data Responden <i>Human resource security</i>	49
Tabel 8. Pengolahan Data Responden <i>Asset management</i>	50
Tabel 9. Pengolahan Data Responden <i>Access control</i>	50
Tabel 10. Pengolahan Data Responden <i>Physical and environmental security</i>	51
Tabel 11. Pengolahan Data Responden <i>Operations security</i>	52
Tabel 12. Pengolahan Data Responden <i>Communications security</i>	53
Tabel 13. Pengolahan Data Responden <i>Systems acquisition, development and maintenance</i>	53
Tabel 14. Pengolahan Data Responden <i>Supplier relationships</i>	54
Tabel 15. Pengolahan Data Responden <i>Information security incident management</i>	55

Tabel 16. Pengolahan Data Responden <i>Information security aspects of business continuity management</i>	55
Tabel 17. Pengolahan Data Responden <i>Compliance</i>	56
Tabel 18. Hasil Keseluruhan <i>Maturity Level</i>	57
Tabel 19. Hasil temuan sub domain <i>Information security policies</i>	59
Tabel 20. Hasil temuan sub domain <i>Organization of information security</i>	60
Tabel 21. Hasil temuan sub domain <i>Human resource security</i>	62
Tabel 22. Hasil temuan sub domain <i>Asset management</i>	64
Tabel 23. Hasil temuan sub domain <i>Access control</i>	66
Tabel 24. Hasil temuan sub domain <i>Physical and environmental security</i>	68
Tabel 25. Hasil temuan sub domain <i>Operations security</i>	70
Tabel 26. Hasil temuan sub domain <i>Communications security</i>	72
Tabel 27. Hasil temuan sub domain <i>Systems acquisition, development and</i>	74
Tabel 28. Hasil temuan sub domain <i>Supplier relationships</i>	77
Tabel 29. Hasil temuan sub domain <i>Information security incident management</i> . 78	
Tabel 30. Hasil temuan sub domain <i>Information security aspects of business</i>	81
Tabel 31. Hasil temuan sub domain <i>Compliance</i>	82
Tabel 32. Hasil Analisis <i>GAP</i>	84
Tabel 33. Rekomendasi Hasil Audit	85

I. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi dan sistem informasi pada pemerintahan semakin pesat, risiko keamanan yang melekat pada informasi juga semakin besar. Lemahnya kendali keamanan atas aset informasi memudahkan pihak-pihak yang tidak bertanggung jawab untuk mencurinya atau sekedar mengganggu jalannya aktivitas yang terkait dengan aset tersebut.

Pengelolaan Teknologi Informasi dan Komunikasi yang baik akan mendorong hadir dan terwujudnya *good governance*. Metodologi dan tata kelola yang baik merupakan suatu prasyarat yang menjadi kewajiban dalam pengelolaan sebuah sistem yang baik. Dengan tata kelola yang baik, maka sistem yang *accountable* serta *sustainable* dapat tercapai bagi suatu badan atau lembaga dan dapat memberikan manfaat kepada publik seluas-luasnya (Ibrachim, 2012).

Audit didefinisikan sebagai proses atau aktivitas yang sistematis, independen dan terdokumentasi untuk menemukan suatu bukti-bukti (*audit evidence*) dan dievaluasi secara obyektif untuk menentukan apakah telah memenuhi kriteria pemeriksaan (audit) yang ditetapkan. Tujuan dari audit adalah untuk memberikan gambaran

kondisi tertentu yang berlangsung di perusahaan dan pelaporan mengenai pemenuhan terhadap sekumpulan standar yang terdefinisi (Sarno & Iffano, 2009).

Mengingat pentingnya informasi, maka kebijakan tentang pengamanan informasi harus mencakup sekurang-kurangnya terdapat prosedur pengelolaan aset, prosedur pengelolaan sumber daya manusia, prosedur pengamanan fisik dan lingkungan, prosedur pengamanan *logical security*, prosedur pengamanan operasional teknologi informasi dan prosedur penanganan insiden dalam pengamanan informasi (Perbankan, 2007).

Dinas Komunikasi Dan Informatika merupakan instansi Pemerintahan dibidang komunikasi informatika, Pos dan Telekomunikasi, bidang statistik, bidang persandian, pengelolaan penyiaran dan informasi publik yang berada di Provinsi Lampung. Dinas Komunikasi Dan Informatika Provinsi Lampung merupakan Saruan Kerja Perangkat Daerah (SKPD) baru. Tugas pokok Kominfo Provinsi Lampung adalah melaksanakan kewenangan daerah di bidang komunikasi dan informatika sesuai dengan kebijakan Kepala Daerah, untuk mencapai hasil yang optimal dalam pelaksanaan tugas.

Audit keamanan sistem informasi diperlukan di Dinas Komunikasi dan Informatika (KOMINFO) untuk dapat memastikan keamanan informasi yang sesuai dengan prosedur. Standar yang digunakan untuk audit keamanan sistem informasi yaitu menggunakan *ISO/IEC27001*. Beberapa hal penting yang patut dijadikan pertimbangan mengapa standar *ISO/IEC 27001* dipilih karena dengan standar ini sangat fleksibel dikembangkan dan sangat tergantung dari kebutuhan organisasi, tujuan organisasi, persyaratan keamanan, proses bisnis dan ukuran struktur

organisasi serta *ISO/IEC27001* menyediakan sertifikat implementasi Sistem Manajemen Keamanan Informasi (SMKI) yang diakui secara internasional yang disebut *Information Security Management System (ISMS) certification* (Sarno & Iffano, 2009).

ISO/IEC 27001 merupakan dokumen standar sistem manajemen keamanan informasi, yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah perusahaan untuk mengevaluasi, mengimplementasikan dan memelihara keamanan informasi di perusahaan. Kontrol keamanan berdasarkan *ISO/IEC 27001* terbagi menjadi 14 klausul kontrol keamanan (*security control*), 39 obyektif kontrol (*control objectives*) dan 133 kontrol keamanan.

Berdasarkan uraian diatas, perlu adanya suatu “Audit Keamanan Sistem Informasi Di Dinas Komunikasi Dan Informatika Provinsi Lampung”.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, adapun rumusan masalah yang dibahas pada penelitian ini sebagai berikut:

1. Apakah audit keamanan sistem informasi di Kominfo telah dilaksanakan menggunakan standar *ISO/IEC27001* ?
2. Apakah hasil audit keamanan sistem informasi di Kominfo berdasarkan standar *ISO/IEC 27001* ?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini sebagai berikut :

1. Framework audit keamanan sistem informasi yang digunakan adalah standar *ISO/IEC 27001*.
2. Audit menggunakan *checklist* yang terdapat dalam panduan *ISO/IEC 27001:2013*
3. Data-data yang digunakan dalam pembahasan masalah adalah data yang diperoleh dari observasi, wawancara, dan kuisisioner.

