

**EVALUASI KEAMANAN INFORMASI  
MENGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI)  
(STUDI KASUS: SEKRETARIAT DPRD KOTA CIMAHI)**

**TUGAS AKHIR**

Disusun sebagai salah satu syarat untuk kelulusan Program Strata 1,  
di Program Studi Teknik Informatika, Universitas Pasundan Bandung

oleh :

Albar Agista  
NRP : 13.304.0096



**PROGRAM STUDI TEKNIK INFORMATIKA  
FAKULTAS TEKNIK  
UNIVERSITAS PASUNDAN BANDUNG  
NOVEMBER 2018**

**LEMBAR PENGESAHAN  
LAPORAN TUGAS AKHIR**

Telah diujikan dan dipertahankan dalam Sidang Sarjana Program Studi Teknik Informatika Universitas Pasundan Bandung, pada hari dan tanggal sidang sesuai berita acara sidang, tugas akhir dari :

Nama : Albar Agista  
Nrp : 13.304.0096

Dengan judul :

**“EVALUASI KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN  
INFORMASI (KAMI)”**

(Studi Kasus : SEKRETARIAT DPRD Kota Cimahi)



Pembimbing Utama,

Pembimbing Pendamping,

(Doddy Ferdiansyah, S.T, M.T)

(Iwan Kurniawan, S.T, M.T.)

## LEMBAR PERNYATAAN KEASLIAN TUGAS AKHIR

Saya menyatakan dengan sesungguhnya bahwa :

1. Tugas akhir ini adalah benar-benar asli dan belum pernah diajukan untuk mendapatkan gelar akademik, baik di Universitas Pasundan Bandung maupun di Perguruan Tinggi lainnya
2. Tugas akhir ini merupakan gagasan, rumusan dan penelitian saya sendiri, tanpa bantuan pihak lain kecuali arahan dari tim Dosen Pembimbing
3. Dalam tugas akhir ini tidak terdapat karya atau pendapat orang lain, kecuali bagian-bagian tertentu dalam penulisan laporan Tugas Akhir yang saya kutip dari hasil karya orang lain telah dituliskan dalam sumbernya secara jelas sesuai dengan norma, kaidah, dan etika penulisan karya ilmiah, serta disebutkan dalam Daftar Pustaka pada tugas akhir ini
4. Kakas, perangkat lunak, dan alat bantu kerja lainnya yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab saya, bukan tanggung jawab Universitas Pasundan Bandung

Apabila di kemudian hari ditemukan seluruh atau sebagian laporan tugas akhir ini bukan hasil karya saya sendiri atau adanya plagiasi dalam bagian-bagian tertentu, saya bersedia menerima sanksi akademik, termasuk pencabutan gelar akademik yang saya sandang sesuai dengan norma yang berlaku di Universitas Pasundan, serta perundang-undangan lainnya



Bandung, 29 November 2018

Yang membuat pernyataan,

Materai  
6000,-

( Albar Agista )

NRP. 13.304.0096

## ABSTRAK

Dewan Perwakilan Rakyat Daerah (DPRD) Kota Cimahi mempunyai divisi-divisi untuk melancarkan proses bisnis dalam menunjang pekerjaan sehari-hari. Penelitian ini dibatasi lingkup, penelitian ini dilakukan di bagian IT & Multimedia yang terdapat di Sub Bagian Umum. Bagian IT & Multimedia tidak masuk kedalam struktur organisasi yang ada di Sekretariat DPRD Kota Cimahi. Bagian IT & Multimedia yang memiliki tugas dan pokok, dan fungsi salah satunya adalah *support* IT merencanakan kegiatan, melaksanakan, dan membagi tugas mengenai di Sekretariat DPRD Kota Cimahi.

Salah satu upaya yang dapat dilakukan untuk meningkatkan kualitas dari keamanan informasi, kementerian Kominfo membuat alat bantu untuk mengukur tingkat kematangan dan kelengkapan dalam keamanan informasi yang disebut dengan Indeks Keamanan Informasi (KAMI). Penggunaan Indeks KAMI ini juga diikuti dengan penerapan ISO 27001 sebagai standar keamanan internasional yang dapat membantu sebuah organisasi memastikan bahwa keamanan informasi yang diterapkan sudah efektif.

Hasil dari penelitian ini adalah sebuah usulan perbaikan bagi bagian IT dan Multimedia Sekretariat DPRD Kota Cimahi berdasarkan hasil penilaian menggunakan Indeks KAMI dan usulan dari ISO27002.

Kata kunci : Indeks KAMI, Indeks KAMI v3.1, Keamanan Informasi, ISO27001



## ABSTRACT

Dewan Perwakilan Rakyat Daerah (DPRD) of Cimahi City has divisions to launch business processes to support daily work. This research is limited in scope, this research is carried out in by IT & Multimedia section which is in the General Sub-Section. The IT & Multimedia section is not included in the organizational structure in the Sekretariat DPRD of Cimahi City. The IT & Multimedia section has the duties and principal, and the function of one of them is to support IT to plan activities, implement, and share tasks in Sekretariat DPRD of Cimahi City.

One effort that can be done to improve the quality of information security, the Ministry of Communication and Information Technology (KOMINFO) makes a tool to measure the level of maturity and completeness in information security, which is called the Index Keamanan Informasi (KAMI). The use of the Indeks KAMI is also followed by the application of ISO 27001 as an international security standard that can help an organization ensure that the information security implemented is effective.

The results of this study are a proposed improvement for the IT and Multimedia section of the Sekretariat DPRD of Cimahi City based on the results of the assessment using the Indeks KAMI and the suggestion from ISO27002.

