AUDIT KEAMANAN SISTEM INFORMASI MANAJEMEN DAERAH (SIMDA) KEUANGAN DI BADAN KEUANGAN DAERAH PROVINSI LAMPUNG MENGGUNAKAN INDEKS KAMI BERDASARKAN STANDAR ISO/IEC 27001

(Skripsi)

Oleh:

NUR FITRIANA

JURUSAN ILMU KOMPUTER
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS LAMPUNG

2019

ABSTRACT

THE SECURITY AUDIT OF FINANCIAL MANAGEMENT INFORMATION SYSTEMS (SIMDA) IN LAMPUNG PROVINCIAL FINANCIAL INSTITUTION USING KAMI INDEX BASED ON ISO/IEC 27001 STANDARD

By

NUR FITRIANA

In the implementation of government activities, Lampung province has used information technology such as the finance department of Lampung Province. The finance department of Lampung province uses Finance SIMDA to manage regional finances. To determine the extent of information security has been applied in Finance SIMDA requires an information security audit. This study uses an security evaluation tool based on the ISO/IEC 27001 standard known as the Information Security Index (KAMI Index). The focus of this research are two main areas which are the electronic systems category and the information security category. Data from this study were based on the results of interviews, observations, and questionnaires. Research has found that the maturity level of information security in the category of electronic systems is 18 which means the level of dependence on electronic systems is high. The total value of the maturity level of the information security category is 336, with maturity levels at I+ and II so it can be classified that the information security in Finance SIMDA needs to be improved. In case, recommendations have been given in each information security category to improve the information security.

Keywords: information security audit, KAMI index, ISO/IEC 27001, maturity level.

ABSTRAK

AUDIT KEAMANAN SISTEM INFORMASI MANAJEMEN DAERAH (SIMDA) KEUANGAN DI BADAN KEUANGAN DAERAH PROVINSI LAMPUNG MENGGUNAKAN INDEKS KAMI BERDASARKAN STANDAR ISO/IEC 27001

Oleh

NUR FITRIANA

Provinsi Lampung dalam pelaksanaan kegiatan pemerintahannya telah menggunakan teknologi informasi, seperti yang ada pada Badan Keuangan Daerah Provinsi Lampung. Badan Keuangan Daerah Provinsi Lampung menggunakan SIMDA Keuangan dalam mengelola keuangan daerah. Untuk mengetahui sejauh mana tingkat keamanan informasi telah diterapkan pada SIMDA keuangan maka diperlukan audit keamanan informasi. Penelitian ini menggunakan alat evaluasi keamanan yang berdasar pada standar ISO/IEC 27001 yang dikenal sebagai Indeks Keamanan Informasi (KAMI). Fokus dari penelitian ini meliputi dua area besar yaitu kategori sistem elektronik dan kategori keamanan informasi. Data dari penelitian ini diperoleh berdasarkan hasil wawancara, observasi, dan kuesioner. Hasil penelitian diketahui bahwa ketergantungan terhadap sistem elektronik pada kategori sistem elektronik adalah 18 yang tergolong tinggi. Total nilai tingkat kematangan dari kategori keamanan informasi adalah 336 dengan tingkat kematangan berada pada level I+ dan II sehingga dapat dikelompokkan bahwa status kesiapan keamanan informasi SIMDA Keuangan adalah perlu perbaikan. Rekomendasi telah diberikan pada setiap kategori untuk meningkatkan keamanan informasi yang ada.

Kata Kunci: audit keamanan informasi, indeks KAMI, ISO/IEC 27001, tingkat kematangan.

AUDIT KEAMANAN SISTEM INFORMASI MANAJEMEN DAERAH (SIMDA) KEUANGAN DI BADAN KEUANGAN DAERAH PROVINSI LAMPUNG MENGGUNAKAN INDEKS KAMI BERDASARKAN STANDAR ISO/IEC 27001

Oleh
Nur Fitriana
1517051056

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 MANAJEMEN DAERAH (SIMDA) KEUANGAN DI BADAN KEUANGAN DAERAH PROVINSI LAMPUNG MENGGUNAKAN INDEKS KAMI BERDASARKAN STANDAR ISO/IEC 27001**

Nama : *Nur Fitriana*

NPM : 1517051056

Jurusan : Ilmu Komputer

Fakultas : Matematika dan Ilmu Pengetahuan Alam

Menyetujui,

Komisi Pembimbing

Tristiyanto, S.Kom., M.I.S., Ph.D.

NIP. 19810414 200501 1 001

Mengetahui,

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.** .....

Penguji

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

Penguji

Bukan Pembimbing II : **Anie Rose Irawati, S.T., M.Cs.** .....

2. Dekan Fakultas Matematika dan Ilmu Pengetahuan Alam

Dr. Suratman, M.Sc.

NIP. 19640604 199003 1 002

Tanggal Lulus Ujian Skripsi : 4 Desember 2019

PERNYATAAN

Saya yang bertanda tangan di bawah ini, menyatakan bahwa skripsi saya yang berjudul **"Audit Keamanan Sistem Informasi Manajemen Daerah (SIMDA) Keuangan di Badan Keuangan Daerah Provinsi Lampung Menggunakan Indeks KAMI Berdasarkan 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,

Nur Fitriana
NPM. 1517051056

RIWAYAT HIDUP

Penulis dilahirkan di Bandar Lampung pada tanggal 22 Januari 1997, sebagai anak kedua dari dua bersaudara dengan ayah bernama Edi Yanto dan ibu bernama Suryana. Penulis memiliki seorang kakak laki-laki bernama Afriyan Nazola.

Penulis menyelesaikan Taman Kanak-Kanak (TK) pada tahun 2003 di TK Istiqlal Raja Basa, Sekolah Dasar (SD) di SD Negeri 3 Raja Basa pada tahun 2009, Sekolah Menengah Pertama di SMP Negeri 8 Bandar Lampung pada tahun 2012, dan Sekolah Menengah Atas di SMA Negeri 9 Bandar Lampung pada tahun 2015.

Pada Tahun 2015, 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 Anggota bidang Kaderisasi dan Eksternal. Pada bulan Juli-Agustus 2018, penulis melakukan Kuliah Kerja Nyata selama 32 hari di Desa Wana, Lampung Timur. Selama menjadi mahasiswa, penulis aktif mengikuti beberapa kegiatan, antara lain:

1. Anggota Abacus Himakom 2015-2016.
2. Anggota Bidang Kaderisasi Himakom 2016-2017.
3. Anggota Bidang Eksternal Himakom 2017-2018.

4. Melaksanakan Kerja Praktik di Kementerian PUPR Direktorat Jenderal Bina Marga Provinsi Lampung pada tanggal 16 Januari-2 Maret 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:

Kedua orangtua yang tak pernah berhenti memberikan doa, nasihat, semangat dan motivasi. Terimakasih selama ini telah mendidik, membesarkan, menjaga, melindungi, memberikan kasih sayang, perhatian dan pengorbanan.

Teman-teman yang selalu ada, yang telah membantu dan memberikan semangat dalam mengejar cita-cita.

Almamater Tercinta, Universitas Lampung

MOTO

“Allah tidak akan membebani seseorang melainkan sesuai dengan kesanggupannya”

QS. Al Baqarah:286

“It’s ok not to be ok.”

SANWACANA

Puji syukur 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 Manajemen Daerah (SIMDA) Keuangan di Badan Keuangan Daerah Provinsi Lampung Menggunakan Indeks KAMI Berdasarkan 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. Kedua orang tua dan abangku tercinta, Ibu Suryana, Ayah Edi Yanto, dan Abang Afriyan Nazola yang telah memberikan doa, dukungan dan motivasi serta memfasilitasi kebutuhan untuk menyelesaikan skripsi ini.
2. Bapak Tristiyanto, S.Kom., M.I.S., Ph.D., selaku pembimbing utama yang telah memberikan bimbingan, ilmu, kritik, saran, dan nasihat sehingga skripsi ini dapat diselesaikan.
3. Bapak Didik Kurniawan, S.Si., M.T. sebagai Sekretaris Jurusan Ilmu Komputer sekaligus pembahas I yang telah memberikan masukan-masukan dan saran yang bermanfaat dalam skripsi ini..

4. Ibu Anie Rose Irawati, S.T., M.CS sebagai pembahas II yang telah memberikan masukan-masukan dan saran yang bermanfaat dalam skripsi ini.
5. Bapak Febi Eka Febriansyah, S.T., M.T. sebagai pembimbing akademik penulis yang telah memberikan saran, motivasi, dan bimbingan selama menjalani masa perkuliahan di Jurusan Ilmu Komputer.
6. Bapak Dr. Ir. Kurnia Muludi, M.S.Sc., selaku Ketua Jurusan Ilmu Komputer FMIPA Universitas Lampung.
7. Bapak Prof. Suratman, M.Sc, selaku Dekan FMIPA Universitas Lampung.
8. Bapak dan Ibu Dosen Jurusan Ilmu Komputer yang telah memberikan ilmu pengetahuan yang bermanfaat bagi penulis.
9. Ibu Ade Nora Maela selaku staf administrasi di Jurusan Ilmu Komputer yang telah membantu segala urusan administrasi selama kuliah.
10. Bapak Sondi, bapak Wira, bapak Chandra, bapak Iwan, ibu Anita, dan pihak-pihak yang turut membantu dalam penelitian di instansi.
11. Rekan-rekan seperjuangan, Ijul, Revi, Empew, Indri, Nadya, Yudha, Dana, Inas, Ardian, Akmal, Brok, dan Jaka yang telah memberikan penulis inspirasi dan keceriaan selama perkuliahan.
12. Egidiah, Sasqia, dan Rahma yang selalu memberikan semangat dan membantu penulis saat masa perkuliahan.
13. Teman-teman *Sister-fillah*, Ayu, Irena, Renita, dan Iton yang sudah setia dari SMA dan selalu membantu penulis.
14. Teman-teman Alumni 9, Yuris, Manda, Tri, Tias, Tika, Saphira, Galih, Fika, Tizha, dan Arum yang telah menjadi penghibur kapanpun dan dimanapun.

15. Keluarga KKN Desa Wana I, Mutia, Dina, Memei, Kak Aldi, dan Fajri yang telah berjuang selama 32 hari dan sampai sekarang masih bersama.
16. Semua pihak yang secara langsung dan tidak langsung yang telah membantu dalam penyelesaian skripsi ini.
17. Teman-teman Ilmu Komputer 2015, yang telah berjuang bersama-sama dalam menjalankan studi di Jurusan Ilmu Komputer Universitas Lampung.

Penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan, akan tetapisedikit harapan semoga skripsi ini bermanfaat bagi perkembangan ilmupengetahuan terutama bagi rekan-rekan Ilmu Komputer.

