BAB II

KAJIAN PUSTAKA

2.1 Badan Pengelolaan Keuangan Daerah

1. Visi Badan Pengelolaan Keuangan Daerah

“Terwujudnya pengelolaan pendapatan, keuangan dan aset daerah yang optimal”

2. Misi Badan Pengelolaan Keuangan Daerah

a. Meningkatkan Kualitas Profesionalisme Aparatur Pengelola Pendapatan, Keuangan dan Aset Daerah.

Bahwa meningkatnya kemampuan aparatur dalam Pengelolaan Pendapatan, pengelolaan Keuangan dan Aset Daerah akan menentukan keberhasilan dalam mewujudkan optimalisasi administrasi Keuangan Daerah dan membantu terselenggaranya kepemerintahan Yang baik dengan berdasarkan peraturan perundang-undangan yang berlaku.

b. Meningkatkan Pendapatan Daerah.

Bahwa Pendapatan Asli Daerah merupakan salah satu sumber pendapatan daerah yang sangat potensial. Untuk mendukung dan lancarnya pembangunan di Kabupaten Ciamis, maka perlu terus diupayakan peningkatan Pendapatan Asli Daerah melalui intensifikasi dan ekstensifikasi serta pengembangan system yang ada dan peningkatan kesadaran masyarakat dalam pembayaran kewajibannya.

c. Meningkatkan Kualitas Sistem Pengelolaan Pendapatan, Keuangan dan Aset Daerah sesuai dengan Peraturan dan Perundangan yang berlaku.

Pelaksanaan administrasi keuangan daerah harus berpedoman pada prinsip Anggaran Berbasis Kinerja. Pentausahaan Keuangan Daerah meliputi proses perencanaan, pelaksanaan serta pelaporan dan Pertanggungjawabannya. Untuk mendukung pelaksanaan prinsip tersebut dan seiring dengan perkembangan teknologi yang demikian cepat maka pengembangan dan peningkatan kemampuan keuangan daerah merupakan hal penting yang harus di implementasikan melalui sistem pengelolaan keuangan. Dengan dilaksanakannya hal tersebut diatas diharapkan dapat menjamin transparansi dan akuntabilitas penyelenggaraan keuangan daerah.

3. Kedudukan, Tugas Dan Fungsi

Peraturan Daerah Kabupaten Ciamis Nomor 8 Tahun 2016 tentang Pembentukan dan Susunan Perangkat Daerah. Peraturan Bupati Nomor 60 Tahun 2016 tentang Tugas, Fungsi dan Tata Kerja Unsur Organisasi Badan Pengelolaan Keuangan Daerah

a. Kedudukan

1) Badan Pengelolaan Keuangan Daerah merupakan unsur pelaksana yang melaksanakan fungsi penunjang urusan pemerintahan bidang keuangan.

2) Badan Pengelolaan Keuangan Daerah dipimpin oleh Kepala Badan yang berkedudukan di bawah dan bertanggung jawab kepada Bupati melalui Sekretaris Daerah.

b. TUGAS :

Tugas Pokok Badan Pengelolaan Keuangan Daerah Kabupaten Ciamis yaitu melaksanakan fungsi penunjang Urusan Pemerintahan Bidang Keuangan

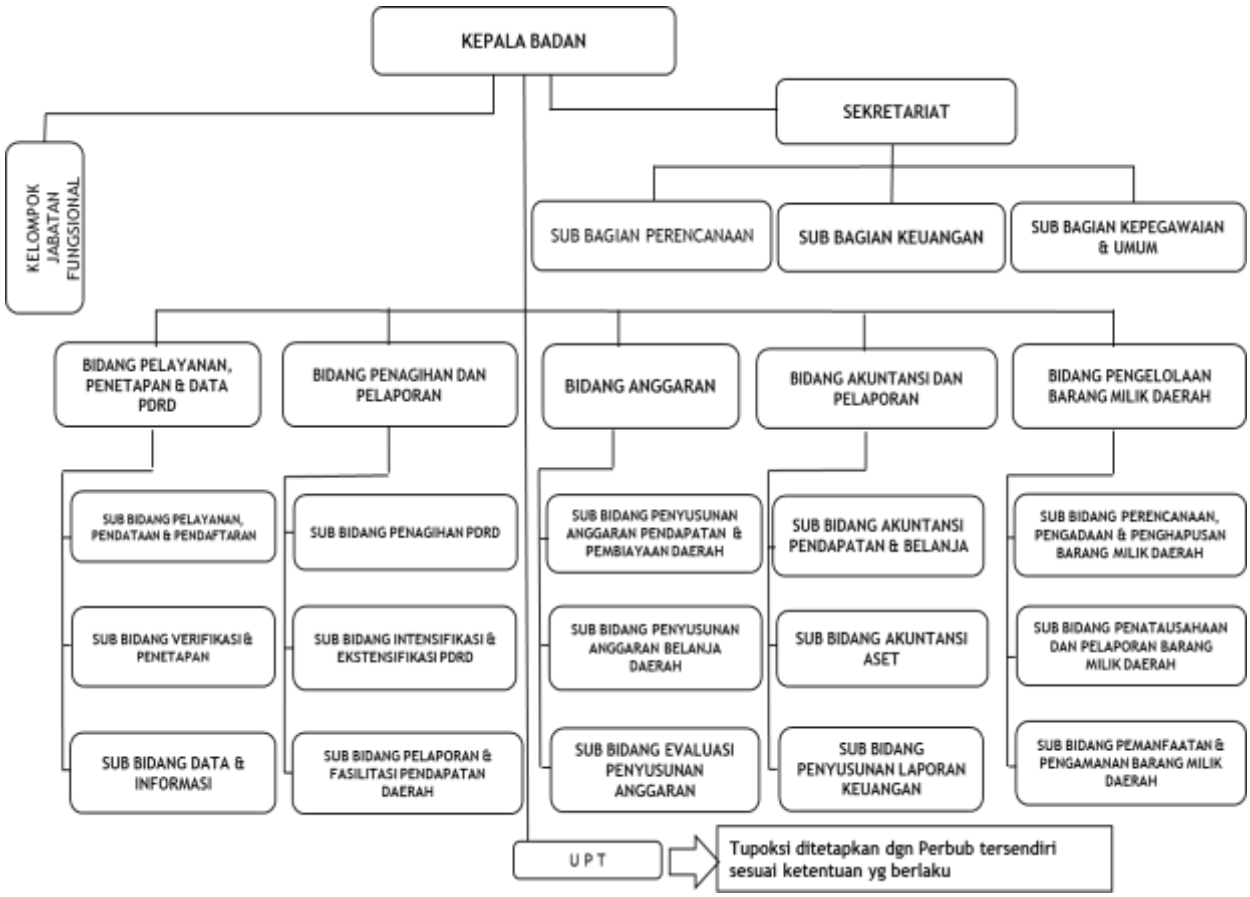
c. FUNGSI :

1) Perumusan Kebijakan teknis pelaksanaan dan pengendalian Pendapatan Daerah.
2) Penyiapan Kebijakan dan Pedoman pelaksanaan APBD.
3) Pengesahan Dokumen dalam Pelaksanaan Anggaran
4) Pengendalian Pelaksanaan APBD
5) Penyusunan petunjuk teknis pelaksanaan sistem penerimaan dan pengeluaran kas daerah
6) Pelaksanaan Pemungutan Pajak Daerah
7) Pemantauan pelaksanaan penerimaan dan pengeluaran APBD oleh Bank dan/ atau lembaga keuangan lainnya yang telah ditunjuk
8) Pengusahaan dan pengaturan dana yang diperlukan dalam pelaksanaan APBD
9) Penyimpan Uang Daerah
10) Pelaksanaan penempatan uang daerah dan pengelolaan/ penatausahaan investasi

11) Pelaksanaan pembayaran berdasarkan permintaan pejabat pengguna
12) anggaran atas beban rekening Kas Umum Daerah
13) Penyiapan pelaksanaan pinjaman dan pemberian jaminan atas nama pemerintah daerah
14) Pelaksanaan pemberian pinjaman atas atas nama pemerintah daerah
15) Pengelola utang dan piutang daerah
16) Penagihan piutang daerah
17) Pelaksanaan sistem akuntansi dan pelaporan keuangan daerah
18) Penyajian informasi keuangan daerah
19) Pelaksanaan kebijakan dan pedoman pengelolaan serta penghapusan barang milik Daerah
20) Perencanaan dan Penyuluhan Pendapatan Daerah Pelaksanaan pendataan, pendaftaran dan penetapan Pendapatan Daerah
21) Pelaksanaan tugas lain yang ditetapkan Bupati

4. Struktur Organisasi

Peraturan Bupati Nomor 36 Tahun 2016 Tentang Kedudukan Tugas Fungsi Susunan Organisasi dan Tata Kerja Perangkat Daerah



Gambar 2.1
Susunan Organisasi dan Tata Kerja Perangkat Daerah

2.2 Keamanan Informasi Berbasis ISO/IEC 27001:2005

2.2.1 Konsep Keamanan Informasi Berbasis ISO/IEC 27001:2005

Sistem manajemen keamanan informasi (SMKI) atau yang disebut juga *Information Management Security System* (ISMS) merupakan suatu proses yang disusun berdasarkan pendekatan risiko bisnis untuk merencanakan (*Plan*), mengimplementasikan (*Do*), memonitor adan meninjau ulang (Check), dan memelihara (*Act*) terhadap keamanan informasi perusahaan [ISO/IEC 27001:2005].