Keywords : Indeks KAMI, Indeks KAMI v3.1, Information System, ISO27001



## KATA PENGANTAR

Puji syukur ke hadirat kepada Allah SWT yang telah melimpahkan rahmat dan berkahnya sehingga penulis membuat Laporan Tugas Akhir dengan judul “EVALUASI KEAMANAN INFORMASI MENGGUNAKAN INDEKS KEAMANAN INFORMASI (KAMI) (STUDI KASUS: DPRD KOTA CIMAHI)”.

Penulis menyadari laporan ini dapat terwujud berkat bantuan dan dorongan dari berbagai pihak. Maka pada kesempatan ini penulis sampaikan terima kasih yang sebesar-besarnya atas segala bantuan yang penulis terima baik secara moril maupun materil, sehingga penulis dapat menyelesaikan laporan ini kepada :

1. Kedua pembimbing, Bapak Doddy Ferdiansyah, S.T, M.T selaku pembimbing utama dan Bapak Ir. Iwan Kurniawan, M.T sebagai pembimbing pendamping.
2. Kepada Orang Tua tersayang, dan keluarga yang selalu memberikan motivasi serta do'anya dalam pembuatan tugas akhir ini.
3. Koordinator Tugas Akhir dan Ketua Kelompok Keilmuan serta seluruh civitas akademika Teknik Informatika di Universitas Pasundan Bandung, yang telah memberikan bekal ilmu selama penulis menimba ilmu.
4. Kepada Nuke Juniarti yang senantiasa membantu penulis dalam pengerjaan Tugas Akhir ini.
5. Kepada teman-teman seperjuangan Universitas Pasundan Bandung yang tidak bisa semua penulis sebutkan.
6. Kepada Ibu Rita Rijayanti, S.T, M.T selaku dosen penguji.

Tiada gading yang tak retak, tiada gelombang tanpa ombak, segala kesalahan merupakan kelemahan dan kekurangan penulis. oleh karena itu, penulis harapkan kritik dan saran dari semua pihak demi perbaikan di masa yang akan datang.

Akhir kata, semoga penulisan laporan ini dapat bermanfaat bagi penulis dan bagi perkembangan ilmu Teknologi dimasa yang akan datang.

Bandung, 29 November 2018

Penulis

## DAFTAR ISI

BAB 1 PENDAHULUAN .....	1-1
1.1. LATAR BELAKANG .....	1-1
1.2. IDENTIFIKASI MASALAH .....	1-2
1.3. TUJUAN TUGAS AKHIR .....	1-2
1.4. LINGKUP TUGAS AKHIR .....	1-3
1.5. METODOLOGI TUGAS AKHIR .....	1-3
1.6. SISTEMATIKA TUGAS AKHIR .....	1-4
BAB 2 LANDASAN TEORI .....	2-1
2.1. PENGERTIAN EVALUASI .....	2-1
2.2. KEAMANAN INFORMASI .....	2-1
2.2.1. PENGERTIAN INFORMASI .....	2-1
2.2.2. PENGERTIAN KEAMANAN INFORMASI .....	2-1
2.2.3. ASPEK KEAMANAN INFORMASI .....	2-1
2.2.4. ANCAMAN TERHADAP KEAMANAN INFORMASI .....	2-2
2.3. SISTEM MANAJEMEN KEAMANAN INFORMASI .....	2-3
2.3.1. PENDUKUNG SMKI .....	2-3
2.3.2. ISO/IEC 27001 SEBAGAI STANDAR SMKI .....	2-4
2.4. DEFINISI ASET .....	2-5
2.4.1. ASET SUMBER DAYA MANUSIA .....	2-5
2.4.2. ASET DATA .....	2-5
2.4.3. ASET HARDWARE .....	2-5
2.4.4. ASET SOFTWARE .....	2-5
2.4.5. ASET DATABASE .....	2-6
2.4.6. ASET NETWORK .....	2-6
2.5. INDEKS KAMI .....	2-6
2.5.1. PENGERTIAN INDEKS KAMI .....	2-6
2.5.2. PETUNJUK PENGGUNAAN ALAT EVALUASI INDEKS KAMI .....	2-6
2.5.3. PERBEDAAN INDEKS KAMI VERSI 2.3 & INDEKS KAMI VERSI 3.1 .....	2-13
2.6. KUESIONER PENGUKURAN AREA PENELITIAN .....	2-14
2.6.1. KATEGORI SISTEM ELEKTRONIK .....	2-15
2.6.2. PEMETAAN KLAUSUL ISO/IEC 27001:2013 DENGAN PERTANYAAN INDEKS KAMI VERSI 3.1 .....	2-15
2.7. PENGKAJIAN HASIL INDEKS KAMI .....	2-21
2.8. DIAGRAM SEBAB AKIBAT .....	2-23
2.8.1. KARAKTERISTIK DIAGRAM SEBAB DAN AKIBAT .....	2-23
2.9. PENELITIAN TERDAHULU .....	2-24
BAB 3 SKEMA PENELITIAN .....	3-1
3.1. ALUR PENELITIAN .....	3-1