1.4 Tujuan Penelitian

Dalam penelitian ini bertujuan untuk:

1. Audit keamanan sistem informasi pada Kominfo berdasarkan standar *ISO/IEC 27001* dengan melakukan wawancara, melakukan kuisisioner, dan melakukan observasi untuk menentukan tingkat keamanan yang baik untuk Kominfo.
2. Hasil audit keamanan sistem informasi di Kominfo berdasarkan rekomendasi yang digunakan sebagai saran untuk perbaikan kontrol keamanan.

1.5 Manfaat Penelitian

Dengan dilakukannya penelitian ini diharapkan dapat memberi manfaat diantaranya :

1. Bagi penulis, penelitian ini bermanfaat untuk menambah wawasan pengetahuan dalam pelaksanaan audit keamanan sistem informasi.

2. Menghasilkan dokumen hasil audit keamanan berdasarkan dokumen temuan audit dan rekomendasi hasil audit.
3. Hasil penelitian ini dapat dijadikan sebagai acuan dalam meningkatkan keamanan sehingga proses bisnis semakin lebih baik dan meningkat.

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 Bangils Berdasarkan 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 Pemeeliharaan.	Hasil Pemeriksaan kontrol keamanan Audit diperoleh Tingkat kematangan sistem sebesar 2,72.
2.	(Ciptaningrum <i>et al</i> , 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 <i>level P (Partially Achieved)</i> , yaitu proses EDM03, APO12, APO13, dan BAI06. Sedangkan DSS05 berada pada <i>level L (Largely Achieved)</i> .

Tabel 1 (Lanjutan)

No	Peneliti	Masalah	Metode	Hasil
3.	(Ikhsan <i>et al</i> , 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 klausul yang telah tersedia, yaitu A.9, A.11, A.12, dan A.13 berdasarkan tingginya <i>level</i> resiko.	Diperoleh Nilai Kematangan pada 4 klausul keamanan yang bernilai 2.5 yang berarti kontrol Keamanan masih berada pada <i>level</i> 2.

2.1 Pengertian Audit

Audit didefinisikan sebagai proses atau aktivitas yang sistematis, independen dan terdokumentasi untuk menemukan suatu bukti-bukti (*audit evidence*) dan dievaluasi secara obyektif untuk menentukan apakah telah memenuhi kriteria pemeriksaan (audit) yang ditetapkan. Tujuan dari audit adalah untuk memberikan gambaran kondisi tertentu yang berlangsung di perusahaan dan pelaporan mengenai pemenuhan terhadap sekumpulan standar yang terdefinisi (Sarno & Iffano, 2009).

2.2 Audit 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.

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.

2.3 Audit Sistem Informasi

Audit Sistem Informasi sebagai proses pengumpulan dan pengevaluasian bukti (*evidence*) untuk menentukan apakah sistem informasi dapat melindungi aset, serta apakah teknologi informasi yang ada telah memelihara integritas data sehingga keduanya dapat diarahkan kepada pencapaian tujuan bisnis secara efektif dengan menggunakan sumber daya secara efektif (Sarno & Iffano, 2009).

2.4 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).

2.5 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. Pernyataan 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 maupun eksternal serta disengaja maupun tidak disengaja (McLeod & Schell, 2007).

Keamanan informasi adalah salah satu upaya untuk mengamankan aset informasi yang dimiliki (Syafriзал, 2007) Sedangkan informasi sendiri merupakan suatu aset penting yang harus dilindungi keamanannya. Untuk menjadi aman adalah dengan cara dilindungi dari musuh dan bahaya (Whitman & Mattord, 2016).

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

a. *Physical Security*

Strategi yang memfokuskan strategi untuk mengamankan pekerja atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.

b. *Personal Security*

Strategi yang *overlap* dengan *physical security* dalam melindungi orang-orang dalam organisasi.

c. *Operation Security*

Strategi yang memfokuskan strategi untuk mengamankan kemampuan organisasi atau perusahaan untuk bekerja tanpa gangguan.

d. *Communications Security*

Strategi yang bertujuan mengamankan media komunikasi, teknologi komunikasi dan isinya, serta kemampuan untuk memanfaatkan alat ini untuk mencapai tujuan organisasi.

e. *Network Security*

Strategi yang memfokuskan pada pengamanan peralatan jaringan data organisasi, jaringannya dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

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

a. *Confidentiality* (kerahasiaan)

Aspek yang menjamin kerahasiaan data atau informasi, memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang dan menjamin kerahasiaan data yang dikirim, diterima dan disimpan.

b. *Integrity* (integritas)

Aspek yang menjamin bahwa data tidak dirubah tanpa ada ijin pihak yang berwenang (*authorized*), menjaga keakuratan dan keutuhan informasi serta metode prosesnya untuk menjamin aspek *integrity* ini.

c. *Availability* (ketersediaan)

Aspek yang menjamin bahwa data akan tersedia saat dibutuhkan, memastikan *user* yang berhak dapat menggunakan informasi dan perangkat terkait.

d. *Privacy* (Privasi)

Informasi yang dikumpulkan, digunakan, dan disimpan oleh organisasi adalah dipergunakan hanya untuk tujuan tertentu, khusus bagi pemilik data saat informasi ini dikumpulkan. *Privacy* menjamin keamanan data bagi pemilik informasi dari orang lain.

e. *Identification* (Identifikasi)

Sistem informasi memiliki karakteristik identifikasi jika bisa mengenali penggunaannya. Identifikasi adalah langkah pertama dalam memperoleh hak akses ke informasi yang diamankan. Identifikasi umumnya dilakukan dengan penggunaan *user name* dan *user ID*.

f. *Authentication* (Otentifikasi)

Autentikasi terjadi pada saat sistem dapat membuktikan bahwa pengguna memang benar-benar orang yang memiliki identitas yang di klaim.

g. *Authorization* (Otorisasi)

Prinsip yang menjamin bahwa pengguna telah mendapatkan otorisasi sehingga dapat mengakses, mengupdate atau menghapus informasi.

h. *Accountability* (Akuntabilitas)

Karakteristik ini dipenuhi jika sebuah sistem dapat menyajikan data semua aktivitas terhadap informasi yang telah dilakukan, dan siapa yang melakukan aktivitas itu.

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

2.6 Keamanan Teknologi Informasi

Menurut (Swastika & 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).

2.7 Tujuan Audit Keamanan

Tujuan utama dari audit keamanan, diantaranya adalah:

1. Memeriksa kesesuaian dari mulai kebijakan, bakuan, pedoman, dan prosedur keamanan yang ada
2. Mengidentifikasi kekurangan dan memeriksa efektifitas dari kebijakan, bakuan, pedoman, dan prosedur keamanan yang ada
3. Mengidentifikasi dan memahami kelemahan (*vulnerability*) yang ada
4. Mengkaji kendala keamanan yang ada terhadap permasalahan operasional, administrasi, dan manajerial, dan memastikan kesesuaian dengan bakuan keamanan minimum
5. Memberikan rekomendasi dan aksi perbaikan/koreksi untuk peningkatan

2.8 Tahapan Audit

Secara umum, tahapan audit dibagi menjadi bagian berikut ini:

1. Perencanaan
2. Pengumpulan data audit
3. Pengujian audit
4. Pelaporan hasil audit
5. Perlindungan atas data dan perangkat audit
6. Penambahan dan tindak lanjut

2.9 ISO

ISO (*International Organization for Standardization*) adalah pengembang terbesar di dunia standar internasional secara sukarela. Standar internasional memberikan sentuhan seni untuk spesifikasi produk, layanan dan praktik yang baik, membantu industri lebih efisien dan efektif. Dikembangkan melalui kesepakatan global, mereka membantu untuk mengatasi hambatan perdagangan internasional (ISO).