Keamanan informasi ditujukan untuk menjaga aspek kerahasiaan (*Confidentially*), Keutuhan (*Integrity*), dan Ketersediaan (*Avaibillity*) dari informasi. (Sarno, 2009) SMKI berdasarkan ISO/IEC 27001:2005 menjelaskan syarat-syarat untuk membuat, menerapkan, melaksanakan, memonitor, menganalisa, dan memelihara serta mendokumentasikan sistem manajemen keamanan informasi (SMKI).

ISO/IEC 27001 mendefinisikan keperluan-keperluan untuk sistem manajemen keamanan informasi yang baik akan membantu memberikan perlindungan terhadap gangguan pada aktivitas-aktivitas bisnis dan melindungi proses bisnis yang terpenting agar terhindar dari resiko kerugian/bencana dan kegagalan pada pengamanan informasi. ISO 27001 digunakan sebagai ikon sertifikasi ISO 27000.

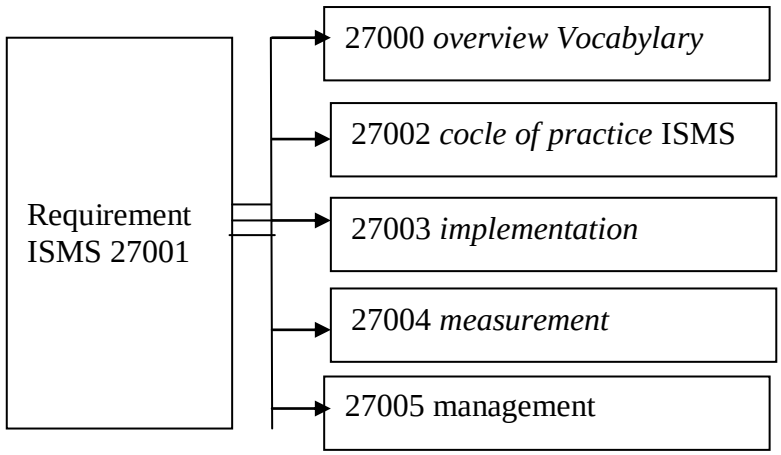
ISO 27000 merupakan dokumen standar sistem manajemen keamanan informasi yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah organisasi dalam usaha untuk mengimplementasikan konsep-konsep keamanan informasi dalam organisasi. (Sarno, 2009) (Nasional, 2009)

2.2.2 Standard *ISO:IEC 27001:2005 Information Security Management System*

Dalam standar keamanan informasi ISO/IEC 27000 memiliki beberapa series yang telah dikembangkan untuk manajemen keamanan informasi atau ISMS. Series dari ISO/IEC 27000 terdiri dari :

a. ISO/IEC 27000- *Informationsecurity management systems Overview and vocabulary*
b. ISO/IEC 27001- *Information Security Management Systems Requirements*

c. ISO/IEC 27002 - *Code of practice for information security management*
d. ISO/IEC 27003 - *Information security management system implementation guidance*
e. ISO/IEC 27004 - *Information security management Measurement*
f. ISO/IEC 27005- *Information security risk management*.



Gambar 2.2. Struktur Series Standar ISO 27000

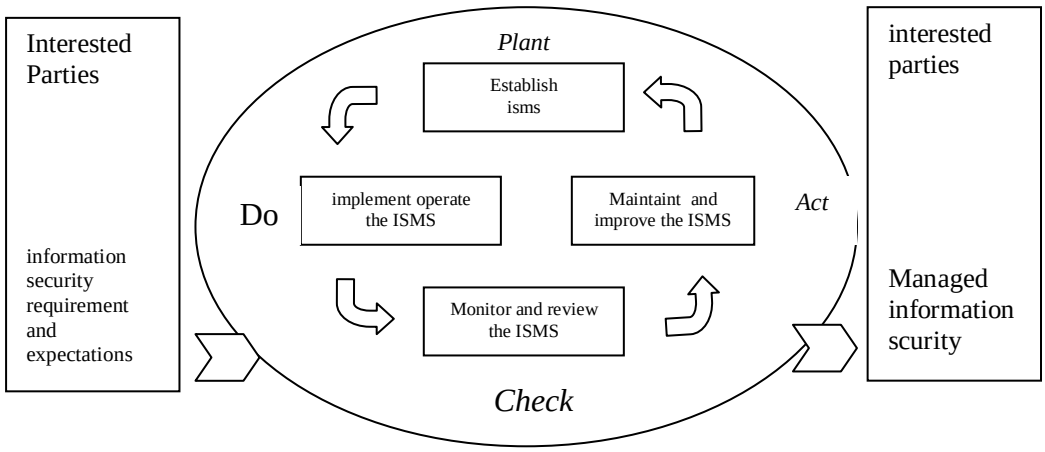
Gambar 2.2 diatas adalah struktur series hubungan dari standar ISO/IEC 27000.

ISO/IEC 27001 merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management Systems* (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha pengimplementasian konsep-konsep keamanan informasi di perusahaan.

Standar internaisonal ini telah dipersiapkan untuk menyediakan sebuah model pembangunan, penerapan, pengerjaan, pengawasan, peninjauan, pemeiliharaan, peningkatan sebuah SMKI. Standar ini mengadopsi model *Plan- Do-Check-Act* (PDCA) yang diterapkan untuk menyusun sebuah proses SMKI. (HUMPHREYS, 2007)

2.2.3 Model Proses

ISO/IEC 27001:2005 menetapkan model tahapan yang dibutuhkan dalam mengimplementasikan pemenuhan manajemen keamaman informasi dengan tujuan orgnisasi dan kebutuhan bisnis. (ISO/IEC, ISO/IEC 27001 *Information security management system - Requirement*s, 2005)



Gambar 2.3. Model PDCA

Gambar 2.3 diatas adalah gambar dari model PDCA yang terdapat pada ISO27001 yang akan dijelaskan pada uraian sebagai berikut.

1. ***Plan* (penetapan SMKI)**

   Menetapkan kebijakan, sasaran, dan prosedur SMKI yang sesuai untukpengolahan risiko dan perbaikan keamanan informasi agar menghasilkan hasilyang sesuai dengan kebijakan dan sasaran organisasi secara keseluruhan.(Nasional, 2009)

2. ***Do* (Penerapan dan pengoperasian SMKI)**

   Menerapkan dan mengoperasikan kebijakan, pengendalian, proses, danprosedur SMKI (Nasional, 2009)

3. *Check* (Pemantauan dan pengkajian SMKI)

Mengakses dan apabila berlaku mengukur kinerja proses terhadap kebijakan,sasaran, SMKI dan pengalaman praktis dan melaporkan hasilnya kepadamanajemen untuk pengkajian. (Nasional, 2009)

4. *Act* (Peningkatan dan pemeliharaan SMKI)

Mengambil tindakan korektif dan pencegahan berdasarkan hasil internal auditSMKI dan tinjauan manajemen atau informasi terkait lainnya untuk mencapaiperbaikan berkesinambungan dalam SMKI (Nasional, 2009)

2.2.2 Struktur Organisasi ISO/IEC 27001

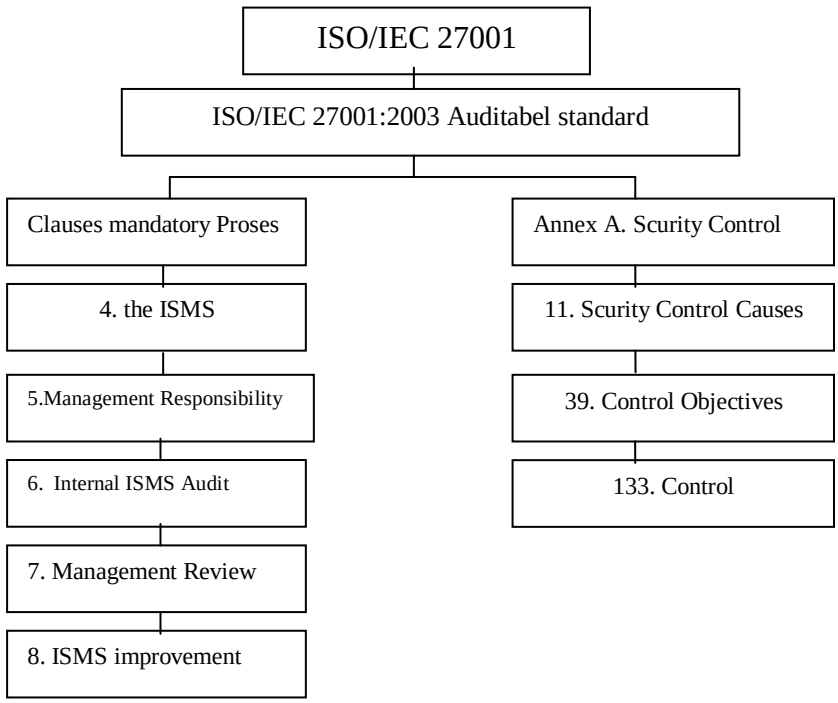
Struktur organisasi ISO/IEC 27001 dibagi dalam dua bagiansebagaimana yang telah dipaparkan sebagai berikut.

a) Klausul : *Mandatory Process*

Klausul (pasal) adalah persyaratan yang harus dipenuhi jika organisasimenerapkan SMKI dengan menggunakan standar ISO/IEC 27001.

b) Annex A : *Security Control*

Annex A adalah dokumen referensi yang disediakan dan dapat dijadikanrujukan untuk menentukan Kontrol Keamanan (*Security Control*) yang perlu diimplementasikan di dalam SMKI, yang terdiri dari 11 klausul control keamanan (*Security Contol Clauses*), 39 Objektif Kontrol (*ControlObjectives*), dan 133 Kontrol (*Controls*). (Sarno, 2009). Struktur organisasi pada ISO 27000 dapat dilihat pada Gambar 2.3.