3.2	ANALISIS MASALAH DAN SOLUSI TA .....	3-3
3.2.1	FISHBONE DIAGRAM .....	3-3
3.3	KERANGKA PEMIKIRAN TEORITIS .....	3-4
3.3.1	SKEMA ANALISIS .....	3-5
3.4	PROFIL OBJEK DAN TEMPAT PENELITIAN.....	3-6
3.4.1	STRUKTUR ORGANISASI .....	3-6
BAB 4 ANALISIS .....		4-1
4.1	PENENTUAN PENDEKATAN ANALISIS .....	4-1
4.1.1	PENGUMPULAN DATA .....	4-1
4.1.2	ANALISIS ASET TEKNOLOGI INFORMASI DAN IDENTIFIKASI ANCAMAN .....	4-2
4.1.2.1	ASET TEKNOLOGI INFORMASI .....	4-2
4.1.2.2	IDENTIFIKASI ANCAMAN .....	4-3
4.2	ANALISIS KONDISI SAAT INI .....	4-3
4.3	HASIL PENGISIAN KUESIONER INDEKS KAMI V.3.1 .....	4-4
4.3.1	HASIL PENGISIAN KUESIONER KATEGORI SISTEM ELEKTRONIK .....	4-6
4.4	HASIL PENGISIAN KUESIONER TINGKAT KEMATANGAN AREA KEAMANAN INFORMASI 4-7	
4.4.1	HASIL PENGISIAN KUESIONER TATA KELOLA KEAMANAN INFORMASI .....	4-7
4.4.2	HASIL PENGISIAN KUESIONER KERANGKA KERJA PENGELOLAAN KEAMANAN INFORMASI .....	4-11
4.4.3	HASIL PENGISIAN KUESIONER PENGELOLAAN ASET INFORMASI .....	4-14
4.4.4	HASIL PENGISIAN KUESIONER TEKNOLOGI DAN KEAMANAN INFORMASI .....	4-16
BAB 5 PEMBAHASAN .....		5-1
5.1	TINGKAT KELENGKAPAN PENERAPAN SMKI .....	5-1
5.2	TINGKAT KEMATANGAN SMKI .....	5-2
5.3	USULAN PERBAIKAN .....	5-7
5.3.1	USULAN PERBAIKAN AREA TATA KELOLA KEAMANAN INFORMASI.....	5-7
5.3.2	USULAN PERBAIKAN AREA PENGELOLAAN RISIKO KEAMANAN INFORMASI.....	5-8
5.3.3	USULAN PERBAIKAN AREA KERANGKA KERJA PENGELOLAAN KI .....	5-10
5.3.4	USULAN PERBAIKAN AREA PENGELOLAAN ASET INFORMASI .....	5-14
5.3.5	USULAN PERBAIKAN AREA TEKNOLOGI DAN KEAMANAN INFORMASI .....	5-20
BAB 6 KESIMPULAN DAN SARAN .....		6-1
6.1	KESIMPULAN .....	6-1
6.2	SARAN .....	6-2
LAMPIRAN .....		6-1



## DAFTAR TABEL

Tabel 1.1 Daftar Istilah.....	x
Tabel 2.1 Penelitian terdahulu .....	2-24
Tabel 2.2 Skor Tingkat Kepentingan [TIM11] .....	2-8
Tabel 2.3 Perbedaan Indeks KAMI ver. 2.3 dan Indeks KAMI ver.3.1 [BAS17] .....	2-14
Tabel 2.4 Bagian II : Tata Kelola Keamanan Informasi [BAS17] .....	2-16
Tabel 2.5 Bagian III : Pengelolaan Risiko Keamanan Informasi [BAS17] .....	2-17
Tabel 2.6 Bagian IV : Kerangka Kerja Pengelolaan Keamanan Informasi [BAS17] .....	2-17
Tabel 2.7 Bagian V : Pengelolaan Aset Informasi [BAS17].....	2-19
Tabel 2.8 Bagian VI : Teknologi dan Keamanan Informasi [BAS17] .....	2-20
Tabel 3.1 Skema Analisis .....	3-6
Tabel 3.2 Deskripsi Kerja.....	3-7
Tabel 4.1 Ringkasan Wawancara .....	4-1
Tabel 4.2 Daftar Narasumber yang melakukan pengisian kuesioner.....	4-2
Tabel 4.3 Aset Teknologi Informasi .....	4-2
Tabel 4.4 Identifikasi Ancaman .....	4-3
Tabel 4.5 Format tabel skor penghitungan KSE .....	4-4
Tabel 4.6 Format skor penghitungan untuk 4 (empat) tingkat area kematangan .....	4-5
Tabel 4.7 Kategori Sistem Elektronik .....	4-6
Tabel 4.8 Skor Kategori Sistem Elektronik .....	4-7
Tabel 4.9 Hasil Pengisian Kuesioner Tata Kelola Keamanan Informasi .....	4-7
Tabel 4.10 Skor Tata Kelola Keamanan Informasi .....	4-9
Tabel 4.11 Hasil Pengisian Kuesioner Kategori Pengelolaan Risiko Keamanan Informasi .....	4-10
Tabel 4.12 Skor Kategori Pengelolaan Risiko Keamanan Informasi .....	4-11
Tabel 4.13 Hasil Pengisian Kuesioner Kategori Pengelolaan Keamanan Informasi .....	4-11
Tabel 4.14 Skor Kategori Kerangka Kerja Pengelolaan Keamanan Informasi .....	4-13
Tabel 4.15 Hasil Pengisian Kuesioner Pengelolaan Aset Informasi .....	4-14
Tabel 4.16 Skor Pengelolaan Aset Informasi .....	4-16
Tabel 4.17 Hasil Pengisian Kuesioner Teknologi dan Keamanan Informasi.....	4-17
Tabel 4.18 Skor Teknologi dan Keamanan Informasi .....	4-18
Tabel 5.1 Tingkat Kematangan Area Keamanan Informasi .....	5-2
Tabel 5.2 Kondisi tingkat kematangan Sekretariat DPRD Kota Cimahi .....	5-4
Tabel 5.3 Tingkat Kematangan kategori Tata kelola keamanan informasi .....	5-4
Tabel 5.4 Tingkat Kematangan kategori Pengelolaan risiko keamanan informasi .....	5-5
Tabel 5.5 Tingkat Kematangan kategori Kerangka kerja keamanan informasi .....	5-5
Tabel 5.6 Tingkat Kematangan kategori pengelolaan aset keamanan informasi .....	5-6
Tabel 5.7 Tingkat Kematangan kategori teknologi dan keamanan informasi .....	5-7

