

**KAJIAN TATA KELOLA IT  
BERDASARKAN INDEKS KAMI PADA  
UNIVERSITAS PAKUAN BOGOR**

**Nur Hidayati**

Program Studi Manajemen Informatika  
AMIK BSI Jakarta  
Jl. RS Fatmawati No. 24, Pondok Labu, Jakarta Selatan  
nur.nrh@bsi.ac.id

**Abstract**

*Corporate governance of information technology is becoming a very important needs for the sake of the survival of an organization. IT governance practices at the University of Pakuan (UNPAK) Faculty of MIPA Bogor in particular has not been done optimally, which still require evaluation in it, this was to be one of the goals in this study. By using descriptive types of qualitative research and exploratory that expected to know the condition of IT governance is ongoing. Results of the evaluation of the implementation of the IT governance is made by using index.KAMI Methode which is an adoption of ISO/IEC 27001, which is a tool to analyze the readiness of the security level of information about an organization's security framework. The maturity of the implementation of the corporate governance of information technology within the Faculty of MIPA UNPAK in level two, which is still in the process of the effectiveness and consistency of application framework used.*

**Keywords :** *Index KAMI, Maturity, Information Technolgy*

**1. PENDAHULUAN**

Teknologi Informasi (TI) telah menjadi bagian penting dalam suatu organisasi, terutama bagi organisasi yang bisnisnya berorientasi pada *profit*. Infrastruktur teknologi informasi tersebut memungkinkan para pelaku bisnis untuk berkomunikasi dan melakukan transaksi dengan para *stakeholder*. Biasanya infrastruktur tersebut sering diistilahkan dengan “*portofolio* teknologi informasi”. *Portofolio* teknologi informasi memungkinkan organisasi untuk menemukan strategi bisnis baru, membantu perusahaan untuk menghadapi persaingan dan juga meningkatkan produktifitas. Infrastruktur teknologi informasi merupakan landasan utama kemampuan teknologi informasi yang disajikan sebagai layanan bersama dalam organisasi dan diarahkan secara terpusat. Tujuannya adalah untuk memungkinkan berbagai data yang bersifat utuh secara organisasi dan integrasi lintas bisnis.

Tatakelola teknologi informasi (*IT Governance*) merupakan hal yang semakin banyak diusahakan oleh organisasi-organisasi, terutama organisasi yang berskala besar, atau telah melakukan IPO (*initial public offering*) sehingga menjadi *go public*. Tata kelola teknologi informasi dapat diartikan sebagai upaya menjamin pengelolaan teknologi informasi agar mendukung bahkan selaras dengan strategi bisnis suatu enterprise yang dilakukan oleh dewan direksi, manajemen eksekutif, dan manajemen teknologi informasi. Berdasarkan definisi dari tata kelola teknologi tersebut, diketahui bahwa aspek terpenting dari tata kelola teknologi informasi adalah

adanya kesesuaian antara teknologi informasi dengan strategi bisnisnya. Penerapan tata kelola teknologi informasi dalam suatu organisasi terutama pada suatu lembaga pendidikan, tentunya tidak terlepas dengan sistem informasi yang akan disajikan nantinya.

Sistem Informasi merupakan bagian dari suatu lembaga Pendidikan yang dapat dijadikan *selling point* dan *value added* terhadap pasar, karena dengan adanya Sistem Informasi ini, maka akan banyak memberikan manfaat terutama terhadap mahasiswa maupun karyawannya. Informasi itu sendiri merupakan salah satu asset yang sangat berharga bagi lembaga Pendidikan, sehingga akurasi dan kerahasiaannya harus selalu terjaga dengan baik. Dengan demikian Informasi tersebut perlu diamankan dari pelanggaran dan penyalahgunaan baik yang disengaja maupun yang tidak disengaja oleh pihak-pihak yang kurang bertanggungjawab, serta bentuk-bentuk kejahatan yang lainnya. Oleh karena itu, lembaga Pendidikan perlu menyelenggarakan sistem pengamanan yang memadai terhadap *file* data atau informasi dan distribusi output yang dihasilkan, serta perangkat lunak dengan memperhatikan resiko-resiko yang akan dihadapi. Hal yang dapat dilakukan untuk mengurangi resiko-resiko tersebut agar dapat lebih memperkuat pengamanan informasi, antara lain menerapkan pengamanan secara fisik, pemisahan tugas secara fungsional, pengendalian mutu atau integritas informasi, kontrol terhadap akses perangkat keras dan perangkat lunak serta audit *intern* secara efektif. Hal inilah yang menyebabkan pentingnya penerapan tata kelola teknologi informasi yang baik dalam lingkup pendidikan tersebut.