Gambar 2.4. Struktur Organisasi ISO/IEC 27001

2.2.4 Panduan Sistem Manajemen Keamanan Informasi

Panduan penyusunan langkah-langkah sistem manajemen keamanan informasi (SMKI) pada tahap *Plan-Do-Check-Act* akan dijelaskan sebagai berikut.

1. SMKI Perencanaan (*Plan)*

a) Melakukan persetujuan komitmen manajemen SMKI

Sebelum SMKI dibangun pihak manajemen dalam organisasi harus memberikan dukungan kepada organisasi dalam melaksanakan SMKI berupa dukungan manajemen.

b) Menentukan ruang lingkup dan kebijakan ISMS

Langkah kedua adalah menentukan ruang lingkup implementasi SMKI yang akan diterpakan dalam organisasi pada ruang lingkup

mana saja, seluruh bagian organisasi atau hanya sebagian. Penentuan ruang lingkup SMKI ini dilakukan berdasarkan :

1) Kebutuhan organisasi

2) Aset yang dimiliki oleh organisasi

c) Menetapkan pendekatan asesmen risiko pada organisasi

Penilaian resiko ini berguna untuk mengetahui bagaimana cara melakukan penilaian resiko sesuai dengan kebutuhan organisasi. Pelaksanaan penilaian resiko tergantung dari ruang lingkup SMKI yang telah ditentukan. Penilaianresiko terdapat dua macam hal yang harus dipaparkan yaitu sebagai berikut.

1) Metode *Risk Assessment* : Metode yang digunakan untuk melakukan penilaian resiko terhadap informasi dapat dilakukan dengan beberapa metode antara lain : metode statistic atau metode matematis. (Sarno, 2009)

2) Kriteria penerimaan resiko : Kriteria penerimaan resiko ditujukan sebagaiacuan tindakan yang akan dilakukan dalam menangani resiko yang ada dalam perusahaan. (Sarno, 2009)

d) Mengidentifikasi resiko

Identifikasi resiko bertujuan untuk memahami seberapa besar dan identifikasiresiko apa yang akan diterima oleh organisasi jika informasi organisasi mendapat ancaman atau gangguan keamananan yang menyebabkan gagalnya penjagaan aspek keamanan informasi. (ISO/IEC, ISO/IEC 27001 *Information security management system* -

Requirements, 2005). Langkah-langkah untuk mengidentifikasi resiko yaitu :

1) Mengidentifikasi aset

   Mengidentifikasi aset dalam SMKI dapat dilakukan dengan menggunakan tabel aset yang telah dikategorikan menurut jenis atau kebutuhan organisasi. (Sarno, 2009)

2) Menghitung nilai aset

   Cara menghitung nilai aset berdasarkan aset keamanan informasi yaitu *Confidentiality*, *Integrity,* dan *Availability* dapat menggunakan table penilaian aset berdasarkan kriteria *Confidentiality* yang ditunjukkan pada Tabel 2.1. (Sarno, 2009)

Tabel 2.1
. Kriteria *Confidentiality*

Kriteria *Confidentiality*	Nilai *Confidentiality* (NC)
Public	*0*
Internal use only	*1*
Private	*2*
Confidential	*3*
Secret	*4*

(Sumber : Riyanarto Sarno: 2009)

Kriteria nilai *Integrity* ditunjukkan pada Tabel 2.2.

Tabel 2.2
Kriteria Integrity

Kriteria *Integrity*	Nilai *Integrity* (NI)
No Impact	0
No Impact	*1*
General disturbance	*2*
Mayor disturbance	*3*
Uncceptable damage	*4*

Kriteria nilai *Availability* ditunjukkan pada Tabel 2.3

Tabel 2.3.
Kriteria *Availability*

Kriteria *Availability*	Nilai *Availability* (NV)
No Availability	0
Office hours Avaibility	*1*
Strong Availability	*2*
High Availability	*3*
Very High Availability	*4*

(Sumber : Riyanarto Sarno: 2009)

Perhitungan nilai aset dapat dihitung dengan menggunakan persamaan matematis berikut :

Nilai Aset (NA) = NC + NI + NV..... (2.1)

dimana:

NC = Nilai *Confidentialy*
NI = Nilai *Integrity*
NA = Nilai *Availability*

3) Mengidentifikasi ancaman dan kelemahan terhadap aset

Mengidentifikasi ancaman dan kelemahan terhadap aset dapat menggunakan tabel *Probability of Occurance* seperti pada Tabel 2.4 dengan menentukan rentang nilai *probability* dari level LOW,MEDIUM, dan HIGH. (Sarno, 2009)

Tabel 2.4
Contoh Kemungkinan Gangguan Keamanan

No	Ancaman	Jenis	Probabilitas	Rerata
1	Gangguan Perangkat Keras	Ancaman	Low	0,3
2	Gangguan sumber daya	Kelemahan	Low	0,2
3	Bencana Alam	Ancaman	High	0,7
4	Akses Ilegal	Ancaman	Medium	0,6
5	**Σ Ancaman Σ PO**	**Σ PO**		

LOW : Nilai Rerata Probabilitas 0,1- 0,3

MEDIUM : Nilai Rerata Probabilitas 0,4- 0,6

HIGH : Nilai Rerata Probabilitas 0,7- 1,0

Nilai ancaman dapat dihitung dengan menggunakan persamaan matematis berikut :

NT = ΣPO/ΣAncaman ..... (2.2)

dimana:

NT = Nilai Ancaman

ΣPO = Jumlah Rerata Probabilitas

ΣAncaman = Jumlah Ancaman

1) Mengidentifikasi dampak hilangnya kerahasiaan, integritas dan ketersediaan terhadap informasi dari aset. Mengidentifikasi dampak hilangnya kerahasiaan, integritas, dan ketersediaan dari masing-msing aset sesuai dengan aspek keamanan informasi.
2) Menganalisis dan mengevaluasi resiko

   Tahap ini bertujuan untuk menganalisa dan mengevaluasi resiko yang sudah diidentifikasi pada tahap sebelumnya, untuk memahami bagaimana dampak resiko terhadap bisnis organisasi, bagaimana level resiko yang mungkin dan menentukan apakah resiko yang terjadi langsung diterima atau masih perlu dilakukan pengolaan (*treatment*) agar resiko dapat diterima dengan dampak yang bisa ditoleransi Analisa dan evaluasi resiko terdiri dari langkah-langkahberikut :

1) Menetukan nilai analisa dampak bisnis (*Business Impact Analysis*)

Analisa dampak bsinis adalah analisa yang menggambarkan seberapa tahan proses bisnis di dalam organisasi berjalan ketika informasi yangdimiliki terganggu dengan menentukan nilai BIA pada masing-masing asset (Sarno, 2009). Skala nilai BIA digunakan untuk menentukan nilai BIA yang ditunjukkan pada Tabel 2.5

Tabel 2.5
Skala Nilai BIA

Batas ToleransiGangguan	**Keterangan**	**Nilai BIA**	**Nilai Skala**
< 1 Minggu	*Not Critical*	0	0-20
< 1 Haris/d 2 Hari	*Mayor Critical*	1	21-40
< 1 Hari	*Mayor Critical*	**2**	41-60
< 12 Jam	*High Critical*	**3**	61-80
< 1 Jam	*Very High Critical*	4	81-100

(Sumber : Riyanarto Sarno: 2009)

2) Mengidentifikasi level resiko

Mengidentifikasi level risiko dilakukan untuk menentukan pilihan penanganan risiko (Sarno, 2009). dan mendefinisikan nilai dari level risiko sesuai dengan pedoman pengukuran yang telah ditetapkan (Bali, 2014).Identifikasi level risiko dapat digambarkan dalam bentuk matriks level risiko yang ditunjukkan pada Tabel 2.6

Tabel 2.6.
Matriks Level Risiko

Probabilitas Ancaman	**Dampak**				
	Not *critical*	**Low *critical***	**Medium *critical***	***High* critical**	***Very high* critical**
Low (0.1)	Low 0	Low 0.1	Low 0.2	Low 0.3	Low 0.4
Medium (0,5)	Low 0	Medium 0.5	Medium 1	Medium 1.5	Medium 2
High (1,0)	Low 0	Medium 1	Medium 2	High *3*	High *4*

(Sumber : *National Institute of Standards and Technology* (NIST) :800-30)

3) Menentukan apakah resiko yang timbul diterima atau masih diperlukan pengolahan resiko dengan menggunakan kriteria penerimaan resiko Untuk menentukan level risiko diperlukan nilai risiko untuk menentukan letak level dari masing-masing-masing aset yaitu dengan menggunakan perhitungan persamaan matematis berikut (Sarno, 2009).