Bandar Lampung, 4 Desember 2019

Nur Fitriana

DAFTAR ISI

Halaman

DAFTAR TABEL

Tabel Halaman

DAFTAR GAMBAR

Gambar Halaman

I. PENDAHULUAN

A. Latar Belakang

Provinsi Lampung dalam pelaksanaan kegiatan pemerintahannya telah menggunakan teknologi informasi, seperti yang ada pada Badan Keuangan Daerah Provinsi Lampung. Dalam menjalankan tugasnya, pemerintah telah memfasilitasi Badan Keuangan Daerah Provinsi Lampung dengan alat bantu dalam pengelolaan keuangan daerah. Alat bantu yang digunakan adalah Sistem Informasi Manajemen Daerah atau SIMDA Keuangan.

SIMDA merupakan sistem informasi yang dikembangkan oleh Badan Pengawasan Keuangan dan Pembangunan (BPKP) untuk membantu pemerintah daerah dalam melaksanakan pengelolaan keuangan daerah. Dalam mempertanggungjawabkan pengelolaan keuangan daerah, pemerintah daerah diwajibkan untuk menyusun laporan keuangan. Untuk itu diperlukan sistem yang dapat diandalkan (*reliable*), yaitu sistem yang mampu mengolah data-data (*input*) dan menghasilkan informasi (*output*) sehingga dapat digunakan oleh manajemen dalam pengambilan keputusan. SIMDA Keuangan bertujuan untuk mengintegrasikan pengelolaan keuangan daerah, baik dalam hal penganggaran, penatausahaan, akuntansi, maupun pelaporannya (BPKP, 2008).

Dalam penggunaan SIMDA Keuangan yang mengintegrasikan pengelolaan keuangan daerah haruslah memastikan semua informasi yang ada di dalamnya terkelola dengan baik. Apabila informasi tidak terkelola dengan baik maka hal itu akan mempengaruhi kepercayaan pimpinan terhadap pengelola sistem yang ada pada pemerintah daerah. Kebocoran informasi sangat merugikan karena dapat mengurangi daya saing organisasi dan juga dapat mengurangi reputasi organisasi. Untuk mengamankan informasi secara terpadu, efektif, dan efisien dibutuhkan kerangka manajemen dan standar keamanan yang baik (Tatiara *et al*, 2017). Standar keamanan dan pelayanan yang digunakan untuk mengatur pelaksanaan proses bisnis bisa menjadi alternatif solusi dalam meminimalisir terjadinya gangguan yang tidak diinginkan (Gehrmann, 2012). Untuk mengetahui sejauh mana keamanan informasi yang telah diterapkan, diperlukan audit keamanan sistem informasi yang cocok dengan tata kelola pelaksanaan SIMDA Keuangan di Badan Keuangan Daerah Provinsi Lampung.

Audit keamanan sistem informasi adalah satu pendekatan untuk mengevaluasi praktik dan operasi sistem informasi organisasi. Proses audit memungkinkan untuk memperoleh bukti keamanan sistem informasi organisasi, efisiensi kebijakan untuk menjaga integritas aset, kerahasiaan dan ketersediaan, serta tujuan keamanan organisasi yang khas. Ada beberapa model atau kerangka kerja untuk mendukung audit keamanan (Onwubiko, 2009), seperti COBIT 5 (Wolden *et al.*, 2015) yang merupakan sebuah *framework* yang dikeluarkan oleh *ISACA (Information System Audit and Control Association)* untuk

mengelola *IT Governance* serta infrastruktur IT di sebuah organisasi dan standar ISO/IEC 27001 (Pelnekar, 2011).

Standar ISO/IEC 27001 dapat membantu organisasi menjaga aset informasi organisasi tetap aman. Standar ini digunakan guna membantu organisasi dalam mengelola keamanan aset seperti informasi keuangan, kekayaan intelektual, rincian karyawan atau informasi yang dipercayakan. ISO/IEC 27001 adalah standar yang diluncurkan oleh ISO (*International Standard Organization*) dan IEC (*International Electronichal Commission*) yang menyediakan persyaratan untuk *Information Security Management System* (ISMS). ISMS adalah pendekatan sistematis untuk mengelola informasi perusahaan yang sensitif sehingga tetap aman. Ini termasuk orang, proses, dan sistem TI dengan menerapkan proses manajemen risiko (ISO, 2013).

ISO/IEC 27001 memungkinkan perusahaan untuk disertifikasi terhadap standar, di mana keamanan informasi dapat didokumentasikan, diterapkan, dan dikelola secara ketat sesuai dengan standar organisasi yang diakui secara internasional (Disterer, 2013). Dengan menerapkan ISO/IEC 27001, organisasi memverifikasi pemenuhan standar keamanan yang diterima sehingga dapat meningkatkan kepercayaan pengguna. Verifikasi kepatuhan dengan standar internasional juga dapat mengurangi risiko denda atau pembayaran kompensasi sebagai akibat dari perselisihan hukum. ISO/IEC 27001 juga menyediakan kerangka kerja proses untuk implementasi keamanan TI dan dapat membantu

dalam menentukan status keamanan informasi dan tingkat kepatuhan terhadap keamanan kebijakan, arahan, dan standar (Pelnekar, 2011).

Dalam menentukan status keamanan informasi dan tingkat kepatuhan suatu organisasi, Indonesia memiliki alat evaluasi tingkat keamanan yang berdasar pada standar ISO 27001:2013 yang dikenal sebagai Indeks Keamanan Informasi (KAMI). Indeks KAMI adalah alat evaluasi yang digunakan untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintah, organisasi berskala nasional, maupun yang berukuran kecil. Alat evaluasi ini merupakan perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi. Evaluasi dilakukan dengan ruang lingkup pembahasan yang juga memenuhi semua aspek yang didefinisikan oleh standar ISO 27001:2013 (Kominfo, 2017) yang mencakup 10 klausul dan 114 kontrol keamanan generik yang dibagi menjadi 14 bagian (*Annex A*) (Bilbao *et al*, 2011).

Dalam Indeks KAMI terdapat enam area target yang akan dievaluasi. Enam area ini dibagi ke dalam dua area besar yaitu satu area pada kategori sistem elektronik dan lima area pada keamanan informasi. Hal ini bertujuan untuk membangun, mengimplementasikan, mengoperasikan, mengamati, memelihara, dan meningkatkan keamanan informasi bagi suatu organisasi. Penerapan ISO/IEC 27001 memungkinkan organisasi atau perusahaan membandingkan persaingan dan memberikan informasi yang relevan tentang keamanan TI (Bilbao *et al*, 2011).

Tata kelola keamanan informasi yang baik dapat menandakan sikap perusahaan secara keseluruhan terhadap keamanan informasi risiko terutama untuk industri yang intensif informasi seperti lembaga keuangan (Fazlida & Jamaliah, 2015). Ketika kebutuhan untuk meningkatkan informasi secara efisien dan efektif maka diperlukan kontrol dan standarisasi termasuk metodologi *review* pengembangan sistem, peninjauan dokumentasi sistem, dan konfirmasi efektivitas kontrol hukum yang digunakan. Semua ini dilakukan oleh proses audit sistem dengan meninjau semua tahapan pengembangan sistem dan konfirmasi kontrol yang tepat serta identifikasi dan penerapannya. Hal ini dapat mengurangi biaya ekonomi sistem dan meningkatkan kualitas informasi yang disediakan oleh sistem. Selain itu dapat pula meningkatkan kemampuan sistem untuk beradaptasi dengan perubahan terbaru yang mengarah pada pencapaian tujuan utama (Alraja & Nayef, 2013).

Indeks KAMI dapat digunakan untuk menilai kematangan keamanan sistem informasi, seperti pada penelitian yang telah dilakukan oleh Basyarahil *et al* (2017) mengenai evaluasi manajemen keamanan informasi pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya. Penelitian ini dilakukan dengan menggunakan Indeks KAMI yang berdasarkan ISO/IEC 27001:2013. Hasil dari penelitian ini didapat tingkat ketergantungan sistem elektronik adalah sebesar 26 dari total skor keseluruhan adalah 50 sehingga dikategorikan Tinggi. Selain itu, dari penilaian kelima area yang telah dilakukan ini didapat 249 dari 645 dan berada pada kategori tidak layak

sehingga DPTSI ITS Surabaya belum dapat dikatakan matang dan sesuai dengan standar ISO/IEC 27001:2013 karena belum mencapai level III+ (penerapan keamanan informasi kemananan telah terdefinisi dan konsisten). Selain itu, indeks KAMI digunakan pula oleh Pratama *et al* (2018) untuk mengevaluasi tata kelola sistem keamanan teknologi informasi pada Kominfo Provinsi Jawa Timur. Hasil dari penelitian ini didapatkan bahwa tingkat kematangan setiap area keamanan informasi masih berada pada tingkat I+ yang berarti Kominfo masih dikatakan tidak layak untuk sertifikasi ISO 27001. Oleh karena itu dilakukan rekomendasi guna meningkatkan standar keamanan informasi yang ada.

Berdasarkan latar belakang di atas maka pada penelitian ini akan dilakukan Audit Keamanan Sistem Informasi Manajemen Daerah (SIMDA) Keuangan di Badan Keuangan Daerah Provinsi Lampung menggunakan Indeks KAMI Berdasarkan Standar ISO/IEC 27001. Dengan adanya penelitian ini diharapkan mampu memberikan rekomendasi terhadap peningkatan keamanan informasi pada SIMDA Keuangan di Badan Keuangan Daerah Provinsi Lampung.

B. Rumusan Masalah

Adapun rumusan masalah berdasarkan latar belakang di atas adalah sebagai berikut:

1. Bagaimanakah hasil audit keamanan sistem informasi pada SIMDA Keuangan menggunakan Indeks KAMI yang ada di Badan Keuangan Daerah Provinsi Lampung berdasarkan standar ISO/IEC 27001?

2. Bagaimana merumuskan rekomendasi perbaikan kebijakan dan prosedur sehingga dapat meningkatkan keamanan informasi di Badan Keuangan Daerah Provinsi Lampung?

C. Batasan Masalah

Adapun batasan masalah pada penelitian ini yaitu:

1. Audit dilakukan dengan menggunakan Indeks KAMI yang berdasar pada standar ISO/IEC 27001 meliputi dua area besar yaitu kategori sistem elektronik dan kategori keamanan informasi.
2. Data acuan yang digunakan adalah data hasil observasi, wawancara, dan kuesioner.
3. *Output* yang dihasilkan berupa tingkat kematangan keamanan informasi, temuan serta rekomendasi perbaikan dari hasil audit keamanan SIMDA Keuangan di Badan Keuangan Daerah Provinsi Lampung.