Pada Universitas Pakuan (UNPAK) Bogor khususnya Fakultas MIPA mulai menerapkan tata kelola teknologi informasi dengan teknologi pelindungnya antara lain antivirus, *firewall*, dan sebagainya, akan tetapi juga membuat kebijakan-kebijakan dan prosedur-prosedur keamanan dengan konsekuen dan terukur dalam pengelolaan datanya. Untuk memastikan adanya implementasi, pengoperasian, pengawasan, pemeliharaan dan perbaikan yang sesuai dengan visi dari UNPAK, yaitu “Univeritas Pakuan sebagai Perguruan Tinggi yang Bermanfaat bagi Masyarakat Indonesia”, maka diperlukan adanya standarisasi terhadap teknologi informasi yang dimiliki dengan melakukan sertifikasi melalui institusi yang independen agar semua unit kerja yang terkait dalam UNPAK selalu memperhatikan terhadap apa yang mereka lakukan dan selalu melihat dari segi CIA.

CIA merupakan *Confidentiality* ( selalu menjaga kerahasiaan informasi yang dimiliki ), *Integrity* ( selalu menjaga keutuhan informasi yang dimiliki ), dan *Availability* ( Informasi selalu ada dan tersedia ). Namun tata kelola teknologi informasi di UNPAK belum terdefinisi dengan baik dan belum terukur tingkat kematangannya. Oleh karena itu, diperlukan evaluasi terhadap penerapan tata kelola teknologi informasi dalam rangka penyesuaian strategi yang matang. Untuk dapat mengukur tingkat kematangan terkait maka dapat menggunakan model kematangan. Model kematangan merupakan metode *skoring* yang memungkinkan organisasi untuk memberi rangking bagi dirinya sendiri dari mulai tidak ada kematangan sampai dengan kematangan yang optimis. Alat bantu pengukuran kematangan ini memudahkan untuk memahami bagaimana menentukan posisi saat ini dan posisi ke depan serta memungkinkan organisasi untuk melakukan perbandingan pada dirinya sendiri berdasarkan praktik-praktik dan panduan standar yang ada.

Hal inilah yang membuat penulis tertarik untuk melakukan penelitian di UNPAK khususnya yang sudah mulai menerapkan Teknologi Informasi Komputer ( TIK ) didalamnya, khususnya di Fakultas MIPA, untuk dapat mengevaluasi kerangka kerja keamanan sistem informasi yang telah diterapkan di Fakultas MIPA UNPAK Bogor dengan menggunakan salah satu alat bantu yaitu Indeks Keamanan Informasi ( Indeks KAMI ).

## **2. KAJIAN LITERATUR**

### **2.1 Evaluasi dan Tata Kelola Teknologi Informasi**

1. Menurut Arifin (2009) “Evaluasi merupakan suatu proses yang sistematis dan berkelanjutan untuk menentukan kualitas ( nilai dan arti ) dari sesuatu berdasarkan pertimbangan ( *judgement* ) dan kriteria dalam rangka pembuatan keputusan”.
2. Menurut Arikunto (2008) “Empat kemungkinan kebijakan berdasarkan hasil evaluasi adalah menghentikan program, merevisi program, melanjutkan program dan menyebarkan program”.

Menurut Surendro(2009) mendefinisikan bahwa “Tata kelola teknologi informasi adalah tanggung jawab direksi dan manajemen eksekutif organisasi”. Tata kelola teknologi informasi merupakan bagian terintegrasi dari pengelolaan perusahaan yang mencakup kepemimpinan, struktur serta proses organisasi yang memastikan bahwa teknologi informasi perusahaan dapat dipergunakan untuk mempertahankan dan memperluas strategi dan tujuan organisasi. Tata kelola teknologi informasi bukan suatu disiplin ilmu atau aktifitas yang terbatas, tapi lebih merupakan suatu pengelolaan yang terintegrasi dengan pengelolaan perusahaan.