Tabel 5.8 Usulan perbaikan Tata Kelola Keamanan Informasi .....	5-7
Tabel 5.9 Usulan perbaikan Pengelolaan Risiko Keamanan Informasi (1) .....	5-8
Tabel 5.10 Usulan perbaikan Pengelolaan Risiko Keamanan Informasi (2) .....	5-8
Tabel 5.11 Usulan perbaikan Pengelolaan Risiko Keamanan Informasi (3) .....	5-8
Tabel 5.12 Usulan perbaikan Pengelolaan Risiko Keamanan Informasi (4) .....	5-9
Tabel 5.13 Usulan perbaikan Pengelolaan Risiko Keamanan Informasi (5) .....	5-9
Tabel 5.14 Usulan perbaikan Pengelolaan Risiko Keamanan Informasi (6) .....	5-10
Tabel 5.15 Usulan perbaikan Kerangka Kerja Pengelolaan KI (1).....	5-10
Tabel 5.16 Usulan perbaikan Kerangka Kerja Pengelolaan KI (2).....	5-11
Tabel 5.17 Usulan perbaikan Kerangka Kerja Pengelolaan KI (3).....	5-11
Tabel 5.18 Usulan perbaikan Kerangka Kerja Pengelolaan KI (4).....	5-11
Tabel 5.19 Usulan perbaikan Kerangka Kerja Pengelolaan KI (5).....	5-12
Tabel 5.20 Usulan perbaikan Kerangka Kerja Pengelolaan KI (6).....	5-13
Tabel 5.21 Usulan perbaikan Kerangka Kerja Pengelolaan KI (7).....	5-13
Tabel 5.22 Usulan perbaikan Kerangka Kerja Pengelolaan KI (8).....	5-14
Tabel 5.23 Usulan perbaikan Kerangka Kerja Pengelolaan KI (9).....	5-14
Tabel 5.24 Usulan perbaikan Pengelolaan Aset Informasi (1) .....	5-14
Tabel 5.25 Usulan perbaikan Pengelolaan Aset Informasi (2) .....	5-15
Tabel 5.26 Usulan perbaikan Pengelolaan Aset Informasi (3) .....	5-15
Tabel 5.27 Usulan perbaikan Pengelolaan Aset Informasi (4) .....	5-17
Tabel 5.28 Usulan perbaikan Pengelolaan Aset Informasi (5) .....	5-18
Tabel 5.29 Usulan perbaikan Pengelolaan Aset Informasi (6) .....	5-19
Tabel 5.30 Usulan perbaikan Pengelolaan Aset Informasi (7) .....	5-19
Tabel 5.31 Usulan perbaikan Teknologi dan KI (1) .....	5-20
Tabel 5.32 Usulan perbaikan Teknologi dan KI (2) .....	5-21
Tabel 5.33 Usulan perbaikan Teknologi dan KI (3) .....	5-21
Tabel 5.34 Usulan perbaikan Teknologi dan KI (4) .....	5-22
Tabel 5.35 Usulan perbaikan Teknologi dan KI (5) .....	5-23
Tabel 5.36 Usulan perbaikan Teknologi dan KI (6) .....	5-23
Tabel 5.37 Usulan perbaikan Teknologi dan KI (7) .....	5-24

## DAFTAR GAMBAR

Gambar 2.1 Aspek Keamanan Informasi .....	2-2
Gambar 2.2 Pemetaan Skor [TIM11] .....	2-8
Gambar 2.3 Ilustrasi Evaluasi Kematangan [DIR15] .....	2-9
Gambar 2.4 Korelasi Kategori Sistem Elektronik pada Indeks KAMI [DIR15] .....	2-9
Gambar 2.5 Tingkat kematangan pada Indeks KAMI [TIM11] .....	2-11
Gambar 2.6 Gambaran Definisi Evaluasi Tingkat Kematangan [TIM11] .....	2-12
Gambar 2.7 Ilustrasi Diagram Radar Indeks KAMI [DIR15] .....	2-22
Gambar 2.8 Ilustrasi dashboard evaluasi akhir Indeks KAMI [DIR15] .....	2-22
Gambar 2.9 Diagram Sebab dan Akibat [KEL95] .....	2-24
Gambar 3.1 Alur Penelitian .....	3-3
Gambar 3.3 Fishbone Diagram .....	3-4
Gambar 3.4 Kerangka Pemikiran Teoritis .....	3-4
Gambar 3.2 Skema Analisis .....	3-5
Gambar 3.5 Struktur Organisasi .....	3-6
Gambar 5.1 Tingkat Kelengkapan Penerapan SMKI di Sekretariat DPRD Kota Cimahi .....	5-1
Gambar 5.2 Diagram Radar Tingkat Kelengkapan Penerapan SMKI pada Sekretariat DPRD Kota Cimahi .....	5-1
Gambar 5.3 Tingkat Kelengkapan Penerapan SMKI di Sekretariat DPRD Kota Cimahi .....	5-2



## DAFTAR LAMPIRAN

LAMPIRAN A REKOMENDASI PENELITIAN .....	A-1
LAMPIRAN B BERITA ACARA OBSERVASI .....	B-1
LAMPIRAN C DOKUMEN PENDUKUNG PENELITIAN .....	C-1



## DAFTAR ISTILAH

Tabel 1.1 merupakan deskripsi untuk istilah-istilah yang digunakan dalam laporan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI.