2.10 ISO/IEC 27001

ISO 27001 adalah Standar Internasional untuk sistem manajemen keamanan informasi atau lebih sering disebut dengan *Information Security Management Systems* (ISMS). Sejak semua organisasi atau perusahaan menerapkan sistem yang berbeda, ISMS selalu disesuaikan untuk menangani kebutuhan keamanan tertentu. ISMS adalah pendekatan sistematis untuk mengelola informasi sensitif perusahaan, sehingga tetap aman. Ini termasuk informasi orang, proses dan sistem teknologi dan informasi dengan menerapkan proses manajemen risiko. Menerapkan standar ISO 27001 akan membantu organisasi atau perusahaan anda dalam mengelola keamanan aset seperti informasi keuangan, kekayaan intelektual, rincian karyawan atau informasi yang dipercayakan kepada anda oleh pihak ketiga. Hal ini dapat membantu usaha kecil, menengah dan besar di sektor apapun menjaga aset informasi aman.

Standar ISO 27001 menyatakan persyaratan utama yang harus dipenuhi menyangkut:

1. Konteks Organisasi

2. Kepemimpinan
3. Perencanaan
4. *Support*
5. Operasional
6. Evaluasi Kinerja
7. *Improvement*

2.11 ISO 27001:2013

Struktur Standar Sistem Manajemen

Standar ISO 27001:2013 telah mengadopsi format terkini dari standar sistem manajemen yang bertujuan menjaga konsistensi, keselarasan dan kompatibilitas dari sistem manajemen organisasi yang dibangun dengan merujuk pada standar-standar yang dikembangkan ISO, seperti ISO 9001, ISO 14001, ISO 27001, dan lainnya. Perubahan dalam ISO 27001:2013 terlihat jelas dalam struktur dan format klausul utama (*mandatory clause*), yaitu klausul 4-10, yang diberlakukan sama untuk seluruh persyaratan standar sistem manajemen yang diterbitkan ISO.

ISO 27001:2013 menggantikan ISO 27001:2005 dalam menetapkan persyaratan untuk mendirikan, melaksanakan, menjaga dan terus meningkatkan sistem manajemen keamanan informasi dalam konteks organisasi atau perusahaan. Ini juga mencakup persyaratan untuk penilaian dan perlakuan risiko keamanan informasi, serta disesuaikan dengan kebutuhan organisasi atau perusahaan. Persyaratan yang ditetapkan dalam ISO 27001: 2013 adalah generik (umum) dan dimaksudkan untuk dapat diterapkan pada semua organisasi, terlepas dari jenis dan bentuknya.

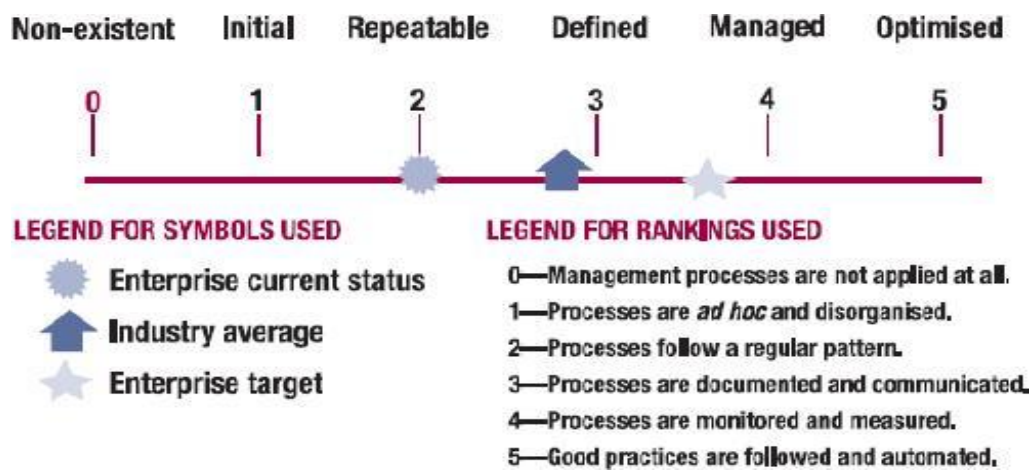
ISO 27001:2013 memiliki 114 kontrol keamanan informasi, dan pada pelaksanaannya perusahaan dapat memilih kontrol mana yang paling relevan dengan kondisi di lapangan dengan melakukan penilaian resiko dan aset pada tahapan awal. Namun pemilihan ini bukan pekerjaan yang mudah, karena banyak parameter yang harus dijadikan pertimbangan. Untuk itu proses pemilihan kontrol keamanan informasi berbasis ISO 27001 umumnya mengandalkan jasa konsultan keamanan informasi.

2.12 Analisis SWOT (*Strength, Weakness, Opportunity, Threat*)

Analisis SWOT adalah analisis untuk mengidentifikasi berbagai faktor secara sistematis dalam merumuskan strategi perusahaan. Analisis ini didasarkan pada logika yang dapat memaksimalkan kekuatan, kelemahan, peluang, dan ancaman. Proses ini melibatkan penentuan tujuan yang spesifik dari bisnis dan mengidentifikasi faktor internal dan eksternal yang mendukung dan yang tidak dalam mencapai tujuan tersebut. Analisis SWOT dapat diterapkan dengan cara menganalisis dan memilah berbagai hal yang mempengaruhi keempat faktornya, yaitu menggunakan analisis SWOT (*strength, weakness, opportunity, threat*) yang menggambarkan pemetaan kondisi kekuatan dan kelemahan di Dinas Komunikasi dan Informatika (kominfo) serta peluang dan ancaman bagi kominfo. Berdasarkan hasil analisis dari dokumen pendukung, observasi, wawancara dan kuisisioner (Rangkuti, 2013).

2.13 Maturity Level

Menurut (Purwanto, 2010) *maturity models* adalah alat bantu yang dapat digunakan untuk melakukan *benchmarking* dan *self-assessment* oleh manajemen Teknologi Informasi untuk menilai kematangan dan *gap* risiko yang ada dalam proses TI.



Secara umum, tingkat kematangan proses Teknologi Informasi dibagi menjadi 6 tingkat, mulai dari tingkat kematangan 0 sampai dengan tingkat kematangan 5. Adapun tingkat kematangan proses tersebut adalah sebagai berikut :

- a. *Level 0 Non-existent* (tidak ada), merupakan posisi kematangan terendah, yang merupakan suatu kondisi dimana organisasi merasa tidak membutuhkan adanya mekanisme proses *IT Governance* yang baku, sehingga tidak ada sama sekali pengawasan terhadap *IT Governance* yang dilakukan organisasi.
- b. *Level 1 Initial Level* (inisialisasi), sudah ada beberapa inisiatif mekanisme perencanaan, tata kelola, dan pengawasan sejumlah *IT Governance* yang dilakukan, namun sifatnya masih *ad hoc*, *sporadis*, tidak konsisten, belum formal, dan reaktif.