Risk Value = NA x BIA x NT ..... (2.3)

dimana:

Risk Value = Nilai Risiko

NA = Nilai Aset

BIA = Nilai BIA

NT = Nilai Ancaman

e) Identifikasi dan evaluasi pilihan penanganan resiko

Langkah ini menjelaskan bahwa organisasi harus melakukan identifikasi dan evaluasi pilihan penanganan resiko. Maksud dari langkah ini adalah melakukan kegiatan identifkasi dan menentukan pilihan penanganan resiko jika resiko yang timbul tidak langsung diterima tetapi perlu dikelola lebih lanjut dengan menggunakan kriteria penerimaan yang telah ditentukan.

Langkahnya adalah mengidentifikasi atau menentukan pilihan pengolahan resikonya. Pilihan pengolahan resikonya dapat ditentukan sebagai berikut:

1) Menerima resiko dengan menerapkan kontrol keamanan yang sesuai
2) Menerima resiko dengan menggunakan kriteria resiko yang telah ditetapkan
3) Menerima resiko dengan mentransfer resiko kepada pihak ketiga (Asuransi, vendor, supplier, atau pihak tertentu).

f) Memilih konrol objektif dan kontrol .

Pemilihan kontrol keamanan mengacu kepada tabel kontrol keamanan dalam dokumen ISO/IEC 27001 (Annex A) yang panduan implementasinya lebih detail dijelaskan pada dokuemen ISO 27002. Kontrol keamanan memiliki Kontrol Objektif dan Kontrol. Implementasi Objektif Kontrol dan Kontrol dapat mereferensi ke standar ISO17799/27002:2005 yang dapat dilihat lebih detail pada dokumen ISO/IEC 27002 (ISO/IEC, ISO/IEC 27001 Information *security management system - Requirements,* 2005) (Sarno, 2009).

ISO/IEC 27002:2005 mendefinisikan 11 (sebelas) klausul, 39 Objektif Kontrol dan 133 Kontrol yang dapat diterapkan untuk membangun sistem manajemen keamanan informasi (SMKI) (ISO/IEC, ISO/IEC 27001 *Information Security Management System Requirements,* 2005). (Sarno, 2009). Klausul-klausul tersebut antara lain:

1) Kebijakan Keamanan (*Security Policy*)- Klausul 5
2) Organisasi Keamanan Informasi (*Organization Of Information Security*)-Klausul 6
3) Manajemen Aset (*Asset Management*) – Klausul 7

4) Pengamanan terhadap SDM (*Human Resources Security*)- Klausul 8
5) Keamanan Fisik dan Lingkungan (*Physical and Environmental Security*)- Klausul 9
6) Komunikasi dan Manajemen Operasional (*Communication & Operation Management)* – Klausul 10
7) Kontrol Akses (*Access Control*)- Klausul 11
8) Akuisisi Sistem Informasi, Pembangunan dan Pemeliharaan (*Information System Acquition, Development and Maintenance*)- Klausul 12
9) Manajemen Insiden Keamanan Informasi (*Information Security Incident Management*) – Klausul 13
10) Manajemen Kelangsungan Bisnis (Business Continuity Management) –Klausul 14
11) Kesesuaian (Complience) – Klasul 15

2. SMKI Implementasi (*Do)*

a. Membuat rencana untuk penanganan resiko

Dalam implementasi dan operasional SMKI penanganan resiko penting dilakukan karena untuk mengetahui seberapa penting keamanan informasi dalam sebuah perusahaan. Dalam melakukan rencana implementasi penanganan resiko dibutuhkan 2 tahapan yang harus dilakukan yaitu :

1) Mendefinisikan metode penilaian resiko
2) Identifikasi aset

3) Identifikasi resiko

4) Menilai resiko

5) Identifikasi kontrol

b. Mengimplementasikan rencana kontrol keamanan

Implementasi kontrol keamanan merupakan hal yang vital dalam SMKI. kontrol tersebut merupakan implementasi dari sistem keamanan yang disusun dalam SMKI dengan tujuan untuk menurunkan tingkat resiko yang harus diterima oleh organisasi jika terjadi kegagalan keamanan informasi sampai pada level yang bisa ditoleransi oleh organisasi. Beberapa persyaratan yang harus diprerhatikan oleh organisasi antara lain :

1) Kontrol keamanan yang dipiih harus benar-benar sesuai dan memenuhi kebutuhan organisasi.
2) Kontrol keamanan yang dipilih merupakan penilaian resiko (*Risk Asessment*) yang dilakukan oleh organisasi terhadap aset yang dimiliki.
3) Kontrol keamanan yang diterapkan harus diukur keefektifitasannya untuk mengetahui apakah telah sesuai dan dapat memenuhi objektif kontrol yang telah ditetapkan.
4) Menentukan metode pengukuran keefektifitasan kontrol keamanan

Langkah menentukan metode pengukuran efektifitas kontrol keamanan ini meliputi :

1) Menentukan subjek yang akan diukur, mencakup : objektif kontrol dan kontrol keamanan
2) Menentukan ukuran atau satuan ukuran, mencakup : satuan jumlah dan satuan prosentase
3) Menentukan kriteria/ kategori keefektifitasan .
4) Mengelola operasi dan penyebaran ISMS

Langkah-langkah dalam tahapan mengelola dan mengeperasionalkan SMKI adalah melaksanakan proses Plan-Do-Check-Act (PDCA). Secara umum hal penting yang dilakukan dalam tahapan ini mencakup hal-hal berikut.

1) Menjalankan penanganan resiko SMKI berdasarkan kontrol yang telah dipilih
2) Selalu memelihara daftar ancaman (threat) dan kelemahan (*vulnerability*) terhadap SMKI
3) Mengoperasional SMKI

c. Mengimplementasikan prosedur dan intruksi kerja

Tahap ini organisasi harus mengimplementasikan hasil dokumen operasional yang telah dibuat seperti prosedur keamanan informasi dan instruksi kerja.

3. SMKI Monitoring (*Check*)

a. Monitoring dan tinjauan ISMS

Monitoring dilakukan untuk memantau pelaksanaan SMKI dengan memperhatikan 10 subjek utama (*Critical Success Factor*)

b. Mengukur efektifitas kontrol keamanan yang digunakan

Tahapan ini merupakan implementasi klausul 4.2.3.c dalam ISO/IEC 27001yang dilakukan untuk peninjuan ulang efektifitas kontrol keamanan yang diolah oleh organisasi. Pengukuran yang dilakukan mencakup langkah-langkahberikut.

1) Identiikasi kontrol keamanan yang akan diukur
2) Bagaimana cara pengukurannya
3) Berapa kali pengukuran yang akan dilakukan
4) Ukuran efektifitas yang didefinisikan
5) Identifikasi data pengukuran yang akan diambil analisa dan buat prosedurpelaporannya
6) Pelaksanaan pengukuran

c. Melaksanakan pengukuran ISMS dalam operasi

Model kedewasaan SMKI akan membantu organisasi dalam menentukan seberapa manfaatkah (berdayaguna) dan bagaimana kesusaian SMKI yang telah diterapkan terhadap apa yang telah diharapkan.

d. Melaksanakan audit internal

Audit merupakan proses atau aktivitas yang sistematik, independen dan terdokumentasi untuk menemukan suatu bukti-bukti dan dievaluasi secara objektif untuk menentukan apakah telah memenuhi kriteria pemeriksaan (Audit) yang telah ditetapkan.

4. SMKI Pemeliharaan (*Act*)
    a. Menerapkan dan memasukkan ke dalam praktek perbaikan identifikasi
    b. Melaksanakan tindakan korektif dan pencegahan
    c. Berkomunikasi dengan semua pihak yang terkait dan berkepentingan dalam meningkatkan efektivitas ISMS (ISO/IEC, ISO/IEC 27001 *Informationsecurity management system - Requirements,* 2005) (Sarno, 2009)

2.3 *Standard* ISO:IEC 27001:2005 *Code Of Practice for ISMS*

ISO/IEC 27001 berisi panduan yang menjelaskan contoh penerapan keamanan informasi dengan menggunakan bentuk-bentuk kontrol tertentu agar mencapai sasaran kontrol yang ditetapkan. Bentuk-bentuk kontrol yang disajikan seluruhnya menyangkut 11 area pengamanan sebagaimana ditetapkan dalam ISO/IEC 27001.