D. Tujuan Penelitian

Adapun tujuan yang ingin dicapai pada penelitian ini yaitu:

1. Melaksanakan audit keamanan sistem informasi pada SIMDA Keuangan menggunakan Indeks KAMI di Badan Keuangan Daerah Provinsi Lampung sesuai dengan standar ISO/IEC 27001.
2. Membuat rekomendasi perbaikan kebijakan dan prosedur berdasarkan hasil audit sehingga dapat meningkatkan keamanan informasi di Badan Keuangan Daerah Provinsi Lampung.

E. Manfaat

Adapun manfaat yang akan diperoleh dari penelitian ini adalah sebagai berikut:

1. Memahami audit keamanan sistem informasi pada SIMDA Keuangan di Badan Keuangan Daerah Provinsi Lampung sesuai dengan Indeks KAMI yang berdasar pada standar ISO/IEC 27001.
2. Menghasilkan dokumentasi hasil audit keamanan SIMDA Keuangan di Badan Keuangan Daerah Provinsi Lampung berdasarkan temuan hasil audit.
3. Memberikan rekomendasi perbaikan mengenai kebijakan dan prosedur yang akan meningkatkan keamanan informasi.

II. TINJAUAN PUSTAKA

A. Audit dan Keamanan Sistem Informasi

Menurut Messier *et al* (2014) audit merupakan proses yang sistematik dalam mengevaluasi data atau bukti secara objektif untuk menentukan tingkat kesesuaian dengan kriteria-kriteria yang ditetapkan dan mengkomunikasikan hasilnya dengan pihak-pihak yang berwenang. Audit sistem informasi merupakan audit secara khusus terhadap manajemen sumber daya informasi atau audit kehandalan sistem informasi berbasis teknologi informasi. Ini mengenai aspek-aspek: efektivitas (*effectiveness*), efisiensi (*efficiency*), dan ekonomis tidaknya unit fungsional sistem informasi pada suatu organisasi), *data integrity, saveguarding assets, realibility, confidentiality, availability*, dan *security* (Gondodiyoto, 2007). Audit sistem informasi bertujuan untuk menilai apakah pengendalian sistem informasi telah memberikan jaminan kerahasiaan dan ketersediaan informasi dalam hal pengamanan aset, apakah integritas data telah terjaga dengan baik, serta apakah sistem informasi telah efektif dalam mencapai tujuannya (Swastika dan Putra, 2016).

Keamanan sistem informasi dalam suatu organisasi memiliki strategi atau prinsip yang penting untuk melindungi kerahasiaan informasinya. Prinsip-prinsip itu diantaranya adalah integritas informasi (*integrity*), kerahasiaan

informasi (*confidentiality*), dan ketersediaan informasi (*availibility*). Prinsip integritas informasi merupakan konsistensi yang utuh dari setiap informasi yang ada. Prinsip kerahasiaan menurut ISO 17799 memiliki arti memastikan informasi hanya dapat diakses oleh orang yang memiliki wewenang atau orang yang memiliki otoritas. Prinsip ketersediaan informasi berarti kepastian tersedianya informasi pada saat yang dibutuhkan oleh orang yang berwenang untuk mengetahui atau mengakses data (Sutabri, 2012).

B. Sistem Informasi Manajemen Daerah

Sistem informasi manajemen atau SIM merupakan sistem berbasis komputer yang menyediakan informasi untuk para pengguna yang memiliki kebutuhan dan tujuan yang sama (Mcleod, 2010). Sistem Informasi Manajemen Daerah atau SIMDA adalah sistem informasi yang dikembangkan dengan tujuan untuk membantu pemerintah dalam pengelolaan keuangan secara efisien dan efektif sesuai dengan aturan yang ada mulai dari penyusunan anggaran, penatausahaan, hingga pertanggungjawaban APBD.

Tujuan adanya sistem informasi manajemen daerah diantaranya adalah:

1. Menyediakan *data base* mengenai kondisi di daerah yang terpadu baik dari aspek keuangan, aset daerah, kepegawaian/aparatur daerah maupun pelayanan publik yang dapat digunakan untuk penilaian kinerja instansi pemerintah daerah.

2. Menghasilkan informasi yang komprehensif, tepat dan akurat kepada manajemen pemerintah daerah. Informasi ini dapat digunakan sebagai bahan untuk mengambil keputusan.
3. Mempersiapkan aparat daerah untuk mencapai tingkat penguasaan dan pendayagunaan teknologi informasi yang lebih baik.
4. Memperkuat basis pemerintah daerah dalam melaksanakan otonomi daerah (BPKP, 2008).

C. SIMDA Keuangan

SIMDA Keuangan merupakan suatu program aplikasi yang bertujuan guna membantu pemerintah dalam mengelola keuangan secara terintegrasi di daerahnya. SIMDA Keuangan meliputi penganggaran, penatausahaan, serta akuntansi dan pelaporan. Adapun hasil dari SIMDA Keuangan adalah sebagai berikut:

1. Penganggaran

   Rencana Kerja Anggaran (RKA), RAPBD dan Rancangan Penjabaran APBD, APBD dan Penjabaran APBD beserta perubahannya, Dokumen Pelaksanaan Anggaran (DPA).

2. Penatausahaan

   Surat Penyediaan Dana (SPD), Surat Permintaan Pembayaran (SPP), Surat Perintah Membayar (SPM), SPJ, Surat Perintah Pencairan Dana (SP2D), Surat Tanda Setoran (STS), beserta register-register, dan formulir-formulir pengendalian anggaran lainnya.

3. Akuntansi dan Pelaporan

   Jurnal, Buku Besar, Buku Pembantu, Laporan Keuangan (Laporan Realisasi Anggaran, Laporan Arus Kas dan Neraca), Perda Pertanggungjawaban dan Penjabarannya (BPKP, 2008).

D. Standar ISO/IEC 27001:2013

ISO/IEC 27001:2013 menyediakan persyaratan untuk menetapkan, menerapkan, memelihara, dan meningkatkan sistem manajemen keamanan informasi dalam suatu organisasi. Standar ini juga mencakup persyaratan untuk penilaian dan penanganan risiko keamanan informasi yang disesuaikan dengan kebutuhan organisasi. Persyaratan yang ditetapkan dalam ISO/IEC 27001:2013 bersifat umum dan dimaksudkan untuk berlaku untuk semua organisasi, terlepas dari jenis, ukuran atau sifatnya (ISO, 2013).

ISO/IEC 27001 memiliki 10 klausul dan 114 kontrol keamanan generik yang dibagi menjadi 14 bagian (*Annex* A) yang bertujuan untuk membangun, mengimplementasikan, mengoperasikan, mengamati, memelihara dan meningkatkan keamanan informasi berdasarkan pendekatan manajemen risiko bagi suatu perusahaan (Bilbao *et al*, 2011).

Adapun 10 klausul yang ada pada standar ISO/IEC 27001 adalah sebagai berikut:

Tabel 1. Klausul ISO/IEC 27001

Klausul	Penjelasan
Klausul 0: Pendahuluan (*Introduction*)	Klausul ini menjelaskan bahwa urutan persyaratan yang disajikan dalam klausul tidak menunjukkan urutan pentingnya persyaratan yang ditetapkan atau urutan dalam implementasi.
Klausul 1: Ruang Lingkup (*Scope*)	Klausul ini menjelaskan bahwa ISO 27001:2013 merupakan persyaratan generik SMKI yang sesuai untuk berbagai jenis, skala dan karakeristik organisasi yang meliputi persyaratan untuk membangun, menerapkan, memelihara dan meningkatkan sistem manajemen keamanan informasi secara terus menerus sesuai konteks organisasi. Klausul ini juga menjelaskan bahwa ISO 27001:2013 menetapkan persyaratan untuk mengkaji dan menanggulangi risiko keamanan informasi sesuai kebutuhan organisasi.
Klausul 2: Rujukan Normatif (*Normative References*)	Klausul ini mencatumkan ISO 27000 *Information technology — Security techniques — Information security management systems — Overview and vocabulary* sebagai referensi untuk memahami istilah dan terminologi yang digunakan.
Klausul 3: Istilah dan Definisi (*Terms and definitions*)	Klausul ini tidak memuat definisi tetapi hanya mencantumkan ISO 27000 sebagai rujukan definisi.
Klausul 4: Konteks Organisasi (*Context of the organization*)	Klausul ini menetapkan konteks organisasi dan pengaruhnya terhadap SMKI. Persyaratan standar dimulai dengan langkah awal untuk mengidentifikasi semua masalah eksternal dan internal yang relevan dengan organisasi dan informasi yang ada dalam organisasi atau informasi yang dipercayakan kepada pihak ketiga.

Tabel 1. (Lanjutan)

Klausul	Penjelasan
Klausul 5: Kepemimpinan (*Leadership*)	Klausul ini membahas semua persyaratan tentang peran "manajemen puncak" atau pimpinan tertinggi dalam organisasi. Manajemen puncak dapat berupa satu atau sekelompok orang yang mengarahkan dan mengendalikan organisasi pada tingkat tertinggi. Manajemen puncak harus memastikan agar keamanan informasi tertanam dalam budaya organisasi, dan bahwa sumber daya yang memadai tersedia untuk mendukung SMKI serta menetapkan kebijakan dan sasaran keamanan.
Klausul 6: Perencanaan (*Planning*)	Klausul ini menguraikan bagaimana suatu organisasi merencanakan tindakan untuk mengatasi risiko dan peluang terkait penggunaan informasi. Persyaratan untuk mengidentifikasi aset informasi, ancaman, kerentanan, dan pemilik aset tidak lagi diperlukan. Tetapi penilaian dampak (*impact*), kemungkinan (*likehood*), kriteria penerimaan risiko dan identifikasi rencana penanggulangan (*risk treatment plan*) masih tetap dipersyaratkan.
Klausul 7: Dukungan (*Support*)	Klausul ini menjelaskan tentang mendapatkan sumber daya, SDM dan infrastruktur yang tepat untuk menetapkan, menerapkan, memelihara dan terus meningkatkan SMKI. Klausul ini menjelaskan persyaratan-persyaratan terkait kompetensi, kesadaran dan komunikasi untuk mendukung SMKI, termasuk kebutuhan melakukan pelatihan dan penyediaan SDM yang memadai.
Klausul 8: Operasi (*Operation*)	Klausul ini menjelaskan semua hal tentang pelaksanaan rencana dan proses yang merupakan subjek dari klausul sebelumnya. Persyaratan yang dicantumkan di klausul ini berkaitan dengan pelaksanaan tindakan yang ditentapkan dan pencapaian tujuan keamanan informasi. Klausul ini juga berkaitan dengan kinerja penilaian risiko keamanan informasi selama periode waktu tertentu, dan kebutuhan akan informasi terdokumentasi yang perlu dipelihara dan dipertahankan sebagai bukti implementasi SMKI.