- c. *Level 2 Repeatable level* (dapat diulang), kondisi dimana organisasi telah memiliki kebiasaan yang terpola untuk merencanakan dan mengelola *IT Governance* dan dilakukan secara berulang-ulang secara reaktif, namun belum melibatkan prosedur dan dokumen formal.
- d. *Level 3 Defined Level* (ditetapkan, pada tahapan ini organisasi telah memiliki mekanisme dan prosedur yang jelas mengenai tata cara dan manajemen *IT Governance*, dan telah terkomunikasikan dan tersosialisasikan dengan baik di seluruh jajaran manajemen.
- e. *Level 4 Managed Level* (diatur), merupakan kondisi dimana manajemen organisasi telah menerapkan sejumlah indikator pengukuran kinerja kuantitatif untuk memonitor efektivitas pelaksanaan manajemen *IT Governance*.
- f. *Level 5 Optimized Level* (dioptimalisasi), *level* tertinggi ini diberikan kepada organisasi yang telah berhasil menerapkan prinsip-prinsip *governance* secara utuh dan mengacu *best practice*, dimana secara utuh telah diterapkan prinsip-prinsip *governance*, seperti *transparency*, *accountability*, *responsibility*, dan *fairness*.

Menurut (Sarno & Iffano, 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 2. Skala Pembulatan Indeks

<i>Maturity Index</i>	<i>Maturity Level</i>
4.51 – 5.00	5 – Dioptimalisasi (<i>Optimised level</i>)
3.51 – 4.50	4 – Diatur (<i>Managed level</i>)
2.51 – 3.50	3 – Ditetapkan (<i>Defined level</i>)
1.51 – 2.50	2 – Dapat diulang (<i>Repeatable level</i>)
0.51 – 1.50	1 – Inisialisasi (<i>Initial level</i>)
0.00 – 0.50	0 – Tidak ada (<i>Non-Existent</i>)

2.14 Lampiran A (Annex A)

Lampiran A ini menjelaskan bagian dari standar yang menetapkan “sasaran kontrol” dan “kontrol” yang langsung diadopsi dari ISO 27002:2013. Selain memuat sasaran kontrol dan kontrol, ISO 27002 juga memberikan panduan praktik terbaik dan dapat digunakan sebagai referensi untuk memilih kontrol-kontrol mana yang paling cocok untuk diterapkan dalam suatu organisasi.

Lampiran A ini menguraikan 114 kontrol (versi sebelumnya 133 kontrol) yang digunakan untuk membantu melindungi informasi di berbagai area organisasi. Kontrol-kontrol ini digunakan dalam konteks untuk memenuhi persyaratan ISO 27001:2013 di klausul 6.1.3. Jika ISO 27001:2005 mencakup 133 kontrol dalam 11 area kontrol, versi ISO 27001:2013 memuat 114 kontrol dalam 14 area control sebagai berikut:

Tabel 3. Klausul ISO 27001:2013

No	Domain ISO 27001
A.5	<i>Security Policies</i>
A.6	<i>Organisation of Information Security</i>
A.7	<i>Human Resource Security</i>
A.8	<i>Asset Management</i>
A.9	<i>Access Control</i>
A.10	<i>Cryptography</i>
A.11	<i>Physical and Environmental Security</i>
A.12	<i>Operations Security</i>
A.13	<i>Communications Security</i>
A.14	<i>Systems Acquisition, Development and Maintenance</i>
A.15	<i>Supplier Relationships</i>
A.16	<i>Information Security Incident Management</i>
A.17	<i>Information Security Aspects of Business Continuity Management</i>
A.18	<i>Compliance</i>

A.5 Kebijakan keamanan informasi – mengendalikan bagaimana kebijakan ditulis dan ditinjau.

A.6 Organisasi keamanan informasi –kontrol tentang bagaimana tanggung jawab ditugaskan; juga mencakup kontrol untuk perangkat *mobile* dan *teleworking*.

A.7 Keamanan sumber daya manusia – mengendalikan sebelum bekerja, selama, dan setelah pekerjaan.

A.8 Manajemen aset - kontrol yang terkait dengan inventarisasi aset dan penggunaan yang dapat diterima, juga untuk klasifikasi informasi dan penanganan media.

A.9 Kontrol akses – kontrol untuk kebijakan kontrol akses, manajemen akses pengguna, kontrol akses sistem dan aplikasi, dan tanggung jawab pengguna.

A.10 Kriptografi - kontrol yang terkait dengan enkripsi dan manajemen kunci.

A.11 Keamanan fisik dan lingkungan - mengendalikan area yang aman, kontrol masuk, perlindungan terhadap ancaman, keamanan peralatan, pembuangan yang aman, peraturan yang jelas dan kebijakan layar yang jelas, dll.

A.12 Keamanan operasional – banyak kontrol yang terkait dengan pengelolaan produksi TI: manajemen perubahan, manajemen kapasitas, perangkat lunak rusak, cadangan, penebangan, pemantauan, pemasangan, kerentanan, dll.

A.13 Keamanan komunikasi - kontrol yang terkait dengan keamanan jaringan, segregasi, layanan jaringan, pengiriman informasi, pesan, dll.

A.14 Pengambilan, pengembangan dan pemeliharaan sistem - yang menentukan persyaratan keamanan dan keamanan dalam proses pengembangan dan dukungan.

A.15 Hubungan pemasok – mengendalikan apa yang harus disertakan dalam kesepakatan, dan bagaimana memonitor pemasok.

A.16 Manajemen insiden keamanan informasi – kontrol untuk melaporkan kejadian dan kelemahan, menentukan tanggung jawab, prosedur tanggapan, dan pengumpulan bukti.

A.17 Aspek keamanan informasi manajemen kesinambungan bisnis - kontrol yang memerlukan perencanaan kelangsungan bisnis, prosedur, verifikasi dan peninjauan, dan redundansi TI.

A.18 Kepatuhan - kontrol yang memerlukan identifikasi undang-undang dan peraturan yang berlaku, perlindungan kekayaan intelektual, perlindungan data pribadi, dan tinjauan keamanan informasi.

III. METODOLOGI PENELITIAN

3.1 Sumber Data

Sumber data adalah segala sesuatu yang dapat memberikan informasi mengenai data. Data yang dibutuhkan dalam penelitian ini ada dua jenis, yaitu:

a. Data Primer

Data Primer merupakan sumber data penelitian yang diperoleh secara langsung dari sumber aslinya yang berupa wawancara (*interview*) mendalam dengan pihak IT di Kominfo. Narasumber yang dipilih adalah pihak yang mempunyai peranan penting dalam perusahaan khususnya di bidang IT. Dengan kata lain, peneliti membutuhkan pengumpulan data dengan cara menjawab pertanyaan riset (metode survei) yang ada dalam penelitian ini. Data primer juga diperoleh dengan cara diskusi dan langsung turun ke lapangan (metode observasi).

b. Data Sekunder

Data sekunder merupakan sumber data penelitian yang diperoleh melalui media perantara atau secara tidak langsung yang berupa buku, catatan, bukti yang telah ada, atau arsip baik yang dipublikasikan maupun yang tidak dipublikasikan secara umum.