ISO/IEC27001 tidak mengharuskan bentuk-bentuk kontrol yang tertentu tetapi menyerahkan kepada pengguna untuk memilih dan menerapkan control yang tepat sesuai kebutuhannya, dengan mempertimbangkan hasil kajian risiko yang telah dilakukannya. Pengguna juga dapat memilih kontrol di luar daftar kontrol yang dimuat standar ini sepanjang sasaran kontrolnya dipenuhi. (ISO/IEC,

ISO/IEC 27002 *Code of practice for Information Security Management*, 2007)ISO 27002:2005 memiliki 133 kontrol dan 11 klausul yang terdaftar antara lain:

1. *Security Policy.*
2. *Organizing Information Security.*
3. *Asset Management.*
4. *Human Resources Security.*
5. *Physical and Environmental Security.*
6. *Communications and Operations Management.*
7. *Access Control.*
8. *Information Systems Acquisition, Development and Maintenance.*
9. *Information Security Incident Management.*
10. *Business Continuity Management.*
11. *Compliance.*

2.4 Standar Sistem Manajemen Keamanan Informasi (SMKI)

Pada 2005, *International Organization for Standarization* (ISO) atau Organisasi Internasioanl untuk Standarisasi telah menjabarkan standar-standar mengenai *Information Security Management Systems* (ISMS) atau Sistem Manajamen Keamanan Informasi (SMKI) baik dalam bentuk persyaratan maupun panduan.

Dari standar seri ISO 27000 ini hingga September 2011, baru ISO/IEC 27001:2005 yang telah diadopsi oleh Badan Standarisasi Nasional (BSN) sebagai Standar Nasional Indonesia (SNI) yang bernomor SNI ISO/IEC 2007:2001.

2.4.1 Kemanan Informasi

Menurut ISO/IEC 27001:2001 keamanan informasi adalah penjagaan kerahasiaan, identitas dan ketersediaan informasi. Keamanan informasi juga

merupakan suatu bentuk usaha yang dilakukan untuk mengamankan informasi atau aset informasi yang dilakukan dengan berbagai upaya dengan tujuan untuk membuat aman suatu informasi yang ada. Keamanan informasi berbeda dengan keamanan teknologi informasi atau *IT Security* akan tetapi, kedua hal tersebut saling terkait. Keamanan teknologi informasi mencakup kegiatan atau usaha-usaha pengamanan infrasruktur TI dari ancaman-ancaman yang berupa akses serta penggunaan jaringan tanpa seizin pihak yang berwenang, sementara keamanan informasi hanya mengacu pada data informasi milik organisasi atau perusahaan. Dalam hal ini usaha yang perlu dilakukan adalah mengembangkan, merencanakan, serta memantau semua kegiatan yang terkait dengan usaha untuk memebuat data dan informasi tersebut dapat berguna sesuai dengan fungsinya serta tidak disalahkan gunakan atau dibocorkan kepada pihak-pihak yanng tidak berwenang.

Berdasarkan hal tersebut maka teknologi informasi merupakan salah satu aset penting yang digunakan untuk mengamankan akses serta penggunaan data dan informasi yang dimiliki perusahaan. Dalam suatu organisasi keamanan informasi adalah aspek yang sangat penting , semakin banyak data dan informasi yang ada dalam organisasi tersebut maka semakin banyak ancaman keamanan informasi yang didapat oleh organisasi tersebut. Terdapat 5 layanan jaminan keamanan informasi, diantaranya adalah sebagai berikut .

1. *Confidentiality*, yaitu memastikan terhadap pengaksesan informasi diakses hanya dapat dilakukan oleh pihak yang berkepentingan.

2. *Authenticity*, yaitu penjaminanan atas keaslian informasi.
3. *Integrity*, yaitu *Pemastian* akan ketepatan dan kelenggkapan informasi sesuai dengan bentuk semula.
4. *Availability*, yaitu memastikan bahwa orang yang berwenanglah yang hanya dapat mengakses suatu informasi dengan tepat waktu apabila data diperlukan
5. *Non-Repudiation*, yaitu menjamin bahwa pihak pengguna tidak dapat menyangkal keaslian tanda tangan digital (digital signature) pada suatu dokumen atau tempat dalam suatu jaringan.

2.4.2 Sasaran Pengendalian Keamanan Informasi

Kebijakan dan Standar Sistem Manajemen Keamanan Informasi yang diadopsi dari ISO 27001:2005, terdapat sebelas sasaran pengendalian yaitu sebagai berikut:

1. Pengendalian Umum

   Sasaran ini digunakan sebagai acuan dalam kegiatan perlindungan aset informasi dalam lingkungan Kementrian Keuangan dari segala macam bentuk ancaman atau gangguan dari lingkungan internal maupun eksternal dan secara sengaja maupun tidak sengaja. Sasaran pengendalian ini mencakup pengelolaan keamanan seluruh aset informasi yang dilakukan oleh seluruh unit kerja, pegawai Kementrian Keuangan baik sebagai pengguna maupun pengelola Teknologi Informasi dan Komunikasi (TIK), serta pihak ketiga di lingkungan Kementrian Keuangan.

2. Pengendalian Organisasi Keamanan Informasi

   Tujuan dari sasaran pengendalian ini yaitu untuk memberikan pedoman dalam suatu pembentukan organisasi yang fungsional dalam konteks keamanan informasi dan bertanggung jawab dalam pengelolaan keamanan informasi termasuk hubungannya dengan pihak luar.

3. Pengendalian Pengelolaan Aset

   Tujuan dari sasaran pengendalian ini yaitu untuk memberikan acuan dalam hal pengelolaan aset informasi guna melindungi dan menjamin keamanan aset informasi.

4. Pengendalian Keamanan Sumber Daya Manusia

   Tujuan dari sasaran pengendalian ini yaitu untuk memastikan bahwa seluruh pegawai maupun pihak ketiga mengerti dan memahami akan tanggung jawab masing-masing mengenai ancaman keamanan informasi serat memahami semua proses yang berhubungan dengan keamanan informasi sebelum, selama dan sesudah bertugas.

5. Pengendalian Keamanan Fisik dan Lingkungan

   Tujuan dari sasarn pengendalian ini adalah untuk mencegah adanya akses fisik yang dilakukan oleh pihak yang tidak berwenang, serta menghindari terjadinya kerusakan pada perangkat pengolah informasi dan gangguan terhadap aktifitas organisasi.

6. Pengendalian Pengelolaan Komunikasi dan Operasi

   Tujuan dari sasaran ini adalah untuk memastikan bahwa perangkat operasional yang ada aman dan benar terhadap pengolahan informasinya. Tujuan lain dari

sasaran ini adalah untuk mengimplementasikan, memelihara keamanan informasi, meminimalkan segala resiko kegagalan, memastikan akan keutuhan dan ketersediaan informasi, memastikan keamanan pertukaran informasi dan pemantauan proses operasional.

7. Pengendalian Akses

   Tujuan dari sasaran pengendalian ini adalah untuk memastikan otorisasi akses pengguna dan melakukan pencegahan terhadap akses oleh pihak yang tidak berwenang pada aset informasi khususnya pada perangkat pengolah informasi.

8. Pengendalian Pengadaan, Pengembangan, dan Pemeliharaan Sistem

   Tujuan dari sasaran pengendalian ini adalah untuk memastikan bahwa keamanan informasi merupakan bagian yang telah terintegrasi dengan sistem informasi, melakukan pencegahan akan terjadinya kesalahan, kehilangan serta modifikasi atau pengubahan oleh pihak-pihak yang tidak bertanggung jawab.

9. Pengendalian Pengelolaan Gangguan Keamanan Informasi

   Tujuan sasaran pengendalian ini adalah untuk memastikan kejadian dan kelemahan informasi yang terhubung dengan sistem informasi agar dapat dikomunikasikan dan dilakukan perbaikan, serta dilakukannya suatu pendekatan yang konsisten agar tidak terulang kembali kesalahan yang serupa.

10. Pengendalian Pengelolaan Kelangsungan Kegiatan

    Tujuan dari sasaran pengendalian ini untuk melindungi sistem informasi, memastikan keberlangsungan kegiatan pada saat keadaan darurat dan untuk memastikan bahwa telah dilakukan pemulihan yang tepat.

11. Pengendalian Kepatuhan

Sasaran pengendalian ini bertujuan untuk menghindari terjadinya pelanggaran terhadap peraturan perundang-undangan yang terkait keamanan informasi.

2.5.4 Penggunaan Alat Evaluasi Indeks Keamanan Informasi

Gambaran proses indeks Kemanan Informasi seperti gambar berikut ini:

Gambar 2.5 Ilustrasi Evaluasi

Ilustrasi diatas menjelaskan bahwa indeks KAMI merupakan seperangkat alat eavluasi yang digunakan dalam penggunaan tata kelola keamanan informasi yang dilakukan dengan berkelanjutan yang bertujuan untuk memberikan ilustrasi terhadap hasil dari penerapan tersebut. Terjadinya perubahan infrastruktur pada kondisi awal evaluasi indeks KAMI, maka peninjauan ulang dilakukan untuk memberikan kepastian terhadap kematangan hasil evaluasi.