Tabel 1. (Lanjutan) (Kominfo, 2017)

Klausul	Penjelasan
Klausul 9: Evaluasi Kinerja (*Performance evaluation*)	Klausul ini menjelaskan semua tentang pemantauan, pengukuran, analisis dan evaluasi SMKI untuk memastikan efektifitas, keberlakuan, dan kesesuaiannya dengan kondisi terkini yang ada. Klausul ini membantu organisasi untuk terus menilai bagaimana tingkat ketercapaian sasaran keamanan dengan penerapan sistem manajemen yang telah dilakukan serta bagaimana terus meningkatkan efektivitas SMKI.
Klausul 10: Peningkatan (*Improvement*)	Klausul ini menjelaskan bagian dari standar yang menetapkan persyaratan tindakan korektif. Organisasi harus menunjukkan bagaimana cara mengatasi adanya ketidaksesuaian, mengambil tindakan, memperbaikinya dan mengelola dampak yang ditimbulkannya. Klausul ini juga menetapkan persyaratan untuk menunjukkan adanya perbaikan berkesinambungan terhadap SMKI.

Sementara itu, *annex* A ini menjelaskan bagian dari standar yang menetapkan "sasaran kontrol" dan "kontrol" yang langsung diadopsi dari ISO 27002:2013 dan juga memberikan panduan praktik terbaik dan dapat digunakan sebagai referensi untuk memilih kontrol-kontrol mana yang paling cocok untuk diterapkan dalam suatu organisasi. Adapun 14 area kontrol pada *annex* A adalah sebagai berikut:

1. *A.5 Security Policies*

   A.5.1 Manajemen direction for information security

2. *A.6 Organisation of Information Security*

   A.6.1 Internal organization

   A.6.2 Mobile device and teleworking

3. *A.7 Human Resource Security*

   A.7.1 Screening

A.7.2 During employment

A.7.3 Termination and change of employment

4. *A.8 Asset Management*

A.8.1 Responsibility for assets

A.8.2 Information classification

A.8.3 Media handling

5. *A.9 Access Control*

A.9.1 Business requirement of access control

A.9.2 User access management

A.9.3 User responsibilities

A.9.4 System and application access control

6. *A.10 Cryptography*

A.10.1 Cryptographic controls

7. *A.11 Physical and Environmental Security*

A.11.1 Secure areas

A.11.2 Equipment

8. *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

9. *A.13 Communications Security*

   A.13.1 Network security management

   A.13.2 Information transfer

10. *A.14 Systems Acquisition, Development and Maintenance*

    A.14.1 Security requirements of information system

    A.14.2 Security in development and support processes

    A.14.3 Test data

11. *A.15 Supplier Relationships*

    A.15.1 Information security in supplier relationship

    A.15.2 Supplier service delivery management

12. *A.16 Information Security Incident Management*

    A.16.1 Management of information security incidents and improvement

13. *A.17 Information Security Aspects of Business Continuity Management*

    A.17.1 Information security continuity

14. *A.18 Compliance*

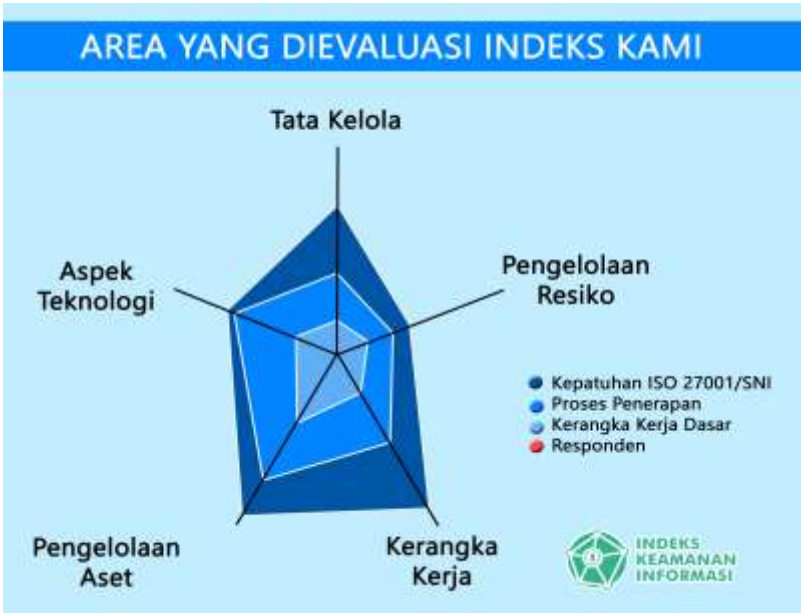
    A.18.1 Compiliance with legal and contractual requirements

    A.18.2 Information security reviews (Kominfo, 2017).

Secara internasional ISO/IEC 27001 diakui sebagai kerangka kerja yang sangat baik yang membantu organisasi mengelola dan melindungi aset informasi mereka sehingga tetap aman. Standar ini dapat membantu untuk melakukan peninjauan dan penyempurnaan keamanan sistem informasi.

E. Indeks Keamanan Informasi (KAMI)

Indeks KAMI (Keamanan Informasi) merupakan aplikasi yang dibuat oleh Badan Siber dan Sandi Negara (BSSN) yang digunakan sebagai alat bantu untuk menganalisa dan mengevalusi tingkat kesiapan (kelengkapan dan kematangan) penerapan keamanan informasi di sebuah organisasi, instansi pemerintah, organisasi berskala nasional, maupun yang berukuran kecil sesuai dengan kriteria pada SNI ISO/IEC 27001 (BSSN, 2015). Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh suatu organisasi dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya proses yang ada. Alat evaluasi ini merupakan perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi. Evaluasi dilakukan dengan ruang lingkup pembahasan yang juga memenuhi semua aspek yang didefinisikan oleh standar ISO 27001:2013.



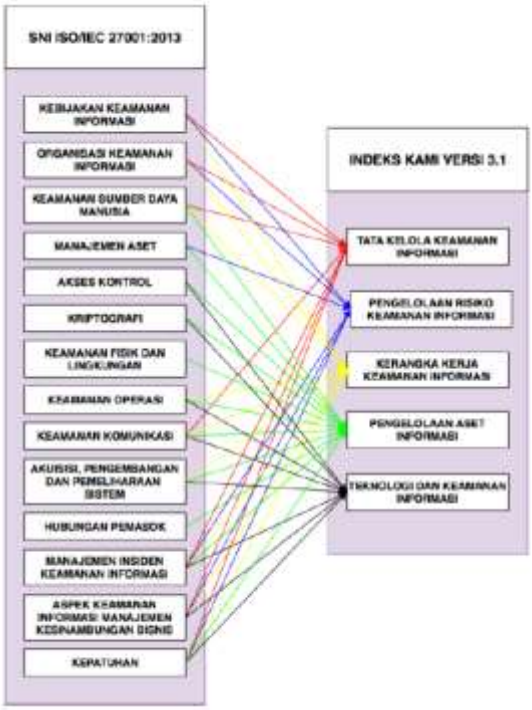
Gambar 1. Area Target Evaluasi Indeks KAMI (BSSN, 2015).

Dalam Indeks KAMI terdapat enam area target yang akan dievaluasi. Area-area ini dibagi ke dalam dua area besar yaitu area kategori sistem elektronik dan area keamanan informasi. Enam area target evaluasi adalah sebagai berikut:

1. Kategori Sistem Elektronik yang digunakan di Instansi.
2. Tata Kelola Keamanan Informasi.
3. Pengelolaan Risiko Keamanan Informasi.
4. Kerangka Kerja Keamanan Informasi.
5. Pengelolaan Aset Informasi.
6. Teknologi dan Keamanan Informasi (Kominfo, 2017).

F. Hubungan Indeks KAMI dengan ISO/IEC 27001

Dalam menentukan status keamanan informasi dan tingkat kepatuhan suatu organisasi, digunakan alat evaluasi tingkat keamanan yang berdasar pada standar ISO 27001 yang dikenal sebagai Indeks Keamanan Informasi (KAMI). Dalam penggunaannya, enam area keamanan informasi pada indeks KAMI telah mencakup kontrol-kontrol yang ada pada standar ISO 27001 dimana dalam sebuah area keamanan terdiri dari beberapa kontrol ISO 27001. Berikut merupakan diagram hubungan indeks KAMI dengan standar ISO 27001.



Gambar 2. Hubungan Indeks KAMI dengan Standar ISO 27001:2013 (Pratama *et al.*, 2018).

Adapun hubungan antara indeks KAMI dengan standar ISO/IEC 27001 yang telah dipetakan adalah sebagai berikut:

Tabel 2. Pemetaan Indeks KAMI dengan Standar ISO/IEC 27001

No	Area Keamanan Indeks KAMI	Area Kontrol ISO/IEC 27001
1	Tata Kelola Keamanan Informasi	• Kebijakan Keamanan Informasi • Organisasi Keamanan Informasi • Keamanan Sumber Daya Manusia • Keamanan Komunikasi • Manajemen Insiden Keamanan Informasi • Aspek Keamanan Informasi Manajemen Kesinambungan Bisnis • Kepatuhan

Tabel 2. (Lanjutan)

No	Area Keamanan Indeks KAMI	Area Kontrol ISO/IEC 27001
2	Pengelolaan Risiko Keamanan Informasi	• Kebijakan Keamanan Informasi • Organisasi Keamanan Informasi • Manajemen Aset • Manajemen Insiden Keamanan Informasi • Aspek Keamanan Informasi Manajemen Kesinambungan Bisnis • Kepatuhan
3	Kerangka Kerja Keamanan Informasi	• Kebijakan Keamanan Informasi • Organisasi Keamanan Informasi • Keamanan Sumber Daya Manusia • Keamanan Operasi • Keamanan Komunikasi • Akuisisi, Pengembangan, dan Pemeliharaan Sistem • Manajemen Insiden Keamanan Informasi • Aspek Keamanan Informasi Manajemen Kesinambungan Bisnis • Kepatuhan
4	Pengelolaan Aset Informasi	• Keamanan Sumber Daya Manusia • Manajemen Aset • Akses Kontrol • Kriptografi • Keamanan Lingkungan dan Fisik • Keamanan Operasi • Keamanan Komunikasi • Akuisisi, Pengembangan, dan Pemeliharaan Sistem • Hubungan Pemasok • Manajemen Insiden Keamanan Informasi • Kepatuhan

Tabel 2. (Lanjutan)