3.2 Tempat dan Waktu Penelitian

1. Waktu Penelitian

Penelitian audit keamanan sistem informasi di Dinas Komunikasi Dan Informatika Provinsi Lampung menggunakan standar *ISO/IEC 27001* ini dilaksanakan pada bulan Januari 2018 sampai selesai.

2. Tempat Penelitian

Penelitian ini dilaksanakan di Dinas Komunikasi Dan Informatika Provinsi Lampung yang beralamat di Jl. WR Monginsidi No.69 Bandar Lampung.

3.3 Gambaran Umum Perusahaan

Gambaran umum Dinas Komunikasi Dan Informatika Provinsi Lampung merupakan Instansi Pemerintahan di bidang komunikasi informatika, Pos dan Telekomunikasi, bidang statistik, bidang persandian, Pengelolaan Penyiaran dan Informasi Publik yang berada di Provinsi Lampung.

3.3.1 Profil Perusahaan

Dinas Komunikasi Dan Informatika Provinsi Lampung yang berada di Jalan RW. Monginsidi No.69 Teluk-Betung-Bandar Lampung 35215 Telp./Fax : (0721) 475270, e-mail : koinfo@lampung.go.id



Gambar 2. Dinas Komunikasi dan Informatika Provinsi Lampung

a. Sejarah Singkat

Sesuai dengan Undang-Undang Nomor 32 Tahun 2004 tentang pemerintah daerah ditegaskan bahwa salah satu prinsip otonomi daerah adalah di berikan nya wewenang pemerintah daerah yang seluas-luas nya untuk mengatur semua urusan pemerintah, di luar pemerintah pusat kemudian melalui otomomi luas, pemerintah daerah juga di harapkan mampu meningkatkan daya saing yang tinggi, dengan memperhatikan prinsip demokrasi, pemerataan, keadilan,serta keanekaragaman daerah yang bertujuan untuk peningkatan pelayanan,pemberdaya dan peran serta masyarakat.

Sejalan dengan semakin meningkatnya perkembangan teknologi informasi,maka di bentuklah Dinas Komunikasi dan Informasi Provinsi Lampung pada tahun 2008 dan mengalami perubahan struktur organisasi pada tahun 2014 dimana bidang

Humas bergabung dengan protocol membentuk biro Humas dan Protocol pembentukan Dinas Komunikasi dan Informatika di Provinsi Lampung berdasarkan pada peraturan daerah Provinsi Lampung Nomor 13 Tahun 2009 sebagaimana telah di ubah dengan peraturan daerah Provinsi Lampung .

b. Visi

“Terwujudnya Pusat Informasi Dan Komunikasi Untuk Menunjang Pembangunan Daerah Menuju Lampung Unggul Dan Berdaya Saing”

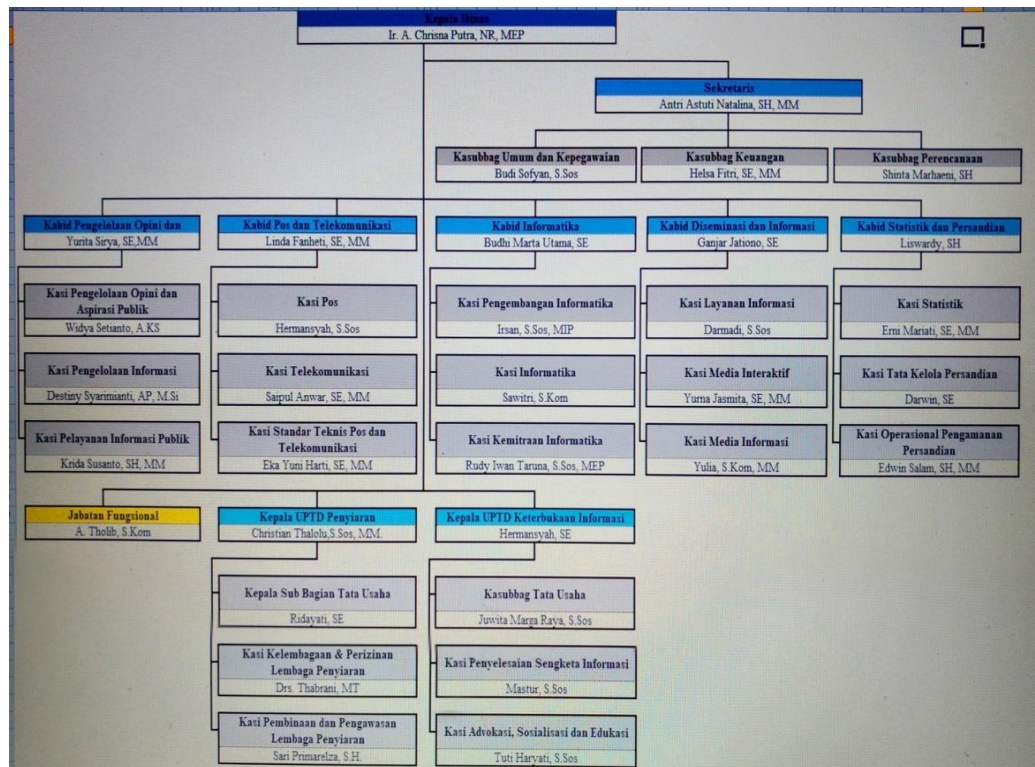
c. Misi

1. Meningkatkan Daya Dukung Infrastruktur Teknologi Komunikasi dan Informasi untuk Memperluas Akses Masyarakat terhadap Informasi Pembangunan Daerah.
2. Meningkatkan Kompetensi Sumber Daya Manusia bidang Komunikasi dan Informatika secara Profesional.
3. Meningkatkan Kualitas Layanan Komunikasi dan Informasi kepada Masyarakat dalam rangka Mewujudkan Masyarakat Berbudaya Informasi.