2.4.4 Penilaian Tingkat Kematangan

Definisi dari tingkat kematangan adalah untuk mengidentifikasi kelengkapan dan tingkat kematangan untuk penerapan pengamanan yang telah ditetapkan sebagai panduan di dalam indeks KAMI. SNI ISO/IEC 27001:2001 termasuk dalam

penjabaran evaluasi kelengkapan yang bertujuan untuk menganalisa tingkat kematangan dengan pengelompokan proses yang terkait terhadap acuan dari *framework* COBIT atau CMMI. Hasil evaluasi nantinya dipergunakan sebagai pelaporan kesiapan keamanan informasi di Institusi/Lembaga Kementrian.

Tingkat kematangan yang di perlukan dalam indeks KAMI di kelompokkan sebagai berikut:

5. Tingkat 0 – Dengan status "Tidak Diketahui (Pasif)"
    a. Tidak diketahuinya status keamanan informasi.
    b. Pihak-pihak yang terkait dalam konsep pengamanan informasi tidak mengikuti dan tidak melaporkan hasil tingkatan indeks KAMI.
6. Tingkat I – Dengan status "Kondisi Awal (Reaktif)"
    a. Pemahaman terhadap pentingnya pengelolaan keamanan informasi mulai terlihat.
    b. Penerapan dalam tingkat pengamanan masih bersifat tak beraturan, reaktif, tidak mengacu terhadap keseluruhan resiko dengan adanya jalur komunikasi tanpa pengawasan yang jelas.
    c. Tidak teridentifikasinya kelemahan teknis dan non-teknis.
    d. Tidak adanya kesadaran dan tanggung jawab dari pihak yang terlibat.
7. Tingkat II – Dengan status "Penerapan Kerangka Kerja Dasar (Aktif)"
    a. Belum terwujudnya keterkaitan terhadap pengaman meskipun pengamanan sudah diterapkan dengan tujuan untuk mendapatkan strategi proses bisnis yang efektif.

b. Tidak ada dokumentasi atau *file* rekaman resmi terhadap proses pengamanan.
c. Prosedur operasional yang akan diterapkan masih bergantung terhadap pengetahuan dan kemauan diri dari setiap individu.
d. Efektifitas bentuk keamanan informasi belum dapat dibuktikan secara menyeluruh.
e. Masih sering ditemukan kelemahan dalam pengelolaan pengamanan dan belum dapat diselesaikan oleh unit pelaksana ataupun pimpinan sehingga memberikan akibat terhadap perubahan.
f. Belum terdefinisikannya prioritas dalam pengelolaan keamanan
g. Masih banyak pihak-pihak yang terlibat yang belum sepenuhnya memahami tanggung jawab masing-masing.

8. Tingkat III – Dengan kondisi "Terdefinisi dan Konsisten (Pro Aktif)"
   a. Penerapan bentuk pengamanan sudah dilakukan dengan konsisten yang diikuti dengan pembuatan dokumentasi proses secara resmi
   b. Dilakukannya evaluasi secara bertahap terhadap efektifitas pengelolaan keamanan.
   c. Pimpinan dan pelaksana sudah dapat menangani apabila ditemukannya permasalahan yang terkait dengan pengelolaan keamanan, meskipun masih terdapat beberapa kelemahan.
   d. Telah tercapainya ambang batas minimun kerangka kerja pengamanan.
   e. Seluruh pihak sudah menyadari terhadap tanggung jawab pengelolaan masing-masing.

9. Tingkat IV – Dengan kondisi “Terkelola dan Terukur (Terkendali)”
    a. Dilakukannya pengamanan yang efektif terhadap pengelolan resiko.
    b. Dilakukan evaluasi dan pengukuran terhadap pencapaian tujuan pengamanan yang dilakukan dengan formal, bertahap dan terdokumentasi.
    c. Dilakukan evaluasi secara rutin terhadap penerapan pengamanan teknis agar efektif.
    d. Telah teridentifikasinya kelemahan pengelolaan keamanan informasi secara terstruktur dan konsisten dalam penindaklanjutan perbaikannya.
    e. Pengelolaan pengamanan yang bersifat pro-aktif serta dilakukan penerapan perbaikan demi terwujudnya suatu bentuk lain dari pengelolaan secara efisien.
    f. Peristiwa terhadap ketidakpatuhan diselesaikan dengan proses formal dengan mengidentifikasi akar masalahnya.
    g. Karyawan adalah bagian yang penting dalam terlaksananya keamanan informasi.
10. Tingkat V – Status kondisi “Optimal (Optimal)”
    a. Penerapan keseluruhan pengamanan dilakukan secara bertahap.
    b. Terintegrasinya pengelolaan resiko dan pengelolaan keamanan informasi.
    c. Dilakukan penilaian kinerja pengamanan secara berkelanjutan, yang mencakup analisis parameter efektifitas kontrol, bahasan akar permasalahan serta diterapkannya langkah-langkah dalam mengoptimalkan peningkatan kinerja.

d. Dalam melakukan peningkatan efektifitas keamanan informasi memerlukan tenanga karyawan yang pro-aktif.

2.4.5 Penetapan Sasaran Pengendalian

Untuk membangun suatu Sistem Manajemen Keamanan Informasi (SMKI) perlu dilakukannya penetapan sasaran pegendalian dan pengendalian sebagai langkah awal. Sasaran Pengendalian dan pengendalian tersebut telah didefinisikan dan diselaraskan dengan ISO/IEC 27001:2005 yang dimulai dari klausal 5 sampai klausal 15.

Tabel 2.7
Tabel Kontrol Keaman ISO/IEC 27001:2005

No.	Klausal	Sub Klausal	Sasaran Pengendalian
1.	A.5		Sasaran Mengenai Kebijakan Keamanan
		a. A.5.1	Kebijakan terhadap Keamanan Informasi
		1). A.5.1.1	Dokumen mengenai kebijakan keamanan informasi
		2). A.5.2.1	Kajian terhadap kebijakan keamanan informasi
2.	A.6		Organisasi mengenai Keamanan Informasi
		a. A.6.1	Organisasi Internal
		1) A.6.1.1	Serangkaian komitmen manajemen terhadap suatu keamanan informasi
		2) A.6.1.2	Koordinasi mengenai keamanan informasi
		3) A.6.1.3	Alokasi tanggung jawab keamanan informasi
		4) A.6.1.4	Proses otorisasi untuk memfasilitasi pengolahan informasi
		5) A.6.1.5	Perjanjian perihal kerahasiaan
		6) A.6.1.6	Adanya kontak terhadap pihak yang berkepentingan
		7) A.6.1.7	Kontak terhadap suatu kelompok khusus (*special interest*)
		8) A.6.1.8	Kajian yang independen terhadap keamanan informasi
		b. A.6.2	Perihal pihak Eksternal
		1) A.6.2.1	Identifikasi resiko dari pihak eksternal
		2) A.6.2.2	Penekanan keamanan ketika menjalin kontak dengan pelanggan

		3) A.6.2.3	Penekanan perjanjian terhadap pihak ketiga
3.	A.7		Perihal Tanggung Jawab Terhadap Aset
		a. A.7.1	Tanggung Jawab Terhadap Aset
		1) A7.1.1	Inventaris aset
		2) A.7.2.2	Kepemilikan aset
		3) A.7.2.3	Penerapan aset yang telah masuk
		b. A.7.2	Klasifikasi Informasi
		1) A.7.2.1	Pedoman Klasifikasi
		2) A.7.2.2	Pelabelan dan penanganan informasi
4.	A.8		Keamanan Sumber Daya Manusia
		a. A.8.1	Sebelum dipekerjakan
		1) A.8.1.1	Tanggung jawab dan fungsi
		2) A.8.1.2	Penyaringan (*screening*)
		3). A.8.1.3	Rumusan syarat dan aturan dalam kepegawaian
		b. A.8.2	Selama Bekerja
		1) A.8.2.1	Tanggung jawab manajemen
		2) A.8.2.2	Pendidikan, kepedulian, dan pelatihan pada keamanan informasi
		3) A.8.2.3	Proses pendisiplinan
		c. A.8.3	Pengakhiran atau Perubahan Pekerjaan
		1) A.8.3.1	Tanggung jawab pengakhiran pekerjaan
		2) A.8.3.2	Pegembalian aset
		3) A.8.3.3	Penghaapusan hak akses
5.	A.9		
		a. A.9.1	Area yang Aman
		1) A.9.1.1	Parameter keamanan fisik
		2) A.9.1.2	Pengendalian entri yang bersifat fisik
		3) A.9.1.3	Menjaga ruangan, kantor, atau fasilitas lainnya
		4) A.9.1.4	Penjagaan terhadap adanya ancaman eksternal dari lingkungan
		5) A.9.1.5	Bekerja di area yang aman
		6) A.9.1.6	Area akses publik dan bongkar muat
		b. A.9.2	Keamanan Peralatan
		1) A.9.2.1	Penempatan dan perlindungan peralatan
		2) A.9.2.2	Sarana pendukung
		3) A.9.2.3	Keamanan kabel
		4) A.9.2.4	Pemeliharaan peralatan
		5) A.9.2.5	Keamanan peralatan diluar lokasi
		6) A.9.2.6	Pembuangan atas penggunaan kembali peralatan dengan aman
		7) A.9.2.7	Pemindahan barang
6.	A.10		Pengelolaan Komunikasi dan Operasi
		a. A.10.1	Prosedur Operasional dan Tanggung Jawab