Tabel 1.1 Daftar Istilah

No.	Istilah	Deskripsi
1	TIK	Teknologi Informasi dan Komunikasi.
2	Indeks KAMI	Sebuah <i>tools</i> untuk mengukur tingkat kematangan dan kepatuhan keamanan informasi yang dikeluarkan oleh Kominfo.
3	ITE	Informasi dan Transaksi Elektronik
4	DOS/DDOS	Metode serangan untuk menghabiskan sumber daya sebuah peralatan jaringan komputer.
5	<i>Sniffing</i>	Metode pencurian data dengan cara mendengarkan seluruh paket yang lewat pada sebuah media komunikasi.
6	<i>IP Spoofing</i>	Metode serangan dimana penyerang menempatkan diri di antara 2 <i>host</i> yang sedang berkomunikasi.
7	<i>Remote Attack</i>	Bentuk serangan terhadap suatu mesin dimana penyerang dilakukan dari jarak jauh diluar sistem jaringan atau media transisi.
8	<i>Password</i>	Kumpulan karakter yang digunakan oleh pengguna jaringan atau sebuah sistem operasi untuk memverifikasi identitas dirinya kepada sistem keamanan.
9	<i>Host</i>	Sistem komputer yang diakses oleh pengguna yang digunakan jika ada dua sistem komputer yang terhubung dengan modem dan saluran telepon.
10	Kriptografi	Ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi, seperti kerahasiaan data.
11	URL	<i>Uniform Resource Locator</i> merupakan rangkaian karakter menurut suatu format standar tertentu, yang digunakan untuk menunjukkan alamat suatu sumber seperti dokumen dan gambar di internet.
12	<i>Malware</i>	Perangkat lunak berbahaya yang dirancang untuk merusak atau melakukan tindakan yang tidak diinginkan terhadap sistem komputer, seperti virus.
13	SMKI (Sistem Manajemen Keamanan Informasi)	Suatu proses yang disusun berdasarkan pendekatan risiko bisnis untuk merencanakan, mengimplementasikan, memonitor dan meninjau ulang serta memelihara dan meningkatkan atau mengembangkan terhadap Keamanan Informasi.
14	PDCA (Plan-Do-Check-Act)	Proses atau gambaran yang memperlihatkan persyaratan keamanan informasi.
15	<i>Hardware</i>	Konsep sumber daya meliputi semua peralatan dan bahan fisik yang digunakan dalam pemrosesan informasi.
16	<i>Software</i>	Konsep sumber daya meliputi semua rangkaian perintah pemrosesan informasi.
17	ISO	<i>International Standard Organization</i> , standar pendembang terbesar di dunia yang bertanggungjawab dalam mengoordinasikan penyusunan standar.
18	COBIT	<i>Control Objective for Information &amp; Related Technology</i> , sekumpulan dokumentasi untuk <i>IT Governance</i> yang dapat membantu pengguna atau manajemen untuk kebutuhan kontrol dan masalah-masalah teknis IT.
19	<i>Monitoring</i>	Suatu proses untuk menyediakan informasi tentang sejauh mana suatu kegiatan tertentu telah dicapai, bagaimana perbedaan pencapaian itu dengan suatu standar tertentu untuk mengetahui apakah ada selisih di antara keduanya, serta bagaimana manfaat yang telah dikerjakan itu bila dibandingkan dengan harapan-harapan yang ingin diperoleh
20	Audit	Evaluasi terhadap suatu organisasi, sistem, proses, atau produk.
21	HAKI	Hak Atas Kekayaan Intelektual (HAKI)
22	<i>Security Patch</i>	Sebuah perubahan yang diaplikasikan ke sebuah perangkat lunak untuk memperbaiki kelemahan atau celah keamanan yang ada
23	<i>Compensating Control</i>	<i>Compensating Control</i> atau pengendalian pengganti merupakan salah satu sistem pengendalian manajemen yaitu, untuk memperkuat pengendalian karena terabaikannya suatu aktivitas pengendalian.
24	<i>Business Continuity Planning (BCP)</i>	Mengenai pembuatan perencanaan dan <i>frame-work</i> untuk menjamin bahwa proses bisnis dapat terus berlanjut dalam keadaan darurat.
25	<i>Disaster Recovery Plan (DRP)</i>	Mengenai pemulihan cepat dari keadaan darurat atau bencana, sehingga hanya mengakibatkan dampak minimum bagi organisasi atau perusahaan.
26	<i>Otentikasi</i>	Verifikasi apakah seseorang itu adalah orang yang berhak.
27	<i>User</i>	Pengguna suatu sistem.
28	<i>User Access Review</i>	Penggunaan akses.
29	<i>User Access Rights</i>	Hak akses.
30	<i>Outsource</i>	Penggunaan tenaga kerja dari luar perusahaan sendiri untuk melaksanakan tugas atau pekerjaan tertentu yang spesifik.

No.	Istilah	Deskripsi
31	<i>Log</i>	Catatan tentang peristiwa yang terjadi dalam sistem organisasi dan jaringan.
32	<i>Lockout</i>	Fitur keamanan yang akan mengunci jika beberapa kali memasukkan <i>username</i> atau <i>password</i> yang tidak sesuai.
33	<i>Antimalware</i>	Antivirus.
34	<i>Fishbone</i>	Salah satu metode dalam menyelesaikan sebuah masalah.
35	<i>Head</i>	Bagian kepala dari fishbone.
36	<i>Spine</i>	Bagian tulang belakang dari fishbone.
37	<i>Bones</i>	Bagian tulang dari fishbone.



# BAB 1

## PENDAHULUAN

Bab ini berisi penjelasan umum mengenai usulan penelitian yang dilakukan dalam pengerjaan tugas akhir. Di dalamnya berisi latar belakang tugas akhir, identifikasi masalah, tujuan tugas akhir, lingkup tugas akhir, metodologi yang digunakan dalam pengerjaan tugas akhir, dan sistematika penulisan laporan tugas akhir.