3.3.2 Jenis Produk atau Jasa

1. Memberi Layanan kepada SKPD di Pemerintah Provinsi Lampung
2. Memberi Layanan Berupa *Hosting Website* ke SKPD
3. Memberi Layanan *Storage Data* di *server* Kominfotik
4. Memberi Layanan Permintaan Sub Domain di SKPD Provinsi Lampung
5. Memberi Layanan mobil M-CAP yaitu mobil internet gratis kepada masyarakat

3.3.3 Bagan Struktur Organisasi Instansi



Gambar 3. Struktur Organisasi Dinas Komunikasi dan Informatika

3.3.4 Job Description

Susunan Organisasi Dinas Komunikasi dan Informatika Provinsi Lampung, terdiri dari:

3.3.4.1 Kepala Dinas

Dinas Komunikasi Dan Informatika mempunyai fungsi:

- Perumusan kebijakan di bidang pengelolaan opini dan aspirasi publik di lingkup provinsi, konten lintas sektoral dan pengelolaan media komunikasi

- publik, layanan infrastruktur dasar data *center*, layanan pengembangan dan pengelolaan aplikasi;
- b. Perumusan kebijakan di bidang statistik dan persandian;
 - c. Pelaksanaan kebijakan di bidang pengelolaan opini dan aspirasi publik di lingkup provinsi, konten lintas sektoral dan pengelolaan media komunikasi publik, layanan infrastruktur dasar data *center*, layanan pengembangan dan pengelolaan aplikasi;
 - d. Pelaksanaan kebijakan di bidang statistik dan persandian;
 - e. Pelaksanaan evaluasi dan pelaporan di bidang pengelolaan opini dan aspirasi publik di lingkup provinsi, konten lintas sektoral dan pengelolaan media komunikasi publik, layanan infrastruktur dasar data *center*, layanan pengembangan dan pengelolaan aplikasi;
 - f. Pelaksanaan evaluasi dan pelaporan di bidang statistik dan persandian

3.3.4.2 Sekretariat

Sekretariat mempunyai fungsi:

- a. Penyiapan bahan pembinaan, pemantauan, pengendalian, dan koordinasi penyusunan program, penyusunan dan penyajian data statistik dan analisis, serta evaluasi dan pelaporan pelaksanaan program
- b. Penyiapan bahan pembinaan, pemantauan, pengendalian dan koordinasi
- c. Penyusunan laporan pelaksanaan kegiatan pada Sekretariat; dan
- d. Pelaksanaan tugas yang diberikan oleh atasan.

- e. Urusan kepegawaian, keuangan, surat menyurat, perlengkapan dan rumah tangga, perundang-undangan serta memberikan pelayanan administrasi kepada semua unit di lingkungan Dinas Komunikasi Dan Informatika.

3.3.4.3 Bidang Umum dan Kepegawaian

- a. Sub Bagian Umum dan Kepegawaian mempunyai tugas melaksanakan urusan tata usaha dan rumah tangga, kearsipan Satker, perencanaan kepegawaian dan pengelolaan administrasi kepegawaian, inventarisasi asset milik daerah di lingkungan satuan kerja.
- b. Melaksanakan dan menyiapkan bahan penyusunan formasi pegawai meliputi formasi kebutuhan, kenaikan pangkat, perbantuan/perpindaan wilayah pembayar gaji
- c. Melaksanakan dan menyiapkan bahan penyelesaian mutasi kepegawaian meliputi, peningkatan status, pengangkatan dalam jabatan, penyesuaian ijasah, peninjau masa kerja, pemberhentian sementara, pemberhentian dan pensiun.
- d. Melaksanakan dan menyiapkan bahan penyusunan kriteria, bimbingan teknis dan evaluasi tingkat pengembangan SDM komunikasi, informatika, statistik, dan persandian.

3.3.4.4 Bidang Pos dan Telekomunikasi

Untuk menyelenggarakan tugas sebagaimana dimaksud pada ayat (1), Bidang Bidang Pos dan Telekomunikasi mempunyai fungsi:

- a. Penyusunan analisa data dan program pelayanan usaha jasa pas, filateli, penyelenggaraan telekomunikasi khusus dan standar teknis pas dan telekomunikasi;
- b. Penyusunan pedoman teknis pelaksanaan kegiatan usaha jasa pas, filateli, penyelenggaraan telekomunikasi khusus dan standar teknis pas dan telekomunikasi;
- c. Pemantauan dan evaluasi serta penyusunan laporan pelaksanaan kegiatan pelayanan usaha jasa pas, filateli, penyelenggaraan telekomunikasi dan penyiaran;
- d. Penyusunan, pedoman dan pemberian bimbingan teknis dibidang sarana telekomunikasi dan pelayanan rekomendasi dibidang penyiaran;
- e. Pemberian izin/ujian amatir radio dan IKRAP dan
- f. Pelaksanaan tugas lain yang diberikan oleh atasan.

3.3.4.5 Bidang Keuangan

Sub Bagian Keuangan mempunyai tugas melaksanakan tugas pengelolaan dan administrasi keuangan. Rincian tugas Sub Bagian Keuangan adalah sebagai berikut:

- a. Melaksanakan dan menyiapkan bahan pembinaan pengelolaan dan administrasi keuangan Satuan Kerja;
- b. Melaksanakan dan menyiapkan bahan pengelolaan perbendaharaan;
- c. Melaksanakan dan menyiapkan bahan verifikasi anggaran dan akuntansi serta menyusun neraca keuangan Satuan Kerja;
- d. Melaksanakan dan menyiapkan bahan guna pelaksanaan kegiatan pengelolaan keuangan dan pelaporan anggaran;

- e. Melaksanakan dan menyiapkan bahan laporan pelaksanaan kegiatan Sub Bagian Keuangan

3.3.4.6 Bidang Perencanaan

- a. Melaksanakan dan menyiapkan bahan koordinasi, integrasi dan sinkronisasi program kerja dan anggaran pembangunan bidang komunikasi, informatika, statistik, dan persandian internal maupun yang lintas sektoral
- b. Melaksanakan dan menyiapkan bahan penyusunan pola perencanaan dan anggaran pembangunan bidang komunikasi, informatika, statistik, dan persandian
- c. Melaksanakan dan menyiapkan bahan sinkronisasi program pembangunan bidang komunikasi, informatika, statistik, dan persandian dengan Kabupaten/Kota
- d. Melaksanakan dan menyiapkan bahan rencana program dan anggaran satker
- e. Melaksanakan dan menyiapkan bahan menyusun, mengumpulkan bahan-bahan evaluasi bidang tugas
- f. Melaksanakan dan menyiapkan bahan evaluasi dan monitoring program kegiatan bidang komunikasi informatika, statistik dan persandian
- g. Melaksanakan dan menyiapkan bahan laporan evaluasi dan monitoring

3.3.4.7 Bidang Pengelolaan Opini dan Aspirasi Publik

Untuk menyelenggarakan tugas sebagaimana dimaksud pada ayat (1), Bidang Pengelolaan Opini dan Aspirasi Publik mempunyai fungsi:

- a. Penyiapan bahan perumusan kebijakan di bidang pengelolaan opini dan aspirasi publik di lingkup pemerintah provinsi, pengelolaan informasi untuk mendukung kebijakan nasional dan pemerintah provinsi, serta pelayanan informasi publik di Provinsi
- b. Penyiapan bahan pelaksanaan kebijakan di bidang pengelolaan opini dan aspirasi publik di lingkup pemerintah provinsi, pengelolaan informasi untuk mendukung kebijakan nasional dan pemerintah provinsi, serta pelayanan informasi publik di Provinsi
- c. Penyiapan bahan penyusunan norma, standar, prosedur, dan kriteria penyelenggaraan di bidang pengelolaan opini dan aspirasi publik di lingkup pemerintah provinsi, pengelolaan informasi untuk mendukung kebijakan nasional dan pemerintah provinsi, serta pelayanan informasi publik di Provinsi
- d. Penyiapan bahan pemberian bimbingan teknis dan supervisi di bidang pengelolaan opini dan aspirasi publik di lingkup pemerintah provinsi, pengelolaan informasi untuk mendukung kebijakan nasional dan pemerintah provinsi, serta pelayanan informasi publik di Provinsi;