No	Area Keamanan Indeks KAMI	Area Kontrol ISO/IEC 27001
5	Teknologi dan Keamanan Informasi	• Akses Kontrol • Kriptografi • Keamanan Operasi • Keamanan Komunikasi • Akuisisi, Pengembangan, dan Pemeliharaan Sistem • Manajemen Insiden Keamanan Informasi • Aspek Keamanan Informasi Manajemen Kesinambungan Bisnis • Kepatuhan

G. Gambaran Umum Perusahaan

1. Profil Perusahaan

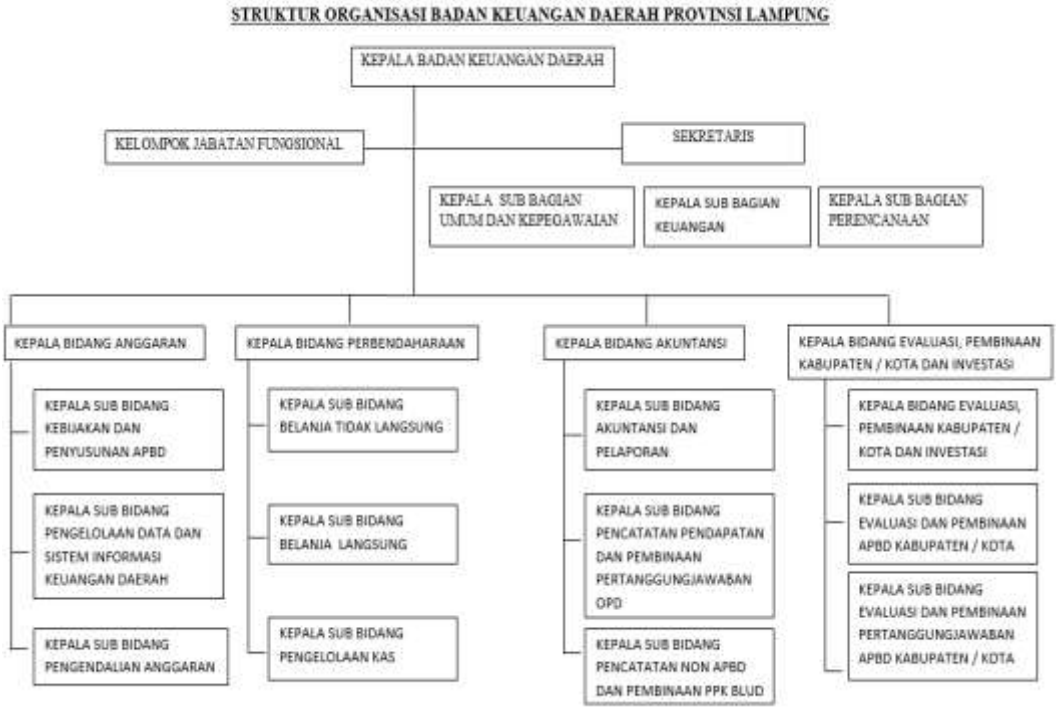
Badan Keuangan Daerah merupakan unsur pelaksana fungsi penunjang urusan pemerintahan bidang keuangan daerah yang menjadi kewenangan daerah provinsi. Badan Keuangan Daerah mempunyai tugas untuk membantu Gubernur melaksanakan fungsi penunjang Urusan Pemerintahan bidang keuangan daerah provinsi berdasarkan asas otonomi dan tugas lain sesuai dengan kebijakan yang ditetapkan oleh Gubernur berdasarkan peraturan perundang-undangan yang berlaku. Adapun fungsi yang mendukung pelaksanaan tugas dari Badan Keuangan Daerah adalah sebagai berikut:

1. Penyusunan kebijakan teknis di bidang keuangan daerah
2. Pelaksanaan tugas dukungan teknis di bidang keuangan daerah

3. Pemantauan, evaluasi, dan pelaporan pelaksanaan tugas dukungan teknis di bidang keuangan daerah
4. Pembinaan teknis penyelenggaraan fungsi penunjang Urusan Pemerintahan Daerah provinsi bidang keuangan daerah
5. Pelaksanaan fungsi lain yang diberikan oleh gubernur sesuai dengan tugas dan fungsinya (Rencana Strategis Badan Keuangan Daerah Provinsi Lampung, 2017).

2. Struktur Organisasi

Adapun struktur organisasi yang ada pada Badan Keuangan Daerah Provinsi Lampung adalah sebagai berikut:



Gambar 3. Struktur Organisasi Badan Keuangan Daerah (Rencana Strategis Badan Keuangan Daerah Provinsi Lampung, 2017).

3. Visi dan Misi Badan Keuangan Daerah

Visi Badan Pengelola Keuangan Daerah dirumuskan untuk mendukung visi dan misi Provinsi Lampung, secara dimensional pernyataan visi berfokus kemasa depan berdasarkan pemikiran masa kini dan pengalaman masa lalu. Upaya untuk mewujudkan keberhasilan visi ini tentunya sangat ditentukan oleh kinerja dan peran aparatur. Badan Keuangan Daerah Provinsi Lampung berkeinginan agar setiap aparatur mempunyai kemampuan melaksanakan tugasnya, lebih maju berdayaguna dan berhasilguna yang didukung dengan Kelembagaan Perangkat Daerah yang efektif dan efisien. Hal ini bertujuan untuk mewujudkan pelayanan yang prima sesuai dengan sistem dan prosedur pengeloaan keuangan serta standar operasional dan prosedur (SOP). Visi yang tercantum dalam Rencana Pembangunan Jangka Panjang (RPJMD) Provinsi Lampung tahun 2015-2019 yaitu:

"LAMPUNG MAJU DAN SEJAHTERA 2019"

Filosofi maju mempunyai arti modern, yang mencakup kemajuan sosial ekonomi, Ilmu Pengetahuan dan Teknologi, politik dan hukum.Perekonomian yang berbasis industri, didukung oleh perdagangan barang dan jasa, peningkatan pendapatan masyarakat dengan konsep ekonomi kerakyatan yang seimbang dengan pertumbuhan penduduk.

Untuk mewujudkan Visi Pembangunan Jangka Menengah Provinsi Lampung Tahun 2015-2019, dirumuskan lima misi sebagai berikut:

1. Meningkatkan pembangunan ekonomi dan memperkuat kemandirian daerah.

2. Meningkatkan infrastruktur untuk pengembangan ekonomi dan pelayanan sosial.
3. Meningkatkan kualitas pendidikan, kesehatan, budaya masyarakat, dan toleransi kehidupan beragama.
4. Meningkatkan pelestarian sumber daya alam dan kualitas lingkungan hidup yang berkelanjutan.
5. Menegakkan supremasi hukum, mengembangkan demokrasi berbasis kearifan lokal, dan memantapkan kepemerintahan yang baik dan antisipatif.

Badan Keuangan Daerah Provinsi Lampung memiliki tugas dalam rangka pencapaian visi kepala daerah dan mengampu misi kelima dengan tujuan pembangunan **"Memperkuat Kapasitas Manajemen Birokrasi"** (Rencana Strategis Badan Keuangan Daerah Provinsi Lampung, 2017).

4. Tujuan dan Sasaran Badan Keuangan Daerah

Dalam rangka merealisasikan pencapaian visi dan misi, tujuan dan sasaran kepala daerah yang ditetapkan dalam RPJMD Provinsi Lampung Tahun 2015-2019, maka dirumuskan langkah-langkah operasional yang lebih terarah dalam bentuk penetapan tujuan dan sasaran. Adapun tujuan dari Badan Keuangan Daerah adalah sebagai berikut:

1. Terwujudnya pengelolaan keuangan daerah yang berkualitas, transparan dan akuntabel.
2. Terwujudnya sistem informasi manajemen pengelolaan keuangan yang terintegrasi.

3. Terciptanya Optimalisasi Kinerja BUMD.
4. Terciptanya SDM berkualitas dan profesionalisme dalam pengelolaan keuangan daerah.

Adapun sasaran dari Badan Keuangan Daerah adalah sebagai berikut:

1. Terciptanya Tertib Administrasi Keuangan yang baik dan efisien dalam Pengelolaan Anggaran Pendapatan dan Belanja Daerah.
2. Penyusunan laporan keuangan daerah tepat waktu dengan penerapan standar akuntansi pemerintah (SAP).
3. Peningkatan pemanfaatan Sistem Informasi manajemen keuangan daerah dalam proses pengelolaan keuangan daerah.
4. Meningkatnya kinerja BUMD.
5. Terciptanya SDM yang handal (Rencana Strategis Badan Keuangan Daerah Provinsi Lampung, 2017).

III. METODOLOGI PENELITIAN

A. Waktu dan Tempat Penelitian

Penelitian ini dilakukan di kantor Badan Keuangan Daerah bidang Anggaran sub bidang Data dan Sistem Informasi Provinsi Lampung yang berada di Jalan Wolter Monginsidi No. 69 Teluk Betung, Bandar Lampung. Penelitian ini dilaksanakan pada semester genap tahun ajaran 2018/2019.

Tabel 3. Jadwal Penelitian

No.	Kegiatan	Bulan					
		Februari	Maret	April	Mei	Juni	Juli
1	Perumusan Masalah						
2	Studi Literatur						
3	Pengumpulan Data						
4	Penilaian dengan Indeks KAMI						
5	Analisis Data Hasil Evaluasi dengan Indeks KAMI						
6	*Risk Assessment* (Analisis Risiko)						
7	Pembuatan Saran dan Rekomendasi Perbaikan Keamanan Informasi						
8	Penyusunan Laporan Akhir						

B. Alat Pendukung Penelitian

Penelitian ini membutuhkan alat yang dapat mendukung pelaksanaan penelitian. Untuk itu, alat pendukung yang digunakan dalam penelitian ini adalah sebagai berikut:

1. Perangkat Keras (*Hardware*)

   Adapun perangkat keras (*hardware*) yang digunakan pada penelitian ini yaitu sebuah laptop dengan spesifikasi sebagai berikut:

   a. *Processor*: Intel(R) Core(TM) i5-5200U CPU @ 2.20GHz, 2195 Mhz, 2 Core(s), 4 Logical Processor(s)
   b. *Installed Physical Memory* (RAM): 8,00 GB
   c. *System Type*: x64-based PC

2. Perangkat Lunak (*Software*)

   Adapun perangkat lunak (*software*) yang digunakan pada penelitian ini adalah sebagai berikut:

   a. Sistem operasi Windows 10
   b. *Web Browser (Google Chrome)*

C. Sumber Data

Pada penelitian ini data yang digunakan adalah informasi tentang kepatuhan pada pelaksanaan keamanan sistem informasi manajemen. Adapun sumber data yang dibutuhkan terdiri dari dua jenis yaitu:

a. Data Primer

   Data primer didapatkan melalui observasi, wawancara, dan kuesioner yang berkaitan dengan keamanan sistem informasi. Pelaksanaan