### 1.1. Latar Belakang

Perkembangan teknologi informasi yang dipandang saat ini sebagai media pendukung organisasi seperti perusahaan maupun instansi pemerintahan dalam mencapai tujuan bisnis dari organisasi tersebut. Penggunaan teknologi informasi yang efektif dan efisien merupakan cita-cita bagi setiap organisasi. Informasi merupakan aset yang bernilai bagi organisasi maupun sistem yang perlu dilindungi dari ancaman yang mungkin terjadi, baik dari pihak luar maupun pihak dalam dari organisasi itu sendiri. Kejahatan terhadap informasi kini semakin banyak, banyak oknum yang melakukan hal tersebut memanfaatkan titik kelemahan terhadap sistem yang ada sehingga dapat merugikan pihak-pihak bersangkutan. Kinerja teknologi informasi akan terganggu apabila keamanan informasi sebagai aspek keamanan informasi mengalami masalah terkait kerahasiaannya (*confidentiality*), keutuhannya (*integrity*), dan ketersediaannya (*availability*) [SAR09].

Hal ini juga perlu diterapkan dan diperhatikan di Sekretariat DPRD Kota Cimahi. Sekretariat DPRD Kota Cimahi sebagai salah satu Satuan Organisasi Perangkat Daerah (SOPD) Pemerintah Kota Cimahi yang mempunyai tugas utama melaksanakan tugas dan fungsinya sebagai fasilitator kepada Pimpinan dan anggota Dewan Perwakilan Rakyat Daerah Kota Cimahi. Sekretariat DPRD Kota Cimahi ini merupakan salah satu instansi pemerintahan, yang dimana salah satu sumber dananya berasal dari APBD (Anggaran Pendapatan Belanja Daerah).

Dewan Perwakilan Rakyat Daerah (DPRD) Kota Cimahi mempunyai divisi-divisi untuk melancarkan proses bisnis dalam menunjang pekerjaan sehari-hari. Penelitian ini dibatasi lingkup, penelitian ini dilakukan di bagian IT & Multimedia yang terdapat di Sub Bagian Umum. Bagian IT & Multimedia tidak masuk kedalam struktur organisasi yang ada di Sekretariat DPRD Kota Cimahi. Bagian IT & Multimedia yang memiliki tugas dan pokok, dan fungsi salah satunya adalah *support* IT merencanakan kegiatan, melaksanakan, dan membagi tugas mengenai di Sekretariat DPRD Kota Cimahi.

Data dari bagian IT & Multimedia di Sekretariat DPRD Kota Cimahi menyatakan bahwa ditemukannya beberapa celah keamanan sistem informasi dan jaringan yang cukup berbahaya. Gangguan keamanan informasi tersebut juga dirasakan oleh pihak pegawai Sekretariat DPRD, seperti pernah terjadinya pembobolan data keuangan yang terjadi. Selain itu, pernah terjadi infeksi virus yang berpusat di Pemerintah Kota (PemKot) Kota Cimahi yang menyebar ke beberapa instansi. Yang mengakibatkan kerugian kebocoran data informasi.

Salah satu upaya yang dapat dilakukan oleh Kementrian Kominfo Republik Indonesia mengeluarkan media *tools*, yaitu Indeks Keamanan Informasi (KAMI). Indeks Keamanan Informasi

(KAMI) merupakan alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintahan. Hasil pemeringkatan memberikan masukan bagi instansi pemerintah yang bersangkutan tentang kekuatan dan kelemahan aspek-aspek pengamanan informasi di instansinya serta langkah-langkah peningkatan yang diperlukan untuk menguatkan profil keamanan informasi [DIR15].

Dalam tugas akhir ini akan melakukan evaluasi keamanan informasi menggunakan Indeks Keamanan Informasi. Indeks Keamanan Informasi (KAMI) dilakukan terhadap beberapa area yang menjadi penerapan keamanan informasi yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001.

ISO/IEC 27001 menyediakan kerangka kerja dalam lingkup penggunaan teknologi informasi dan pengelolaan aset yang dapat membantu sebuah organisasi memastikan bahwa keamanan informasi yang diterapkan sudah efektif. Ada juga ISO 27002 yang memberikan rekomendasi praktik terbaik untuk manajemen keamanan informasi untuk digunakan oleh mereka yang bertanggung jawab untuk memulai, melaksanakan atau memelihara sistem manajemen keamanan informasi [ISO13].

Dasar kegiatan yang mendasari dilakukannya evaluasi keamanan informasi menggunakan Indeks KAMI yaitu Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) [REP08], dan Peraturan Menteri KOMINFO No. 04 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi [REP16].

### 1.2. Identifikasi Masalah

Berdasarkan uraian dari latar belakang masalah, maka dapat disimpulkan bahwa terdapat permasalahan yang dapat terjadi pada keamanan informasi yang ada di bagian IT & Multimedia Sekretariat DPRD Kota Cimahi diantaranya sebagai berikut :

1. Bagaimana menentukan Kategori Sistem Elektronik di bagian IT & Multimedia Sekretariat DPRD Kota Cimahi ?
2. Bagaimana tingkat kelengkapan dan kematangan keamanan informasi pada bagian IT & Multimedia Sekretariat DPRD Kota Cimahi?
3. Bagaimana rekomendasi untuk meningkatkan keamanan informasi yang ada di bagian IT & Multimedia Sekretariat DPRD Kota Cimahi ?

### 1.3. Tujuan Tugas Akhir

Tujuan dari penelitian tugas akhir ini adalah mengacu kepada Indeks Keamanan Informasi (KAMI) yaitu sebagai berikut :

1. Mengetahui tingkat kategori sistem elektronik yang digunakan di bagian IT & Multimedia Sekretariat DPRD Kota Cimahi.
2. Mengetahui nilai tingkat kelengkapan & kematangan Keamanan Informasi di bagian IT & Multimedia Sekretariat DPRD Kota Cimahi pengukuran keamanan informasi di DPRD Kota Cimahi
3. Memberikan usulan perbaikan keamanan informasi kepada pihak bagian IT & Multimedia Sekretariat DPRD Kota Cimahi Keamanan Informasi yang harus dijalankan.