		1) A.10.1.1	Prosedur operasi yang terdokumentasi
		2) A.10.1.2	Pengelolaan perubahan
		3) A.10.1.3	Pemisahan tugas
		4) A.10.1.4	Pemisahan fasilitas pengujian, pembangunan, dan operasional
		b. A.10.2	Manajemen dalam Pelayanan Jasa Pihak Ketiga
		1) A.10.2.1	Pelayanan jasa
		2) A.10.2.2	Pemantauan dan pengkajian jasa pihak ketiga
		3) A.10.2.3	Pengelolaan perubahan terhadap jasa pihak ketiga
		c. A.10.3	Perencanaan dan Penerimaan Sistem
		1) A.10.3.1	Pengelolaan kapasitas
		2) A.10.3.2	Keberterimaan sistem
		d. A.10.4	Perlindungan terhadap *malicious and mobile code*
		1) A.10.4.1	Pengendalian terhadap *malicious code*
		2) A.10.4.2	Pengendalian terhadap *mobile code*
		e. A.10.5	Back-up
		1) A.10.5.1	*Back-up* informasi
		f. A.10.6	Manajemen Keamanan Jaringan
		1) A.10.6.1	Pengendalian jaringan
		2) A.10.6.2	Keamanan layanan jaringan
		g. A.10.7	Penanganan Media
		1) A.10.7.1	Manajemen yang dapat dipindahkan
		2) A.10.7.2	Pemusnahan media
		3) A.10.7.3	Prosedur penanganan informasi
		4) A.10.7.4	Keamanan dokumentasi sistem
		h. A.10.8	Pertukaran Informasi
		1) A.10.8.1	Aturan dan prosedur perihal pertukaran informasi
		2) A.10.8.2	Perjanjian dalam pertukaran
		3) A.10.8.3	Media fisik dalam transit
		4) A.10.8.4	Pesan elektronik
		5) A.10.8.5	Sistem informasi bisnis
		i. A.10.9	Layanan *E-Commerce*
		1) A.10.9.1	*Electronic Commerce*
		2) A.10.9.2	Transaksi online
		3) A.10.9.3	Aspek Informasi yang tersedia untuk umum
		j. A.10.10	Pemantauan
		1) A.10.10.1	*Log audit*
		2) A.10.10.2	Pemantauan penggunaan sistem
		3) A.10.10.3	Perlindungan informasi log
		4) A.10.10.4	*Log* Adiminstrator dan operator
		5) A.10.10.5	*Log* pada kesalahan yang terjadi

		6) A.10.10.6	Sinkronisasi penunjuk waktu
7.	A.11		Pengendalian Akses
		a. A.11.1	Persyaratan proses bisnis dalam Pengendalian Akses
		1) A.11.1.1	Kebijakan pengendalian akses
		b. A.11.2	Manajemen Akses Pengguna
		1) A.11.2.1	Pendaftaran pengguna
		2) A.11.2.2	Pengelolaan hak khsusus
		3) A.11.2.3	Manajemen *password* pengguna
		4) A.11.2.4	Tinjauan terhadap hak akses pengguna
		c. A.11.3	Tanggung Jawab Pengguna
		1) A.11.3.1	Penggunaan *password*
		2) A.11.3.2	Peralatan yang telah ditinggalkan oleh penggunanya
		3) A.11.3.3	Kebijakan *clear desk* dan *clear screen*
		d. A.11.4	Pengendalian Akses Jaringan
		1) A.11.4.1	Kebijakan mengenai penggunaan layanan jaringan
		2) A.11.4.2	Otentikasi pengguna untuk koneksi eksternal
		3) A.11.4.3	Identifikasi peralatan dalam jaringan
		4) A.11.4.5	Perlindungan terhadap *remote diagnostic* dan *configuration port*
		5) A.11.4.6	Segregasi dalam jaringan
		6) A.11.4.7	Pengendalian koneksi jaringan
		7) A.11.4.8	Pengendalian *routing* jaringan
		e. A.11.5	Pengendalian Akses Sistem Operasi
		1) A.11.5.1	Langkah log-on yang aman
		2) A.11.5.2	Proses identifikasi dan otentikasi pengguna
		3) A.11.5.3	Sistem manajemen *password*
		4) A.11.5.4	Penggunaan *system utilities*
		5) A.11.5.5	Sesi *time-out*
		6) A.11.5.6	Pembatasan waktu koneksi
		f. A.11.6	Pengendalian Akses Aplikasi dan Informasi
		1) A.11.6.1	Pembatasan akses informasi
		2) A.11.6.2	Isolasi sistem yang sensitif
		g. A.11.7	*Mobile Computing* dan Kerja Jarak Jauh (*Teleworking*)
		1) A.11.7.1	*Mobile Computing* dan komunikasi
		2) A.11.7.2	Kerja jarak jauh
8.	A.12	a. A.12.1	Pengembangan, Pemeliharaan, dan Akuisisi Sistem Informasi
		1) A.12.1.1	Persyaratan Keamanan dari Sistem Informasi
		b. A.12.2	Pengolahan yang Benar dalam Aplikasi

		1) A.12.2.1	Validasi dan masukan
		2) A.12.2.2	Pengendalian pengolahan internal
		3) A.12.2.3	Integritas pesan
		4) A.12.2.4	Validasi dan keluaran
		c. A.12.3	Pengendalian dengan Cara Kriptografi
		1) A.12.3.1	Kebijakan tentang hal penggunaan pengendalian kriptografi
		2) A.12.3.2	Manajemen kunci
		d. A.12.4	Keamanan *System Files*
		1) A.12.4.1	Pengendalian terhadap perangkat lunak yang operasional
		2) A.12.4.2	Perlindungan data uji sistem
		3) A.12.4.3	Pengendalian akses terhadap kode sumber program
		4) A.12.5.4	Kebocoran informasi
		5) A.12.5.5	Pengembangan perangkat lunak yang telah di alihdayakan
		f. A.12.6	Manajemen Kerawanan Teknis
		1) A.12.6.1	Pengendalian Kerawanan Teknis
9.	A.13		Manajemen Insiden Keamanan Informasi
		a. A.13.1	Melaporkan insiden dan Kelemahan dari Keamanan Informasi
		1) A.13.1.1	Melaporkan insiden terhadap keamanan informasi
		2) A.13.1.2	Pelaporan kelemahan keamanan
		b. A.13.2	Manajemen mengenai Insiden Keamanan Informasi dan perbaikan
		1) A.13.2.1	Tanggung jawab dan prosedur
		2) A.13.2.2	Pembelajaran dari insiden keamanan informasi
		3) A.13.2.3	Pengumpulan informasi
10.	A.14		Manajemen Keberlanjutan Bisnis (*Business Continuity Management*)
		a. A.14.1	Konsep Keamanan Informasi berdasarkan Manajemen Keberlanjutan Bisnis
		1) A.14.1.1	Memasukkan keamanan informasi ke dalam suatu proses manajemen keberlanjutan bisnis
		2) A.14.1.2	Keberlanjutan bisnis dan assesment resiko
		3) A.14.1.3	Pengembangan serta penerapan rencana keberlanjutan yang termasuk keamanan informasi
		4) A.14.1.4	Kerangka kerja perencanaan keberlanjutan bisnis

		5) A.14.1.5	Pengujian, pemeliharaan, dan assemen ulang rencana keberlanjutan bisnis
11.	A.15		Kesesuaia
		a. A.15.1	Kesesuaian dengan Persyaratan Hukum
		1) A.15.1.1	Identifikasi peraturan hukum yang berlaku
		2) A.15.1.2	Hak Kelayakan Intelektual (HAKI)
		3) A.15.1.3	Perlakuan pada perlindungan dokumentasi organisasi
		4) A.15.1.4	Perlakuan perlindungan data dan rahasia informasi pribadi
		5) A.15.1.5	Melakukan pencegahan penyalahgunaan fasilitas pengolahan informasi
		6) A.15.1.6	Disusunya regulasi pengendalian kriptografi
		b. A.15.2	Dilakukan pemenuhan terhadap standar Kebijakan Keamanan dan Pemenuhan Teknis
		1) A.15.2.1	Dilakukan pemenuhan terhadap standar kebijakan keamanan
		2) A.15.2.2	Dilakukan pengecekan pemenuhan teknis
		c. A.15.3	Pertimbangan Audit Sistem Informasi
		1) A.15.3.1	Dilakukan pengendalian audit sistem informasi
		2) A.15.3.2	Dilakukan perlindungan terhadap alat audit informsasi

2.5 Penilaian Resiko (*Risk Asessment*)

Penilaian Resiko (*Risk Asessment*) adalah langkah atau tahap pertama dari proses manajemen resiko. Penilaian resio bertujuan untuk mengetahui ancaman-ancaman (threat) dari luar yang berpotensi menggangu keamanan informasi organisasi dan potensial kelemahan (*vulnerability*) yang mungkin dimiliki oleh informasi di organisasi (Sarno, 2009). Metode penilaian resiko terdiri dari enam tahapan yaitu :

1. Identifikasi Aset
2. Identifikasi ancaman (*threat*)

3. Identifikasi Kelemahan (*vulnerability*)
4. Menentukan kemungkinan ancaman
5. Analisa dampak
6. Menentukan nilai resiko

2.6 *Asessment* Kontrak Kinerja (ICR)

Assessment kontrak kinerja pada ICR adalah landasan penilaian kontrak kinerja PT PJB untuk setiap unit yang dijadikan acuan untuk mengetahui kondisi suatu perusahaan saat ini dengan menghasilkan nilai maturity di tiap semester.