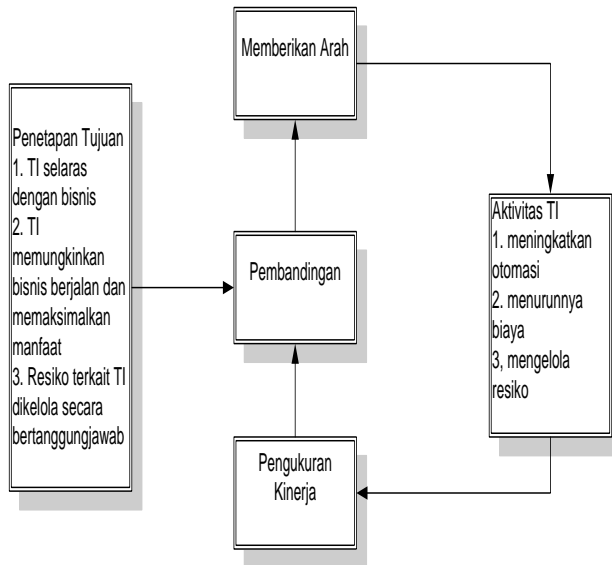
Tanggung jawab tata kelola teknologi informasi membentuk suatu bagian dari kerangka kerja yang lebih luas dari pengelolaan perusahaan dan sebaiknya diperlakukan seperti agenda strategi lainnya bagi dewan direksi. Dalam bentuk yang sederhana, untuk suatu sistem teknologi informasi yang sangat bergantung, pengelolaan harus efektif, transparan dan akuntabel. Maksudnya dewan direksi harus memahami benar tanggung jawab manajemen dan pribadinya, dan harus mempunyai suatu sistem untuk melaksanakan tanggung jawabnya tersebut. Kegunaan tata kelola teknologi informasi adalah untuk mengatur penggunaan teknologi informasi, serta untuk memastikan kinerja teknologi informasi sesuai dengan tujuan berikut ini :

1. Keselarasan teknologi informasi dengan perusahaan dan realisasi keuntungan-keuntungan yang dijanjikan dari penerapan teknologi informasi
2. Penggunaan teknologi informasi agar memungkinkan perusahaan mengeksplorasi kesempatan yang ada dan memaksimalkan keuntungan
3. Penggunaan sumber daya teknologi informasi yang bertanggung jawab
4. Penanganan manajemen resiko yang terkait informasi secara tepat.

Tata kelola teknologi informasi sering kali berjalan dalam lapisan yang berbeda-beda antara lain *team leader* memberikan laporan kepada manajer serta menerima pengarahan darinya, manajer memberikan laporan kepada eksekutif, dan eksekutif kepada dewan direksi. Dalam merespon arahan yang diterima, maka fungsi teknologi informasi harus fokus dalam :

- a Memberikan keuntungan dengan menambah otomatisasi dan membuat perusahaan menjadi lebih efektif, dan mengurangi biaya dan membuat keseluruhan perusahaan lebih efisien
- b Menangani resiko (keamanan, kelayakan, dan kesesuaian)

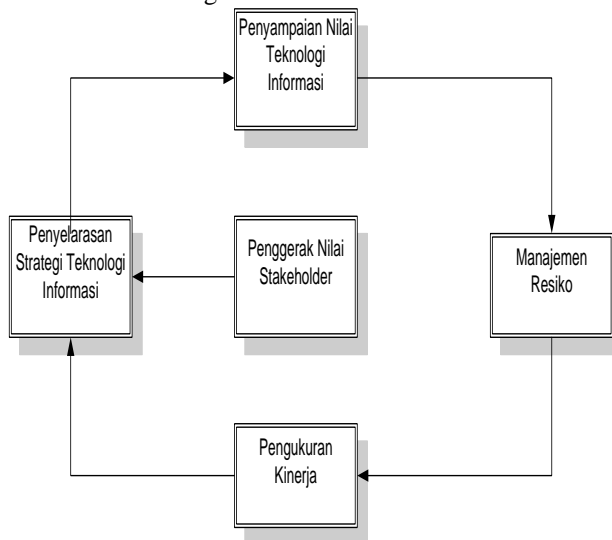
Dengan demikian kerangka kerja tata kelola teknologi informasi dapat diselaraskan seperti yang terlihat pada gambar berikut ini :



Sumber : Surendro (2009)

Gambar 1 Kerangka Kerja Tata Kelola TI

Lima area yang menjadi fokus tata kelola teknologi informasi, semuanya dikendalikan oleh *stakeholder*. Dua diantaranya adalah penyampaian layanan dan manajemen resiko. Tiga fokus yang lainnya berperan sebagai penentu yaitu penyalarsan strategi, pengelolaan sumber daya, dan pengukur kinerja. Tata kelola teknologi informasi dapat dianggap juga sebagai sebuah proses dimana strategi teknologi informasi mengendalikan kumpulan proses-proses yang dilakukan dengan teknologi informasi, mengumpulkan sumber daya yang dibutuhkan untuk melaksanakan kewajibannya. Berikut gambar fokus tata kelola teknologi informasi :