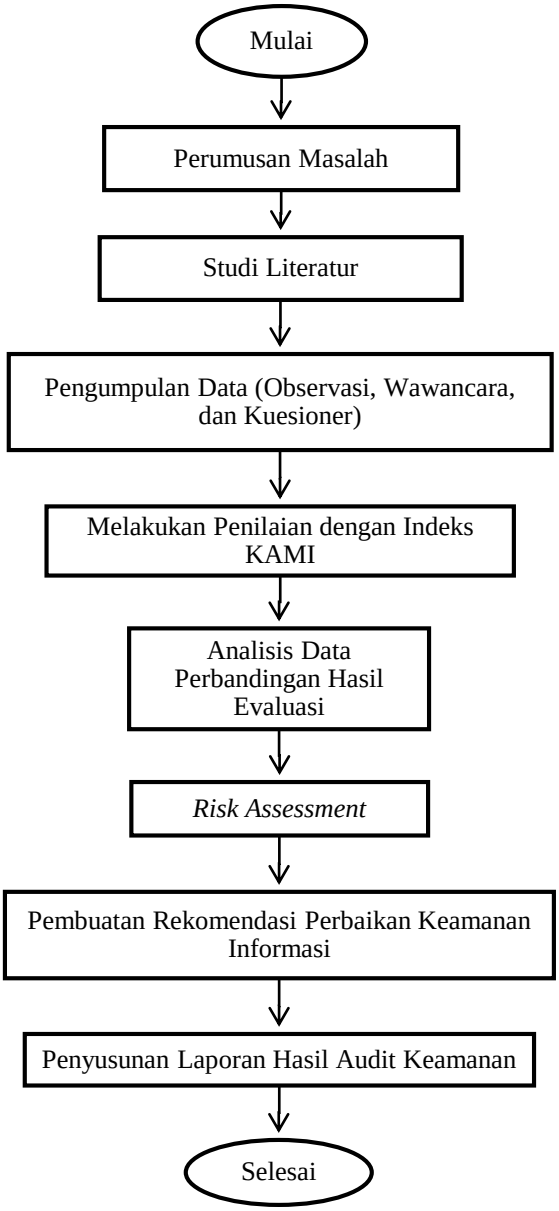
pengambilan data dari observasi, wawancara, dan pengisian kuesioner dengan Indeks KAMI oleh narasumber yang terkait dengan bidang TI yang telah dipilih di Badan Keuangan Daerah Provinsi Lampung.

b. Data Sekunder

Data sekunder diperoleh dari informasi pendukung yang berupa dokumen *softcopy* terkait dengan rencana strategis (Renstra), rencana kerja, serta gambaran umum Badan Keuangan Daerah.

D. Metode Penelitian

Adapun metode penelitian yang digunakan pada audit keamanan sistem informasi manajemen keuangan menggunakan Indeks KAMI berdasarkan standar ISO/IEC 27001 ini dapat dilihat pada gambar berikut.



Gambar 4. Metodologi Penelitian.

1. Perumusan Masalah

Perumusan masalah merupakan tahap awal yang dilakukan pada penelitian ini. Pada tahap ini, dirumuskan masalah yang akan dibahas dalam penelitian, penentuan ruang lingkup audit, dan penyusunan audit *working plan*. Dalam hal ini topik permasalahannya adalah seputar keamanan sistem informasi.

Keamanan sistem informasi merupakan hal yang penting bagi suatu organisasi. Oleh karena itu, diperlukan audit untuk mengetahui tingkat keamanan pada sistem informasi. Audit keamanan sistem informasi manajemen keuangan di Badan Keuangan Daerah Provinsi Lampung pada penelitian ini menggunakan Indeks KAMI berdasarkan standar ISO/IEC 27001.

2. Studi Literatur

Pada tahap ini, studi literatur diambil dari berbagai sumber seperti buku, jurnal, dan *web* resmi organisasi yang berhubungan dengan penelitian ini. Selain itu, standar-standar *checklist* terkait keamanan sistem informasi juga dijadikan sebagai studi literatur pada penelitian ini.

3. Pengumpulan Data dan Penilaian dengan Indeks KAMI

Dalam proses pengumpulan data dilakukan dengan tiga cara yaitu wawancara, kuesioner, dan observasi. Wawancara dilakukan pada kunjungan langsung di badan keuangan daerah dengan mewawancarai narasumber yang berhubungan dengan penelitian ini. Observasi dilakukan dengan mengidentifikasi kondisi *existing* pengelolaan keamanan sistem informasi pada organisasi. Setelah didapat data-data terkait keamanan sistem informasi, dilakukan pemeriksaan kelengkapan dokumen seperti kebijakan dan prosedur keamanan informasi. Kuesioner dilakukan pada unit-unit kerja yang akan diaudit dengan membagikan kuesioner berisi beberapa pertanyaan yang berkaitan dengan keamanan sistem informasi yang ada pada Indeks KAMI.

Pada tahap pengumpulan data juga dilakukan penilaian dengan Indeks KAMI. Penilaian dilakukan dengan wawancara dan observasi serta mengisi pertanyaan-pertanyaan yang ada pada Indeks KAMI. Penilaian dilakukan pada dua area besar yaitu pada area Sistem Elektronik dan area Keamanan Informasi. Pertanyaan dikategorikan berdasarkan tingkat kesiapan penerapan pengamanan sesuai dengan kelengkapan kontrol yang diminta oleh standar ISO/IEC 27001:2013.

Responden diminta untuk memberi tanggapan mulai dari area sistem elektronik dan area keamanan informasi.

Adapun nilai yang diberikan untuk jawaban pertanyaan sesuai tingkat kematangannya adalah sebagai berikut:

Tabel 4. Skala Penilaian dengan Indeks KAMI (Kominfo, 2017)

Kategori Sistem Elektronik			
Status Ketergantungan TIK	Skor		
Rendah (C)	1		
Tinggi (B)	2		
Strategis (A)	5		
Kategori Pengamanan			
Status Pengamanan	Kategori Pengamanan		
	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan secara Menyeluruh	3	6	9

Adapun pada kategori sistem elektronik, status ketergantungan TIK memiliki definisi yang berbeda yaitu:

a. "Rendah", apabila TIK sudah digunakan untuk mendukung proses kerja, namun belum pada tingkat yang signifikan.
b. "Tinggi", apabila TIK sudah menjadi bagian yang tidak terpisahkan dari proses kerja yang berjalan.
c. "Strategis", apabila TIK merupakan satu-satunya cara untuk menjalankan proses kerja yang bersifat strategis atau berskala nasional.

Selain itu, pada area keamanan informasi juga terdapat tiga kategori pengamanan yang memiliki definisi berbeda yaitu kategori pengamanan 1 terkait dengan bentuk kerangka kerja dasar keamanan informasi, kategori pengamanan 2 terkait efektifitas dan konsistensi penerapannya, dan kategori pengamanan 3 terkait kemampuan untuk selalu meningkatkan kinerja keamanan informasi. Namun, untuk pertanyaan kategori pengamanan 3 hanya dapat diisi apabila semua pertanyaan pada kategori pengamanan 1 dan 2 sudah diisi dengan status pengamanan minimal “Diterapkan Sebagian”. Setiap jawaban diberikan nilai yang kemudian dikonsolidasi untuk menghasilkan angka indeks yang digunakan untuk menampilkan hasil evaluasi (Kominfo, 2017).

Pada pengumpulan data yang berupa kuesioner terbagi menjadi enam bagian besar yang ada pada dua area besar yaitu satu bagian kategori sistem informasi dan lima bagian kategori keamanan informasi. Berikut merupakan pertanyaan-pertanyaan yang ada pada kuesioner yang akan diberikan kepada responden.

Tabel 5. Kuesioner Indeks KAMI

Bagian I: Kategori Sistem Elektronik	
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan	
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis	
#	**Karakteristik Instansi**
1,1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar
1,2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C] Kurang dari Rp.1 Miliar
1,3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus
1,4	Menggunakan algoritma khusus untuk keamanan informasi dalam Sistem Elektronik [A] Algoritma khusus yang digunakan Negara [B] Algoritma standar publik [C] Tidak ada algoritma khusus
1,5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna
1,6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi
1,7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/ atau Terbatas [C] Biasa
1,8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang tidak berdampak bagi kepentingan orang banyak

Tabel 5. (Lanjutan)

Bagian I: Kategori Sistem Elektronik			
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan			
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis			
#	**Karakteristik Instansi**		
1,9	Dampak dari kegagalan Sistem Elektronik [A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik atau proses penyelenggaraan negara dalam 1 provinsi atau lebih [C] Tidak tersedianya layanan publik atau proses penyelenggaraan negara dalam 1 kabupaten/kota atau lebih		
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan merugikan finansial)		
Bagian II: Tata Kelola Keamanan Informasi			
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
#			**Fungsi/Instansi Keamanan Informasi**
2,1	II	1	Apakah pimpinan Instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?
2,2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?
2,3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?
2,4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?
2,5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?
2,6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?
2,7	II	1	Apakah semua pelaksana pengamanan informasi di Instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?

Bagian II: Tata Kelola Keamanan Informasi			
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
#			**Fungsi/Instansi Keamanan Informasi**
2,8	II	1	Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?
2,9	II	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?
2.10	II	2	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?
2.11	II	2	Apakah instansi anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?
2.12	II	2	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?
2.13	II	2	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?
2.14	III	2	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?
2.15	III	2	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan Instansi secara rutin dan resmi?
2.16	III	2	Apakah kondisi dan permasalahan keamanan informasi di Instansi anda menjadi konsideran atau bagian dari proses pengambilan keputusan strategis di Instansi anda?
2.17	IV	3	Apakah pimpinan satuan kerja di Instansi anda menerapkan program khusus untuk mematuhi tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?
2.18	IV	3	Apakah Instansi anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?

Tabel 5. (Lanjutan)

Bagian II: Tata Kelola Keamanan Informasi			
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
#			**Fungsi/Instansi Keamanan Informasi**
2.19	IV	3	Apakah Instansi anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?
2.20	IV	3	Apakah Instansi anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan Instansi?
2.21	IV	3	Apakah Instansi anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?
2.22	IV	3	Apakah Instansi anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?
Bagian III: Pengelolaan Risiko Keamanan Informasi			
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
#			**Kajian Risiko Keamanan Informasi**
3,1	II	1	Apakah Instansi anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?
3,2	II	1	Apakah Instansi anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?
3,3	II	1	Apakah Instansi anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?
3,4	II	1	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi anda?
3,5	II	1	Apakah Instansi anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?
3,6	II	1	Apakah Instansi anda sudah mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?