Asessment ICR PT PJB di bagi menjadi dua bagian yaitu *Asessment* Kinerja Proses dan *Assessment* Kinerja Hasil. *Assessment* kinerja proses merupakan landasan penilaian yang berupa nilai *maturity level* untuk setiap semester, sedangkan Assessment kinerja hasil merupakan landasan penilaian yang berupa nilai yang berasal dari KPI (*Key Performance Index*) dan menghasilkan nilai target yang ingin dicapai oleh ICR (Putranto, 2013).

Menurut PT PJB (2012), ICR merupakan suatu penilaian kontrak kinerja kesiapan informasi yang dimiliki oleh PT PJB yang mengatur masalah teknologi informasi dalam mengelola *infrastructure*, dan *bussiness process management* untuk keberlangsungan proses bisnisnya. *Infrastructure* menjelaskan tentang ketersediaan layanan dan kesiapan *infrastruktur. Bussiness Process Management* menjelaskan tentang peningkatan kompetensi pengguna dan konsistensi pengguna aplikasi TI (Putranto, 2013).

2.7 Penelitian Terkait

Daftar Penelitian terkait sebelumnya dapat dilihat pada tabel 2.1 berikut :

Tabel 2.8
Penelitian Terkait ISO/IEC 27001:2005

No.	Nama Peneliti dan Tahun	Masalah	Metode	Hasil
1.	**Nina Sulistiyowati**	Keamanan informasi	Kuantitatif	Daftar resiko yang akan dimitigasi menjadi acuan dalam penentuan kontrol keamanan. Resiko yang dimitigasi adalah resiko yang berhubungan dengan teknikal berjalannya sistem informasi sehingga kontrol yang dipilih adalah berdasarkan klausa yang berhubungan dengan teknikal
2	Raden Budiarto,2017	• Bagaimana kondisi tingkat perawan dan risiko keamanan pada sistem informasi organisasi XYZ saat ini? • Apa saja yang menjadi akar permasalahan yang potensi menimbulkan kerawanan atau kegagalan sistem informasi organisasi XYZ?	Kuantitatif	Penelitian ini telah berhasil membuktikan secara empiris melalui serangkaian hasil percobaan menunjukkan bahwa metode FMEA merupakan salah upaya nyata yang dapat dilakukan untuk mengetahui keadaan tingkat kerawanan dari sistem informasi, mengidentifikasi penyebab potensial dari berbagai bentuk kegagalan serta mengurutkan prioritas kegagalan berdasarkan nilai RPN.

		• Bagaimanakah model manajemen risiko keamanan informasi yang seharusnya diterapkan dalam upaya meningkatkan keamanan dan kehandalan sistem informasi di lingkungan organisasi XYZ?		
3.	Mochammad Arief Ramadhana	Evaluasi Keamanan Informasi	Penulis menggunakan standar ISO 27002 dalam pembuatan perangkat audit yang berfungsi sebagai perangkat untuk melakukan pemeriksaan rutin	sistem sesuai dengan klausul yang telah ditentukan sehingga risiko yang terjadi dapat teratas
4.	Merliana Halim, Haryanto Tanuwijaya, dan Ignatius Adrian Mastan	Audit Keamanan Sistem Informasi	Berdasarkan Standar ISO 27002	Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27002
5.	Farroh Sakinah, Bambang Setiawan	Indeks Penilaian Kematangan (*Maturity*) Manajemen Keamanan Layanan	manajemen TI menggunakan ITIL, COBIT dan ISO / IEC 27002 akan	kombinasi antara metodologi memberikan hasil yang lebih komprehensif dan efisien. Indeks penilaian yang dibuat memiliki fitur yang dikhususkan untuk organisasi penyelenggara layanan

				publik, terutama di perguruan tinggi sehingga fitur/pertanyaan yang ada di dalam indeks lebih bersifat khusus.
6.	Akhmad Zaki Al-Safi.	Keamanan dan Integritas Sistem Informasi Akuntansi	DBMS AS/400 dengan Basis Pengukuran COBIT 4.1 oleh	Manajemen keamanan dan pengendalian internal sistem informasi akuntansi di Bank DKI secara umum telah berjalan baik, walaupun masih ditemukan kekurangan dan kelemahan yang merupakan indikator tidak adanya peningkatan proses pengendalian aplikasi dan keamanan sistem informasi akuntansi.
7.	Nina Sulistiyowati	Analisa resiko menggunakan ISO 27001	ISO 27001	menunjukan tingkat resiko yang harus dimitigasi diperoleh kesimpulan bahwa (1) Klausa 8: keamanan sumber daya manusia, (2) Klausa 9: Keamanan fisik dan lingkungan, (3) Klausa 11: kontrol akses, dan (4) Klausa 12: Akuisisi sistem informasi pembangunan dan pemeliharaan. Hasil evaluasi menunjukan bahwa masih banyak aktivitas yang sebaiknya diperbaiki dan diterapkan untuk meningkatkan keamanan informasi di BPKD
8.	Rosmiati, Imam Riadi	Maturity level keamanan informasi	Kantor Biro Teknologi Informasi PT.	Nilai kesenjangan antara nilai maturity level saat ini dan nilai maturity

			XYZ berada pada level 2	level yang diharapkan adalah 0.79. Rekomendasi perbaikan yang diberikan membutuhkan pemahaman tentang perusahaan dan juga dibutuhkan koordinasi dengan pihak internal perusahaan.
9.	Herman Afandi1 Abdi Darmawan	Audit Kemanan Informasi Menggunakan ISO 27002	Manajemen keamanan sistem informasi	Hasil audit keamanan sistem informasi yang telah dilakukan, maka didapatkan kesimpulan yaitu pada bidang Keamanan Sumber Daya Manusia (Klausul 7) menghasilkan nilai maturity level 2.71 dan pada bidang Kontrol Akses (Klausul 9) memiliki nilai maturity level 2,75 dan bidang Keamanan Fisik dan Lingkungan (Klausul 11) kemanan sumber daya manuia menghasilkan nilai maturity level 2.75 yaitu berada pada level 2 (limited/repeatable) yang berarti kontrol keamanan sedang dalam pengembangan, sudah ada dokumentasi terbatas tetapi belum ada pelatihan dan pengukuran efektifitas kontrol keamanan, dan bidang oprasional (Klausul 12) menghasilkan nilai maturity level 1,33 yaitu berada pada level Level 2 (limited/repeatable) Pada level ini, kontrol

				keamanan masih dalam pengembangan dan/atau ada dokumentasi terbatas untuk mendukung kebutuhan. Diharapkan PT. GIGA PATRA MULTIMEDIA dapat melakukan perbaikan manajemen keamanan sistem informasi, aturan, dan prosedur keamanan sistem informasi agar ancaman-ancaman terkait keamanan informasi dapat diminimalisir
10	Yuli Praptomo	Informasi merupakan komoditi yang sangat penting bagi sebuah organisasi baik comersial maupun individual		Kemampuan untuk mengakses dan menyediakan informasi secara tepat dan akurat menjadi suatu hal yang sangat esensial. Keamanan itu tidak dapat muncul demikian saja. Dia harus direncanakan. Jika tidak kita budgetkan di awal, kita akan dikagetkan dengan kebutuhan akan adanya perangkat pengamanan (firewall, Intrusion Detection System, anti virus, Dissaster Recovery Center, dan seterusnya). Pengelolaan terhadap keamanan dapat dilihat dari sisi pengelolaan resiko (risk management). Lawrie Brown dalam menyarankan menggunakan "*Risk Management Model*" untuk menghadapi

				ancaman (*managing threats*). Ada tiga komponen yang memberikan kontribusi kepada Risk, yaitu *Asset*, *Vulnerabilities*, dan *Threats*. Kejahatan komputer dapat digolongkan kepada yang sangat berbahaya sampai ke yang hanya mengesalkan (*annoying*). Menurut David Icove berdasarkan lubang keamanan, keamanan dapat diklasifikasikan menjadi empat, yaitu: Keamanan yang bersifat fisik, Keamananyang berhubungan dengan orang, Keamanan dari data dan media serta teknik komunikasi, Keamanan dalam operasi

Berdasarkan jurnal-jurnal yang telah dipaparkan diatas dapat disimpulkan, bahwa standar ISO/IEC 27001:2005 digunakan dalam audit terhadap keamanan sistem informasi. Penelitian ini juga akan menggunakan metode-metode yang sama dengan metode yang dipakai dari jurnal-jurnal terdahulu, namun sedikit berbeda dengan menggunakan kombinasi dari penelitian yang ada.