#### 1.4. Lingkup Tugas Akhir

Dari permasalahan yang timbul, maka penulis membatasi permasalahan di antaranya:

1. Penelitian dilakukan di bagian IT & Multimedia Sekretariat DPRD Kota Cimahi.
2. Menggunakan Indeks Keamanan Informasi (KAMI) versi 3.1.
3. Yang diberi usulan yang memiliki status pada hasil pengisian kuesioner KAMI yaitu ‘tidak dilakukan’ dan ‘dalam perencanaan’.
4. Rekomendasi yang diberikan mengacu pada standar kontrol Keamanan Informasi ISO/IEC 27002:2013. Dalam standar ini memberikan panduan serta rekomendasi dalam perencanaan & implementasi suatu program untuk melindungi aset informasi.

#### 1.5. Metodologi Tugas Akhir

Langkah – langkah yang digunakan pada saat menyusun tugas akhir, yaitu sebagai berikut :

##### 1. Pengumpulan Data

Teknik pengumpulan data dilakukan secara paralel dengan menggunakan empat cara, yaitu:

###### a. Tinjauan Pustaka

Penulis mencari referensi sebuah landasan teori dalam menentukan langkah-langkah penyelesaian, dengan cara melakukan peninjauan pustaka dari buku maupun sumber bacaan dalam memecahkan masalah berdasarkan permasalahan yang dikerjakan dalam tugas akhir.

###### b. Observasi

Melakukan observasi ke lapangan untuk mendapatkan data mengenai kondisi lingkungan DPRD Kota Cimahi.

###### c. Wawancara

Merupakan teknik pengumpulan data dengan mengadakan wawancara berupa tanya jawab secara langsung yang melibatkan dua pihak dengan narasumber atau pegawai yang ada di instansi tersebut dalam memperoleh data dan informasi.

###### d. Kuesioner

Melakukan pengisian kuesioner variabel Indeks KAMI dengan pihak terkait untuk mendapatkan informasi.

##### 2. Perumusan Masalah

Pada tahap ini dilakukan perumusan masalah mengenai topik tugas akhir yang diambil yaitu mengenai pengukuran dan evaluasi keamanan informasi menggunakan Indeks Keamanan Informasi (KAMI). Pada tahap ini akan menghasilkan suatu rumusan masalah yang akan menjadi acuan dalam melakukan pengerjaan dan penyelesaian tugas akhir.

##### 3. Pengolahan Data

Pengolahan data merupakan tahapan untuk menghasilkan pengukuran berdasarkan hasil dari pengumpulan data sebelumnya.

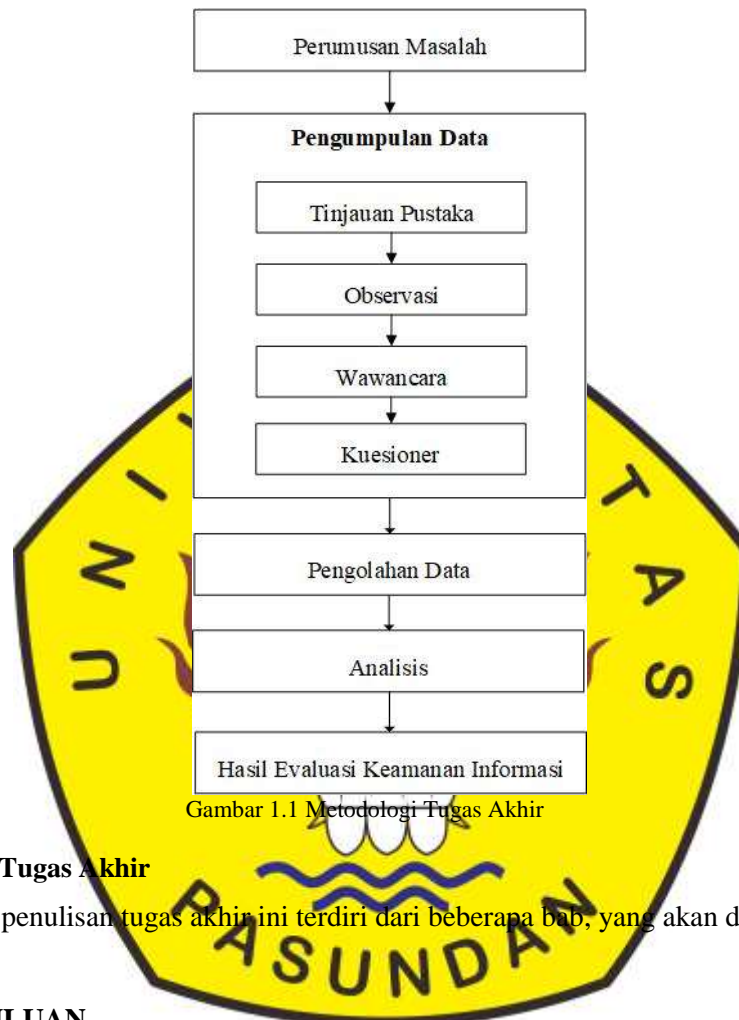
##### 4. Analisis



Tahap Analisis merupakan tahapan untuk menganalisis penelitian tugas akhir terhadap permasalahan yang terjadi.

#### 5. Hasil Evaluasi Keamanan Informasi

Hasil evaluasi keamanan informasi merupakan hasil akhir dari tugas akhir. Yang berupa hasil akhir dari evaluasi yang telah diukur sebelumnya dan usulan penulis terkait evaluasi tersebut.