Tabel 5. (Lanjutan)

Bagian III: Pengelolaan Risiko Keamanan Informasi			
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
#			**Kajian Risiko Keamanan Informasi**
3,7	II	1	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?
3,8	II	1	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?
3,9	II	1	Apakah Instansi anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?
3.10	II	1	Apakah Instansi anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?
3.11	III	2	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?
3.12	III	2	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?
3.13	IV	2	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?
3.14	IV	2	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?
3.15	V	3	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?
3.16	V	3	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?

Tabel 5. (Lanjutan)

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi			
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
#			**Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi**
4,1	II	1	Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggungjawab pihak-pihak yang diberikan wewenang untuk menerapkannya?
4,2	II	1	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?
4,3	II	1	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?
4,4	II	1	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?
4,5	II	1	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyetif tertentu yang ditetapkan oleh pimpinan Instansi?
4,6	II	1	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?
4,7	II	1	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?
4,8	II	2	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?
4,9	II	2	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak-lanjuti konsekwensi dari kondisi ini?
4.10	III	2	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggungjawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?
4,11	III	2	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?

Tabel 5. (Lanjutan)

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi			
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
#		**Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi**	
4,12	III	2	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?
Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi			
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
#		**Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi**	
4,13	III	2	Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman *(Secure SDLC)* dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?
4,14	III	2	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?
4,15	III	2	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya?
4,16	III	3	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?
4.17	III	3	Apakah uji-coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?
4.18	IV	3	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plan*) dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan (misal, apabila hasil uji-coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?
4.19	IV	3	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?

Tabel 5. (Lanjutan)

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi			
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
#	**Pengelolaan Strategi dan Program Keamanan Informasi**		
4.20	II	1	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?
4,21	II	1	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?
4.22	III	1	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?
4,23	III	1	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?
4,24	III	1	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektifitas penerapan keamanan informasi?
4.25	III	2	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?
4,26	III	2	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?
4,27	IV	3	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?
4,28	V	3	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah pembenahan yang diperlukan, telah diterapkan secara efektif?

Tabel 5. (Lanjutan)

Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi			
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
#			**Pengelolaan Strategi dan Program Keamanan Informasi**
4,29	V	3	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?
Bagian V: Pengelolaan Aset Informasi			
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
#			**Pengxzelolaan Aset Informasi**
5,1	II	1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terperlihara ? (termasuk kepemilikan aset)
5,2	II	1	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?
5,3	II	1	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya?
5,4	II	1	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matrix yang merekam alokasi akses tersebut?
5,5	II	1	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?
5,6	II	1	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?
5,7	II	1	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?
			Apakah Instansi anda memiliki dan menerapkan perangkat di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?
5,8	II	1	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di Instansi anda
5,9	II	1	Tata tertib penggunaan komputer, email, internet dan intranet
5.10	II	1	Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI
5.11	II	1	Peraturan terkait instalasi piranti lunak di aset TI milik instansi
5.12	II	1	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi

Tabel 5. (Lanjutan)

Bagian V: Pengelolaan Aset Informasi			
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
#			**Pengelolaan Aset Informasi**
5.13	II	1	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya
5.14	II	1	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi
5.15	II	1	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data
5.16	II	1	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya
5.17	II	1	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi
5.18	II	1	Prosedur *back-up* dan ujicoba pengembalian data (*restore*) secara berkala
5.19	II	2	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya
5.20	III	2	Proses pengecekan latar belakang SDM
5.21	III	2	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.
5.22	III	2	Prosedur penghancuran data/aset yang sudah tidak diperlukan
5.23	III	2	Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya *(user access rights*) berikut langkah pembenahan apabila terjadi ketidak sesuaian (*non-conformity*) terhadap kebijakan yang berlaku
5.24	III	2	Prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.
5.25	III	3	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?
5.26	III	3	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?
5.27	III	3	Apakah tersedia prosedur penggunaan perangkat pengolah informasi milik pihak ketiga (termasuk perangkat milik pribadi dan mitra kerja/vendor) dengan memastikan aspek HAKI dan pengamanan akses yang digunakan?
#			**Pengamanan Fisik**
5.28	II	1	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?
5.29	II	1	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?

Tabel 5. (Lanjutan)

Bagian V: Pengelolaan Aset Informasi			
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
#			**Pengamanan Fisik**
5.30	II	1	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?
5.31	II	1	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?
5.32	II	1	Apakah tersedia peraturan pengamanan perangkat komputasi milik Instansi anda apabila digunakan di luar lokasi kerja resmi (kantor)?
5.33	II	1	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (dalam daftar inventaris)
5.34	II	2	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?
5.35	II	2	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?
5.36	II	2	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?
5.37	II	2	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)
5.38	III	3	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan Instansi anda?

Tabel 5. (Lanjutan)

Bagian VI: Teknologi dan Keamanan Informasi			
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
#			**Pengamanan Teknologi**
6,1	II	1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?
6,2	II	1	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian Instansi, kebutuhan aplikasi, jalur akses khusus, dll)?
6,3	II	1	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?
6,4	II	1	Apakah Instansi anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?
6,5	II	1	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?
6,6	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?
6,7	II	1	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?
6,8	II	1	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?
6,9	II	1	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?
6.10	II	1	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?
6.11	II	1	Apakah Instansi anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?
6.12	III	2	Apakah Instansi anda mempunyai standar dalam menggunakan enkripsi?
6.13	III	2	Apakah Instansi anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?
6.14	III	2	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?
6.15	III	2	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?
6.16	III	2	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*,dan penarikan akses?

Tabel 5. (Lanjutan)

Bagian VI: Teknologi dan Keamanan Informasi			
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
#			**Pengamanan Teknologi**
6.17	III	2	Apakah Instansi anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?
6.18	II	1	Apakah Instansi anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar Instansi?
6.19	II	1	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?
6.20	II	1	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?
6.21	III	2	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?
6.22	III	2	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?
6.23	III	2	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?
6.24	III	2	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji-coba?
6.25	III	3	Apakah instansi ada menerapkan lingkungan pengembangan dan uji-coba yang sudah diamankan sesuai dengan standar platform teknologi yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?
6.26	IV	3	Apakah Instansi anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?

4. Analisis Data Hasil Perbandingan Evaluasi Indeks KAMI

Pada tahap ini, analisis data dilakukan untuk mengetahui apakah kontrol-kontrol ISO/IEC 27001 telah diterapkan dengan baik di organisasi. Data yang dibandingkan adalah nilai hasil evaluasi dengan indeks KAMI oleh responden dan nilai maksimum yang telah ditetapkan oleh indeks KAMI. Analisis dilakukan dilakukan dengan berdasar pada *checklist* hasil wawancara,

observasi, kuesioner maupun dokumen-dokumen yang telah dikumpulkan yang berhubungan dengan keamanan sistem informasi.

Terdapat definisi nilai tingkat kematangan keamanan informasi dalam analisis *gap* berdasarkan klausul ISO/IEC 27001 pada indeks KAMI, yaitu:

Tabel 6. Capaian Tingkat dan Kondisi Kematangan Keamanan Informasi

Tingkat	Kondisi
I	Kondisi Awal
II	Penerapan Kerangka Kerja Dasar
III	Terdefinisi dan Konsisten
IV	Terkelola dan Terukur
V	Optimal

Untuk membantu memberikan uraian yang lebih detail, terdapat penambahan tingkatan antara tingkat I+, II+, III+, dan IV+, sehingga total terdapat sembilan tingkatan kematangan. Sebagai awal, semua responden akan diberikan kategori kematangan tingkat I. Penentuan ambang batas pencapaian suatu tingkat kematangan ditentukan berdasarkan perumusan di bawah ini:

1. Tingkat Kematangan I: Tidak ada ambang batas minimum diasumsikan semua responden diberikan status ini pada saat dimulainya evaluasi.
2. Tingkat Kematangan I+ mencapai minimal, jika:
   a. Empat bentuk pengamanan TK.II-Tahap 1 dengan status "Dalam Penerapan/Diterapkan Sebagian".
   b. Sisa jumlah pengamanan TK.II-Tahap 1 yang ada dengan status "Sedang Direncanakan".
3. Tingkat Kematangan II mencapai minimal, jika:
   a. Seluruh bentuk pengamanan TK.II-Tahap 1 dengan status "Dalam Penerapan/Diterapkan Sebagian".

b. Seluruh bentuk pengamanan TK.II-Tahap 2 dengan status "Dalam Penerapan/Diterapkan Sebagian".

4. Tingkat Kematangan II+ mencapai minimal, jika:

a. Prasyarat Dasar TK.II+, yaitu mencapai nilai total bentuk pengamanan Tingkat Kematangan Il> (80% dari nilai seluruh bentuk pengamanan TK.I-Tahap 1 & 2 dengan status "Diterapkan Secara Menyeluruh").

b. Seluruh bentuk pengamanan TK.Ill-Tahap 1 dengan status "Diterapkan Secara Menyeluruh".

c. Dua bentuk pengamanan TK.III-Tahap 2 dengan status "Sedang Direncanakan".

d. Sisa jumlah pengamanan TK.III-Tahap 2 yang ada dengan status "Dalam Penerapan/Diterapkan Sebagian".

e. Satu bentuk pengamanan TK.II-Tahap 3 dengan status "Sedang Direncanakan".

f. Sisa jumlah pengamanan TK.III-Tahap 3 dengan status "Dalam Penerapan/Diterapkan Sebagian".

5. Tingkat Kematangan III mencapai minimal, jika:

a. Prasyarat Dasar TK.II+.

b. Seluruh bentuk pengamanan TK.III-Tahap 1 dengan status "Diterapkan Secara Menyeluruh".

c. Dua bentuk pengamanan TK.III-Tahap 2 dengan status "Dalam Penerapan/Diterapkan Sebagian".

d. Sisa jumlah pengamanan TK.III-Tahap 2 yang ada dengan status "Diterapkan Secara Menyeluruh".

e. Dua bentuk pengamanan TK.III-Tahap 3 dengan status Dalam Penerapan/Diterapkan Sebagian".

6. Tingkat Kematangan III+ mencapai minimal, jika:

a. Prasyarat Dasar TK. III.

b. Seluruh bentuk pengamanan TK.III-Tahap 1 dengan status "Diterapkan Secara Menyeluruh".

c. Sisa jumlah pengamanan TK.III-Tahap 2 yang ada dengan status "Diterapkan Secara Menyeluruh".

d. Satu bentuk pengamanan TK.III-Tahap 3 dengan status "Dalam Penerapan/Diterapkan Sebagian".

e. Sisa jumlah pengamanan TK.III-Tahap 3 yang ada dengan status "Diterapkan Secara Menyeluruh".

f. Dua bentuk pengamanan TK..IV-Tahap 3 dengan status Dalam Penerapan/Diterapkan Sebagian".

g. Sisa jumlah pengamanan TK.IV-Tahap 3 yang ada dengan status "Diterapkan Secara Menyeluruh".