Sumber : Surendro (2009)

Gambar 2 Fokus Tata Kelola Teknologi Informasi

## 2.2 Indeks KAMI

Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di sebuah Instansi. Alat evaluasi ini tidak ditujukan untuk menganalisa kelayakan atau efektifitas bentuk

pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan ( kelengkapan ) kerangka kerja keamanan informasi kepada pimpinan instansi. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2005.

Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh sebuah instansi dari berbagai tingkatan, ukuran, maupun bentuk tingkat kepentingan penggunaan Teknologi Informasi Komputer ( TIK ) dalam mendukung terlaksananya tugas pokok dan fungsi yang ada. Data yang digunakan dalam evaluasi ini nantinya akan memberikan *snapshot* indeks kesiapan ( kelayakan ) dan kematangan kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembandingan dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya.

Alat evaluasi ini kemudian bisa digunakan secara berkala untuk mendapatkan gambaran perubahan kondisi kelemahan informasi sebagai hasil dari program kerja yang dijalankan, sekaligus sebagai sarana untuk menyampaikan peningkatan kesiapan atau kematangan kepada pihak yang terkait ( *stakeholder* ). Penggunaan dan publikasi hasil evaluasi indeks KAMI merupakan tanggungjawab penggunaan dana publik sekaligus menjadi sarana untuk meningkatkan kesadaran kebutuhan keamanan informasi di suatu instansi yang mulai ditandai dengan penerapan tata kelola teknologi informasinya.

## 2.3 Petunjuk Penggunaan Indeks KAMI

Alat evaluasi Indeks KAMI ini secara umum ditujukan untuk digunakan oleh instansi pemerintah di tingkat pusat. Akan tetapi dengan semakin berkembangnya teknologi informasi, alat evaluasi ini dapat juga digunakan untuk instansi lainnya. Proses evaluasi dilakukan melalui sejumlah pertanyaan di masing-masing area di bawah ini :

1. Peran TIK didalam instansi
2. Tata Kelola Keamanan Informasi
3. Pengelolaan Resiko Keamanan Informasi
4. Kerangka Kerja Keamanan Informasi
5. Pengelolaan Aset Informasi, dan
6. Teknologi dan Keamanan Informasi

Alat evaluasi ini hanya akan memberikan nilai tambah bagi semua pihak apabila pengisiannya menggunakan azas keterbukaan dan kejujuran. Pertanyaan dikelompokkan berdasarkan tingkat kematangan yang diharapkan, mulai dari area yang terkait dengan bentuk kerangka kerja dasar keamanan informasi ( label "1" ), efektifitas dan konsistensi penerapannya ( label "2" ) sampai dengan kemampuan untuk meningkatkan kinerja keamanan informasi ( label "3" ).

Tingkat terakhir ini sesuai dengan kesiapan minimum yang diprasyaratkan oleh proses sertifikasi standart ISO/IEC 27001:2005. Berikut skor yang diberikan untuk

jawaban pertanyaan sesuai tingkat kematangannya yang mengacu kepada :

**Tabel 1 Skor Tingkat Kematangan**

Status Pengamanan	Tingkat Kematangan		
	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

Sumber : ( Depkominfo, 2008 )

Pertanyaan terkait peran TIK dalam instansi tidak diberikan label dan merupakan kelompok yang terpisah. ( Catatan : untuk keseluruhan area pengamanan, pengisian pertanyaan dengan label “3” hanya dapat memberikan hasil apabila semua pertanyaan terkait dengan label “1” dan “2” sudah diisi dengan status minimal “Diterapkan Sebagian” ).