Gambar 1.1 Metodologi Tugas Akhir

#### 1.6. Sistematika Tugas Akhir

Sistematika penulisan tugas akhir ini terdiri dari beberapa bab, yang akan dijelaskan sebagai berikut:

##### **BAB 1. PENDAHULUAN**

Pada BAB ini berisi mengenai garis besar permasalahan yang akan dibahas dan diselesaikan sesuai dengan tujuan yang telah dirumuskan seperti latar belakang tugas akhir, identifikasi masalah, tujuan tugas akhir, lingkup tugas akhir, metodologi tugas akhir, dan sistematika penulisan laporan tugas akhir.

##### **BAB 2. LANDASAN TEORI**

Pada BAB ini berisi mengenai definisi-definisi, teori-teori, konsep-konsep dasar yang diperlukan terkait dengan objek dan situasi yang diteliti. Di dalam bab ini dikemukakan hasil-hasil penelitian yang terdapat di buku-buku teks ataupun makalah-makalah di jurnal-jurnal ilmiah yang terkait yang relevan sebagai referensi pengerjaan tugas akhir ini. Teori yang dipaparkan diantaranya mengenai Indeks KAMI versi 3.1, ISO/IEC 27001, Tata Kelola Teknologi Informasi, Perbedaan Indeks KAMI 2.3 & Indeks KAMI 3.1.

##### **BAB 3. SKEMA PENELITIAN**

Pada BAB ini berisi mengenai rancangan penelitian, skema analisis, dan tempat penelitian. **BAB 4. ANALISIS**

Pada BAB ini berisi mengenai analisis keamanan informasi dengan melakukan penilaian keamanan informasi yang disesuaikan dengan batasan dan kebutuhan pada penyusunan laporan tugas akhir.

**BAB 5. PEMBAHASAN**

Pada BAB ini berisi mengenai kuesioner yang telah direkapitulasi dan diolah yaitu hasil evaluasi keamanan informasi. Dan pemberian rekomendasi berdasarkan ISO/IEC 27002:2013.

**BAB 6. KESIMPULAN DAN SARAN**

Pada BAB ini berisi mengenai kesimpulan dari hasil penelitian atau tugas akhir dan merupakan sebagai tindak lanjut dari kesimpulan maka pada akhir penulisan dikemukakan saran-saran yang berhubungan dengan permasalahan yang telah dibahas.



## DAFTAR PUSTAKA

- [AKH16] Akhirina, Yani Tri, Sutan M. & Rahmatika. 2016. Evaluasi Keamanan Teknologi Informasi Pada PT Indotama Partner Logistics Menggunakan Indeks Keamanan Informasi (KAMI). Universitas Indraprasta PGRI
- [BAS17] Basyarahil, A. Firzah. 2017. Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013. Institut Teknologi Sepuluh Nopember (ITS).
- [DIR15] Direktorat Keamanan Informasi. 2015. *Indeks KAMI versi 3.1*. Jakarta : Kementerian Komunikasi dan Informatika.
- [ECH00] Echols, M. John, Hassan Shadily. 2000. Kamus Inggris Indonesia *An English-Indonesia Dictionary*. Jakarta : PT. Gramedia.
- [HER17] Heryatna, Erman Dian. 2017. Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI. Universitas Pasundan (UNPAS).
- [ISO13] ISO/IEC 27001 – Information Security Management” ISO, 2013. [Online]. Available: <https://www.iso.org/isoiec-27001-information-security.html> [diakses 06 September 2018]
- [JOG99] Hartono, Jogiyanto. 1999. Analisis & Desain Sistem Informasi: Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis. Yogyakarta :ANDI.
- [KEL95] Kelleher, Kevin, Casey G., Lois D. 1995. *Cause and Effect Diagram : Plain & Simple*. USA : Joiner Associates Inc.
- [NUR17] Nuryanti, Nia. 2017. Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI). Universitas Pasundan. Bandung
- [OBR10] O’Brien, James A. & Marakas, George M. 2010. Introduction to Information Systems Fifteenth Edition. New York : Mc.Graw-Hill Irwin.
- [REP08] Republik Indonesia. 2008. Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE). Lembaran Negara RI Tahun 2008, No. 58. Sekretariat Negara. Jakarta.
- [REP12] Republik Indonesia. 2012. Peraturan Pemerintah No. 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Lembaran Negara RI Tahun 2012 No. 189. Sekretariat Negara. Jakarta.
- [REP16] Republik Indonesia. 2016. Peraturan Menteri KOMINFO No. 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi. Lembaran Negara RI Tahun 2016 No. 551. Sekretariat Negara. Jakarta.
- [SAR09] Sarno R, Iffano I. 2009. Sistem Manajemen Keamanan Informasi Berbasis ISO 27001. Surabaya : Penerbit ITS Press.

- [SIM06] Simarmata, Janner. 2006. Pengamanan Sistem Komputer. Yogyakarta : ANDI
- [SOE13] Soernardi, Iqbal & M. Ichsan. 2013. Analisis Kematangan Sistem Manajemen Keamanan Informasi Badan Pendidikan Dan Pelatihan Keuangan Diukur menggunakan Indeks Keamanan Informasi. Badan Pendidikan Dan Pelatihan Keuangan. Jakarta
- [TIM11] Tim Direktorat Keamanan Informasi Depkominfo. 2011. Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik. Menteri Keuangan Republik Indonesia. 2010. KMK Nomor 479/KMK.001/2010.
- [WAR15] Wardani, Restu Diah. 2015. Evaluasi Keamanan Informasi Pada Divisi Pengembangan Teknologi Informatika PDAM Tirta Moedal Kota Semarang Berdasarkan Indeks Keamanan Informasi SNI ISO/IEC 27001:2009. Universitas Dian Nuswantoro.