7. Tingkat Kematangan IV mencapai minimal, jika:

a. Prasyarat Dasar TK.II+.

b. Seluruh bentuk pengamanan TK.IV-Tahap 3 dengan status "Diterapkan Secara Menyeluruh".

8. Tingkat Kematangan IV+ mencapai minimal, jika:

a. Mencapai Tingkat Kematangan IV.

b. Satu bentuk pengamanan TK.V-Tahap 3 dengan status "Dalam Penerapan/Diterapkan Sebagian”.

9. Tingkat Kematangan V mencapai minimal, jika:

a. Mencapai Tingkat Kematangan IV.

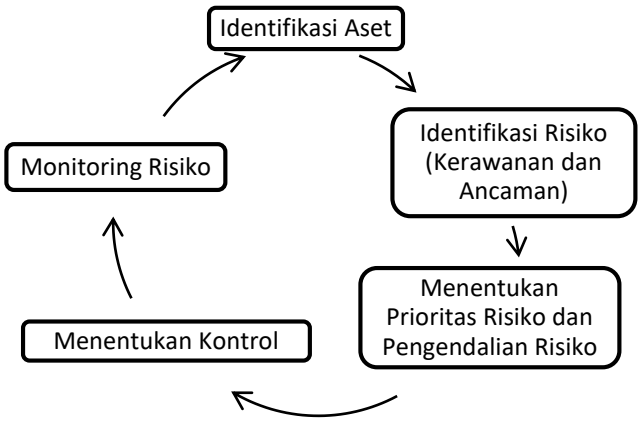
b. Seluruh bentuk pengamanan TK.V-Tahap 3 dengan status “Diterapkan Secara Menyeluruh”.

Berdasarkan indeks KAMI, tingkat kematangan yang diharapkan untuk ambang batas minimum adalah Tingkat III+.

Gambar 5. Rentang Tingkat Kematangan Keamanan Informasi (Kominfo, 2017).

5. *Risk Assessment*

Risk Assessment atau penilaian risiko dilakukan untuk mengetahui risiko yang mungkin muncul dari tahap sebelumnya, seperti risiko ancaman pada keamanan sistem informasi. Terdapat lima tahapan dalam *risk assessment* yaitu:



Gambar 6. Alur Proses *Risk Assessment*

1. Identifikasi aset. Tahap ini dilakukan identifikasi aset TI yang mendukung penyelenggaraan layanan terkait dengan teknologi infomasi yang ada pada organisasi. Aset yang diidentifikasi berupa aset perangkat lunak (*software*), aset perangkat keras (*hardware*), aset jaringan, dan aset lain-lain yang mendukung keamanan informasi.
2. Identifikasi kerawanan dan ancaman (analisis risiko). Analisis risiko dilakukan setelah tahap identifikasi aset yang berkaitan dengan keamanan sistem informasi. Analisis ini didapatkan dari wawancara, referensi, dan diskusi dengan staf di instansi. Analisis risiko dilakukan berdasarkan standar ISO/IEC 27001. Analisis ini berhubungan dengan resiko dari aset, kerawanan (*vulnerability*), ancaman (*threats*), dampak serta peluang ancaman dapat terjadi pada aset seperti kerahasiaan informasi termasuk hak akses terhadap informasi (apakah dapat diakses oleh pihak yang tidak berwenang), dan lain sebagainya.
3. Menentukan prioritas risiko yang akan dikendalikan dengan menggunakan kriteria penilaian risiko. Penentuan ini dilakukan berdasarkan penggabungan data aset dan identifikasi kerawanan dan ancaman pada tahap sebelumnya. Setelah didapat prioritas risiko, lalu dikelompokkan kategori risiko dan identikasi nilai kecenderungan (*likelihood*) dan dampak risiko. Hasil dari identifikasi kerawanan dan ancaman serta pengukuran dampak akan memberikan nilai risiko (*risk value*). Setelah itu, dapat ditentukan langkah pengendalian risiko berdasarkan nilai risiko yang dihasilkan.
4. Menentukan kontrol beserta rencana kerja yang dapat mengendalikan risiko berdasarkan nilai risiko yang didapatkan sebelumnya sehingga akan

didapatkan rekomendasi pengendali risiko yang berupa instruksi, dokumentasi, kebijakan, maupun prosedur yang dapat diterapkan oleh instansi di masa depan dalam upaya memitigasi risiko keamanan yang akan muncul sesuai dengan ISO 27001.

5. Memantau atau *monitoring* risiko. Tahap ini dilakukan *review* identifikasi risiko yang telah dilakukan sebelumnya (Kominfo, 2017).

6. Pembuatan Rekomendasi Perbaikan Keamanan Informasi

Pada tahap ini, dilakukan penyusunan daftar hasil dari temuan audit berupa data-data atau bukti-bukti berdasarkan fakta yang ada. Kemudian diberikan rekomendasi perbaikan terkait keamanan sistem informasi yang mengacu pada standar ISO/IEC 27001 pada organisasi untuk dapat lebih baik lagi dalam melakukan penetapan kontrol keamanan sistem informasi yang ada.

Rekomendasi yang diberikan bertujuan agar organisasi dapat memperbaiki mekanisme sistem untuk mencapai tujuan, sasaran, dan strategi organisasi dalam pengelolaan keamanan sistem informasi.

7. Penyusunan Laporan Hasil Audit

Penyusunan laporan hasil audit keamanan sistem informasi dilakukan sesuai dengan format penyusunan laporan tugas akhir yang ada di Universitas Lampung. Laporan tugas akhir ini berupa dokumentasi dari hasil audit yang telah didapatkan selama masa penelitian.

V. KESIMPULAN DAN SARAN

A. Kesimpulan

Berdasarkan penelitian yang telah dilakukan sebelumnya, maka didapat kesimpulan sebagai berikut, yaitu:

1. Hasil rata-rata penilaian tingkat ketergantungan terhadap sistem elektronik pada bagian I kategori sistem elektronik adalah sebesar 17,67 (dibulatkan menjadi 18) sehingga tergolong tinggi. Hal ini menunjukan bahwa TIK sangat berperan pada pelayanan dan keamanan sistem informasi di instansi. Selain itu, hasil rata-rata dari keseluruhan penilaian kelima kategori keamanan informasi adalah sebesar 336 dan berada pada level I+ dan II yang berarti masih dalam kondisi awal dan penerapan kerangka kerja dasar. Dalam hal ini dapat disimpulkan bahwa tingkat keamanan informasi pada SIMDA Keuangan di Badan Keuangan Daerah Provinsi Lampung masih perlu perbaikan.
2. Pemberian rekomendasi perbaikan keamanan informasi pada masing-masing kategori pengamanan dan kategori sistem elektronik dilakukan berdasarkan pada standar ISO/IEC 27001 dengan tujuan agar dapat diterapkan guna meningkatkan keamanan informasi yang ada pada organisasi.

B. Saran

Berdasarkan penelitian yang telah dilakukan sebelumnya, maka saran yang diberikan untuk penelitian selanjutnya diharapkan dapat melakukan pemeriksaan dokumen secara menyeluruh terkait Sistem Manajemen Keamanan Informasi (SMKI) dan melakukan audit keamanan informasi dengan menggunakan *framework* lainnya.

DAFTAR PUSTAKA

Alraja, M.N., dan Alomiam, N.R. 2013. *The Effect of General Controls of Information System Auditing in The Performance of Information Systems: Field Study*. Interdisciplinary Journal of Contemporary Research In Business 2013. Institute of Interdisciplinary Business Research 356 Vol. 5, No. 3.

Basyarahil, F. A., Astuti, H. M. and Hidayanto, C. 2017. *Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya*. Jurnal Teknik ITS Vol. 6, No. 1, ISSN: 2337-3539.

Bilbao, E., Bilbao, A., dan Pecina, K. 2011. *Physical Logical Security Risk Analysis Model*. IEEE, 1-7, 2011.

BPKP. 2008. http://www.bpkp.go.id/sakd/konten/333/versi-2.1.bpkp.

BSSN. 2015. https://bssn.go.id/indeks-kami/.

Disterer, G. 2013. *ISO/IEC 27000, 27001 and 27002 for Information Security Management*. Department of Business Administration and Computer Science, University of Applied Sciences and Arts. Journal of Information Security, 2013, 4, 92-100.

Fazlida, M.R. dan Said, J. 2015. *Information Security: Risk, Governance and Implementation Setback.* Procedia Economics and Finance. Elsevier B.V., 28(April), pp. 243–248. doi: 10.1016/S2212-5671(15)01106-5.

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, pp. 66–77.

Gondodiyoto, S. 2007. *Audit Sistem Informasi + Pendekatan CobIT Edisi Revisi*. Jakarta: Mitra Wacana Media.p

ISO. 2013. https://www.iso.org/isoiec-27001-information-security.html.

Kominfo. 2017. *Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi (Indeks KAMI).* Jakarta: Direktorat Keamanan Informasi Direktorat Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika.

Mcleod, R. 2010. *Sistem Informasi Manajemen*. Jakarta: Salemba Empat.

Messier, W.F., Glover, S.M., dan Prawitt, D. F. 2014. *Jasa Audit dan Assurance Edisi 8*. Jakarta: Salemba Empat.

Onwubiko, C. 2009. *A Security Audit Framework for Security Management in the Enterprise*. pp. 9–17 In 5th International Conference, ICGS3 2009, London, UK, September 1-2, 2009.

Pratama, E. R., Suprapto, dan Perdanakusuma, A. R. 2018. *Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001 (Studi Kasus KOMINFO Provinsi Jawa Timur).* Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer. Vol. 2, No. 11, November 2018, hlm. 5911-5920.

Pelnekar, C. 2011. *Feature Planning for and Implementing ISO 27001*. ISACA Journal, Vol. 4, No. 4, 2011, pp. 1-8.

Sutabri, T. 2012. *Konsep Sistem Informasi*. Yogyakarta: Penerbit ANDI.

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

Tatiara, R., Fajar, A.N., Siregar, B., dan Gunawan, W. 2017. *Analysis of factors that inhibiting implementation of Information Security Management System (ISMS) based on ISO 27001*. IOP Publishing. Journal of Physics: Conf. Series 978 (2018) 012039 pp. 0–6.

Wolden, M., Valverde, R., dan Talla, M. 2015. *The Effectiveness COBIT Information for Reducing Cyber Attacks on Supply Management System.* IFAC-PapersOnLine. Volume 48, Issue 3, 2015, Pages 1846-1852. Elsevier Ltd., 48(3), pp. 1846–1852. doi:10.1016/j.ifacol.2015.06.355 .