3.3.4.8 Bidang Informatika

Untuk menyelenggarakan tugas sebagaimana dimaksud pada ayat (1), Bidang Informatika mempunyai fungsi:

- a. Penyiapan bahan perumusan kebijakan aplikasi layanan *e-government* dan *e-business*;

- b. Penyiapan bahan perumusan kebijakan, pengaturan dan penetapan standar/pedoman pemanfaatan perangkat lunak dan konten, pemberdayaan telematika dan audit aplikasi telematika;
- c. Penyusunan norma, standart, pedoman, kriteria dan prosedur di bidang telematika dan informasi serta komunikasi berbasis elektronika/media bam;
- d. Pembangunan, pengelolaan dan pengembangan infrastruktur dan Manajemen Aplikasi Sistem Informasi Pemerintah;

3.3.4.9 Bidang Statistik dan Persandian

Untuk menyelenggarakan tugas sebagaimana dimaksud pada ayat (1). Bidang Statistik dan Persandian mempunyai fungsi:

- a. Perumusan kebijakan statistik sektoral di lingkungan pemerintah daerah;
- b. Perumusan peraturan teknis tata kelola statistik sektoral;
- c. Perumusan kebijakan keamanan informasi di lingkungan pemerintah daerah;
- d. Perumusan peraturan teknis tata kelola persandian untuk pengamanan informasi;
- e. Pengelolaan informasi berklasifikasi;
- f. Pengelolaan administratif.

3.3.3.10 Bidang Desiminasi dan Informasi

Untuk menyelenggarakan tugas sebagaimana dimaksud pada ayat (1), Bidang Diseminasi dan Informasi mempunyai fungsi:

- a. Pelaksanaan rumusan dan kebijakan pelayanan informasi publik

- b. Pelaksanaan penyiapan rumusan dan kebijakan pelaksanaan pemberdayaan media interkatif
- c. Pelaksanaan penyiapan rumusan dan kebijakan pelaksanaan pemberdayaan media informasi
- d. Pelaksanaan tugas-tugas lain yang diberikan oleh Kepala Dinas.

3.3.5 Peralatan, *Software* dan Aplikasi Pendukung

- a. Peralatan pendukung

Peralatan pendukung yang digunakan di Kominfo diantaranya: komputer, printer, meja, *scanner*, AC, jam dinding, lemari, dispenser, CCTV, kontak sampah, alat tulis kantor, koneksi internet, *monitor*, CPU, telepon.

- b. *Software* pendukung

Software pendukung yang digunakan di Kominfo diantaranya: *Microsoft Office*, *Mozilla*.

- c. Aplikasi pendukung

Aplikasi pendukung yang digunakan di Kominfo diantaranya: *Mail server*, media *online*, aplikasi keuangan dan Kominfo memiliki *website* yaitu lampungprov.go.id.

3.3.6 Proses Produksi Instansi

Proses produksi adalah suatu kumpulan aktivitas atau pekerjaan terstruktur yang saling terkait untuk menyelesaikan suatu masalah tertentu atau yang menghasilkan layanan adalah sebagai berikut :

1. Adanya permintaan hosting dan Sub domain dari satuan kerja yang bersangkutan, setelah itu Dinas Kominfotik memberi tanggapan terkait hosting yang di dalam nya terdapat *user* dan *password* .
2. Setelah jadi ada besaran kuota dan yang dan fasilitas hosting *file* yang di peruntukan mengelola data satuan kerja untuk di tampilkan kedalam *website*.

3.3.7 Identifikasi Proses Bisnis

Pada tahapan ini pemahaman proses bisnis dan IT perusahaan yang diaudit (*auditee*). Proses bisnis yang ada di Dinas Komunikasi dan Informatika yaitu:

- a. Menerima pesanan, proses pertama adanya permintaan hosting dan sub domain dari satuan kerja yang bersangkutan yaitu dengan dibuatkan surat permohonan dari SKPD ke Dinas Komunikasi dan Informatika Provinsi Lampung.
- b. Pemrosesan, setelah itu Dinas Komunikasi dan Informatika Provinsi Lampung memberikan tanggapan terkait hosting yang di dalam nya terdapat *user* dan *password*.
- c. Kontrak kerja, proses kontrak kerja antara Dinas Kominfo dengan SKPD terkait ada besaran kuota dan fasilitas *hostingfile* yang di peruntukan mengelola data satuan kerja untuk ditampilkan kedalam *website*.

3.3.8 Produk yang Sudah Dhasilkan

Produk yang dihasilkan oleh Dinas Komunikasi Dan Informatika yaitu:

1. *Website* dan *Hosting*
2. *Server*

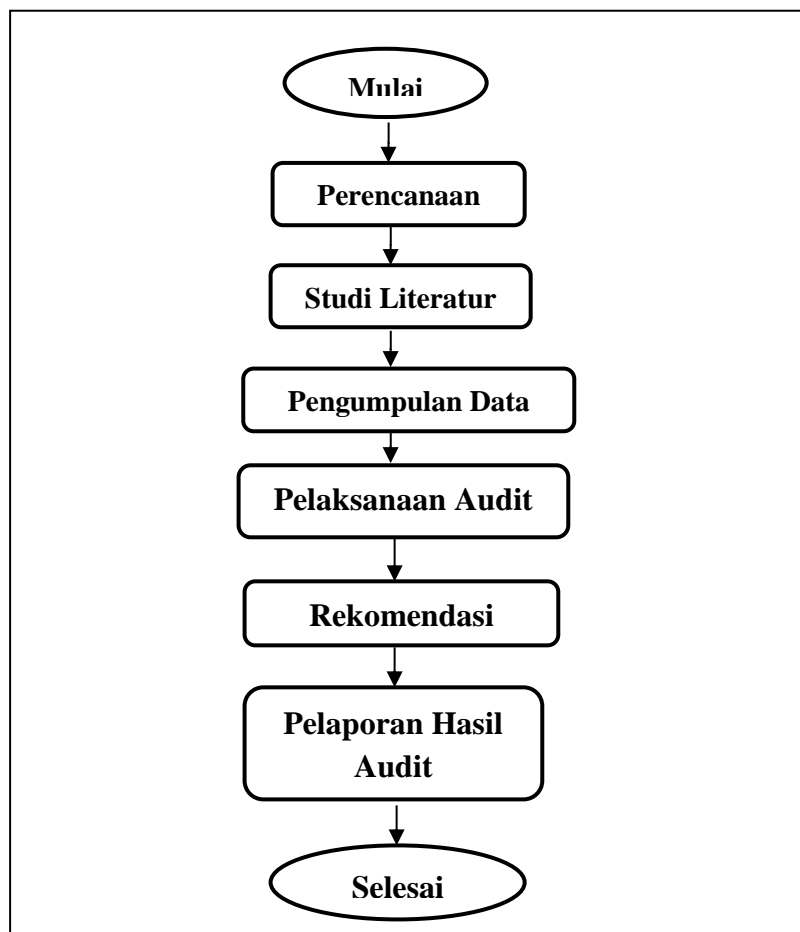
3.3.9 Mitra Perusahaan dan Klien

Rekan mitrayang telah bekerja sama dengan Dinas Komunikasi Dan Informatika berjumlah 2 Instansi yaitu:

1. Satuan Kerja Perangkat Daerah Provinsi Lampung
2. Radio ASN 107,9 FM

3.4 Kerangka Penelitian

Berdasarkan landasan teori dan rumusan masalah, maka dapat diidentifikasi bahwa kerangka berfikir dalam penelitian yang digunakan adalah seperti yang diilustrasi pada gambar dibawah ini :



Gambar 4. Tahapan Metode Penelitian

3.5 Perencanaan

Berdasarkan data yang didapatkan sebelumnya, maka dibuat daftar kerja yang berguna sebagai acuan untuk pelaksanaan audit keamanan. Perencanaan ini termasuk merencanakan daftar pertanyaan yang akan ditanyakan ke narasumber tertentu, hal yang perlu di observasi dan dokumen lainnya yang dibutuhkan. Penyusunan daftar kerja yang dibuat dari Annex A di *ISO/IEC 27001:2013*, menjelaskan bagian dari standar yang menetapkan “sasaran kontrol” dan “kontrol” dan menguraikan versi *ISO/IEC 27001:2013* memuat 114 kontrol dalam 14 area kontrol.

3.6 Studi Literatur

Studi literatur yaitu melakukan *review*, perbandingan dan melihat literatur yang terkait dengan penelitian. Studi literatur sejenis digunakan untuk menambah referensi teori-teori yang dibutuhkan dalam penelitian dengan mempelajari literatur yang turut mendukung penelitian sebelumnya tentang audit keamanan sistem informasi menggunakan *ISO/IEC*, jurnal ilmiah tentang proses audit menggunakan *ISO/IEC* dan buku teks tentang *ISO/IEC*.

3.7 Metode Pengumpulan Data

Teknik pengumpulan data yang digunakan dalam penelitian menggunakan metode sebagai berikut:

a. Metode Observasi

Observasi dilakukan secara langsung terhadap perusahaan yang bertujuan untuk mendapatkan data yang digunakan untuk penelitian ini. Observasi ini juga dilakukan melihat seberapa sesuai data yang dikumpulkan, dan keefektifan kontrol keamanan yang ada di Dinas Komunikasi dan Informatika Provinsi Lampung

b. Metode Wawancara

Metode wawancara ini digunakan untuk mendapatkan data yang lebih mendalam dan langsung bertatapapan dengan narasumber. Metode wawancara ini dilakukan dengan pihak IT di Dinas Komunikasi Dan Informatika Provinsi Lampung untuk mengetahui proses keamanan apa sudah sesuai prosedur iso atau belum sesuai.

c. Kuisisioner

Kuisisioner merupakan daftar pertanyaan yang akan digunakan oleh periset untuk memperoleh data dari sumber nya secara langsung melalui proses komunikasi atau dengan mengajukan pertanyaan. Jenis kuisisioner yang digunakan pada penelitian ini dengan menggunakan kuisisioner terstruktur yang terbuka.

3.8 Pelaksanaan/Analisis Audit

Analisis proses ini menggambarkan tentang pembuatan kuesioner yang diberikan kepada responden dan diperoleh sejumlah kriteria yang dilakukan dari awal dan selama proses dilaksanakan. Data diperoleh, kemudian dikumpulkan untuk diolah secara sistematis.

3.9 Rekomendasi

Saran berupa perbaikan, perubahan untuk perusahaan berdasarkan hasil pengelolaan dan analisis pada proses sebelumnya. Rekomendasi berdasarkan standar *ISO/IEC 27001:2013*.

3.10 Pelaporan Hasil Audit

Berdasarkan hasil temuan, maka auditor harus menyusun hasil laporan audit sebagai tanggungjawab atas penugasan audit yang telah dilaksanakan. Tahapan dalam pelaporan ini yang dilakukan mulai dari menganalisa laporan hasil audit, penyusunan laporan hasil audit, persetujuan laporan hasil audit dan hasil akhir audit.

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 didapat, disimpulkan bahwa Sistem Informasi di Dinas Komunikasi dan Informatika belum memenuhi standar keamanan *ISO 27001*. Saat ini sistem memiliki indeks penilaian sebesar 2.40 dan jika dibulatkan ke dalam penilaian *maturity* berada pada *level 2 (Repeatable)* pada skala 5 sesuai standar *ISO/IEC 27001:2013*.
2. Sub domain *Systems acquisition, development and maintenance* hasil responden bernilai 1.41 dan hasil temuan bernilai 1.58 yang merupakan nilai terkecil dari hasil *maturity level*. Nilai dari hasil responden dan hasil temuan terdapat perbedaan dimana belum adanya kebijakan dalam pengembangan sistem yang melalui proses uji keamanan.
3. Rekomendasi yang diberikan dapat meningkatkan keamanan sistem. Terdapat 8 pengelompokan rekomendasi pengendalian keamanan berdasarkan domain yang ada sesuai dengan standar *ISO 27001*.

5.2 Saran

Berdasarkan hasil penelitian yang telah dilakukan, saran untuk penelitian selanjutnya yaitu melakukan audit sistem informasi di Dinas Komunikasi dan Informatika menggunakan *ISO* agar dapat melakukan audit kelayakan dokumen sesuai standar keamanan sistem informasi.

DAFTAR PUSTAKA

- 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>.
- Hidayat, M. N. 2011. Kajian tata kelola keamanan informasi berdasarkan *information security management system (ISMS) ISO 27001:2005* untuk outsourcing teknologi informasi pada PT.Kereta Api Indonesia (Persero), (Program Studi Magister Teknologi Informasi Fasilkom UI).ISO/IEC 27001:2013
- Ibrachim, N. e. (2012). *Bakuan Audit Keamanan Informasi Kemenpora*. Indonesia: Kementrian Pemuda dan Olahraga.
- ISO/IEC 27001:2013. 2017. ISN.
- McLeod, R., & 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* , 50-62.
- Perbankan, D. P. (2007). *Pedoman Penerapan Manajemen Resiko dalam Penggunaan Teknologi Informasi oleh Bank Umum*. Jakarta: Bank Indonesia.
- Purwanto, M. (2010). *Metodologi Penelitian Kuantitatif untuk Psikologi dan Pendidikan*. Yogyakarta: Pustaka Pelajar.
- Rangkuti, F. (2013). *Analisis SWOT: Teknik Membedah Kasus Bisnis*. Jakarta: Percetakan PT.Gramedia.
- Sarno, R., & Iffano, I. (2009). *Sistem Manajemen Keamanan Informasi*. Surabaya: ITS Press.
- Swastika, I. P., & Putra, I. (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)* .

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

Whitman, M. E., & Mattord, H. J. (2016). *Manajemen of Information Security (5th ed)*. Boston: Course Technology.