Khusus untuk korelasi antara peran atau tingkat kepentingan TIK dalam instansi, kriteria penilaiannya dapat didefinisikan melalui tabel sebagai berikut :

**Tabel 2 Peran TIK dalam Instansi**

Rendah		Indeks ( Skor Akhir)		Status Kesiapan
0	12	0	124	Tidak Layak
		125	272	Perlu Perbaikan
		273	588	Baik/Cukup
Sedang		Skor Akhir		Status Kesiapan
13	24	0	174	Tidak Layak
		175	312	Perlu Perbaikan
		313	588	Baik/Cukup
Tinggi		Skor Akhir		Status Kesiapan
25	36	0	272	Tidak Layak
		273	392	Perlu Perbaikan
		393	588	Baik/Cukup
Kritis		Skor Akhir		Status Kesiapan
37	48	0	333	Tidak Layak
		334	453	Perlu Perbaikan
		454	588	Baik/Cukup

Sumber : ( Depkominfo, 2008 )

Terdapat lima status keamanan informasi yang dimiliki Peran TIK dalam Instansi, yang masing-masing memiliki skala penilaian sebagai berikut :

**Tabel 3 Skor Nilai Kuesioner Bagian I**

Status	Nilai
--------	-------

Minim	0
Rendah	1
Sedang	2
Tinggi	3
Kritis	4

Sumber : Depkominfo ( 2008 )

Sedangkan untuk area tata kelola keamanan informasi, pengelolaan resiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan asset informasi dan teknologi keamanan informasi, memiliki empat status keamanan informasi, yang memiliki skala penilaian sebagai berikut :

**Tabel 4 Skor Nilai Kuesioner Bagian II, III, IV, V dan VI**

Status Pengamanan	Tingkat Kematangan		
	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

Sumber : Depkominfo ( 2008 )

### 2.3 Tinjauan Studi

Tinjauan Studi yang penulis lakukan, antara lain:

1. Kajian Manajemen Resiko Teknologi Informasi ( Birowo, 2006), mengatakan bahwa Penelitian yang dilakukan untuk menghasilkan panduan strategi umum kebijakan Teknologi Informasi dan perencanaan kegiatan pengamanan informasi yang dapat dilakukan oleh organisasi, dengan melakukan implementasi COBIT dan ISO 27001. Penelitian dalam kajian ini dilakukan pada unit kerja yang bergerak dalam kegiatan teknologi informasi di lingkup organisasi Departemen Keuangan yakni Pusintek, dengan melakukan kegiatan pengumpulan data melalui wawancara serta studi dokumentasi organisasi. Hasil penelitian ini adalah berupa kajian terhadap kelemahan kinerja Pusintek terkait dengan pengamanan informasi, serta arahan pada Pusintek untuk melakukan penanganan terhadap resiko yang diakibatkan kelemahan pengamanan informasi. Kajian ini dipergunakan oleh Pusintek sebagai dasar untuk mewujudkan strategi kebijakan teknologi informasi serta melakukan perencanaan kegiatan manajemen resiko terhadap pengamanan informasi, agar dapat menjaga ketersediaan dan kehandalan sistem teknologi informasi untuk mendukung proses bisnis yang berada di Departemen Keuangan Republik Indonesia.

2. Perancangan dan Implementasi Sistem Manajemen Keamanan Informasi ( Fauzi, 2007), mengemukakan bahwa Informasi merupakan aset organisasi yang harus dilindungi keamanannya. Sistem Manajemen Keamanan Informasi diimplementasikan untuk melindungi aset informasi dari berbagai ancaman untuk menjamin kelangsungan usaha, meminimalisasi kerusakan akibat terjadinya ancaman, mempercepat kembalinya investasi dan peluang usaha. Pada penelitian ini, standard internasional ISO/IEC 17799, ISO/IEC 27001, dan analisa resiko berdasarkan metode OCTAVE-S digunakan dalam perancangan dan implementasi Sistem Manajemen Keamanan Informasi PT.X.
3. Evaluasi Kinerja Sistem Manajemen Keamanan Informasi ( Mursito, 2008 ), mengemukakan bahwa Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Sayangnya masalah keamanan informasi ini sering kali kurang mendapatkan perhatian dari para pemilih dan pengelola sistem informasi. Departemen Pertanian, sebagai lembaga pemerintahan yang bertanggungjawab pada penentu kebijakan, standarisasi dan sosialisasi pertanian di seluruh wilayah Republik Indonesia, tidak dapat dipungkiri juga membutuhkan informasi yang berkualitas guna menjalankan tugas pokok dan fungsi sebagaimana mestinya. Keamanan informasi tidak dapat diimplementasikan dengan baik apabila faktor-faktor pendukungnya tidak dipertimbangkan. Media untuk menghasilkan informasi, menyimpan informasi dan menyebarkan informasi, baik yang berupa *hardware*, *software* dan perangkat jaringan harus diperhatikan sebagai aspek teknis dari keamanan sistem informasi. Begitu pula aspek non teknis seperti kebijakan keamanan informasi, tata kelola, yang meliputi tugas dan tanggungjawab masing-masing personil yang harus diperhatikan dalam pengembangan Manajemen Keamanan Sistem Informasi yang komprehensif di Departemen Pertanian. Evaluasi sistem keamanan informasi yang dilakukan sebagai upaya untuk menjaga keamanan aset sekaligus menjamin kegiatan pertukaran informasi dapat berjalan dengan aman dan *seamless* ( mulus ). Aspek yang dikaji meliputi aspek kebijakan dan prosedur keamanan informasi meliputi aspek arsitektur dan model keamanan informasi, aspek keamanan fisik, aspek teknis, aspek personil dan aspek tata kelola sistem informasi.
4. Audit Sistem Informasi/Teknologi Informasi Dengan Kerangka Kerja COBIT untuk Evaluasi manajemen Teknologi Informasi Di UNIVERSITAS XYZ (Devi Fitriyah dan Giri Suahyo), mengatakan bahwa pemanfaatan teknologi informasi sebagai pendukung pencapaian tujuan dan sasaran organisasi harus diimbangi dengan keefektifan dan efisiensi pengelolaannya.

### ***Jurnal Paradigma vol XVI no.2 September 2014***

Maka dari itu, audit TI haruslah dilakukan untuk menjaga keamanan sistem informasi sebagai aset organisasi, untuk mempertahankan integritas informasi yang disimpan dan diolah serta tentu saja untuk meningkatkan keefektifan penggunaan teknologi informasi serta mendukung efisiensi dalam organisasi. Penelitian ini bertujuan untuk melakukan pemetaan terhadap tahap audit TI beserta kontrolnya yang kemudian diaplikasikan pada sebuah organisasi, yaitu Universitas XYZ untuk melihat kinerja TI yang ada. Kerangka kerja yang digunakan sebagai acuan adalah COBIT ISACA dengan menggunakan 120 *deatiled control objective* yang ada. Penyelenggaraan audit dilakukan dengan menggunakan tahapan-tahapan yang ada pada *IT Assurance Guide*. Hasil evaluasi atau temuan dilakukan analisa *root cause* sehingga didapat sebuah rekomendasi untuk manajemen TI yang lebih baik lagi.

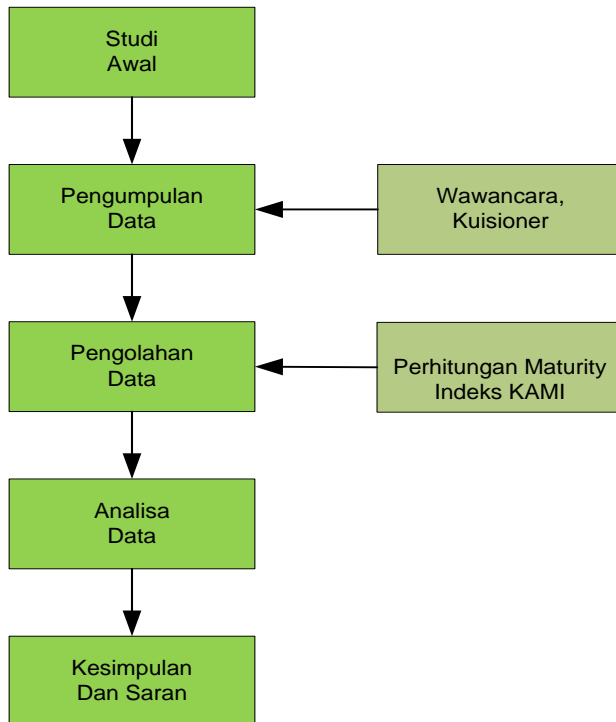
### **3. METODE PENELITIAN**

Jenis penelitian yang dilakukan oleh penulis yaitu :

1. Penelitian tentang evaluasi kematangan penerapan tata kelola teknologi informasi ini bersifat penelitian deskriptif kualitatif artinya hasil penelitian disampaikan dalam bentuk deskripsi.
2. Selain itu Penelitian ini bersifat eksploratif artinya penelitian dilakukan dengan cara menggali informasi untuk mengetahui kematangan penerapan tata kelola teknologi informasi yang berlangsung di UNPAK khususnya pada Fakultas MIPA.

Metode yang digunakan untuk memperoleh evaluasi kerangka kerja keamanan sistem informasi berdasarkan indeks KAMI adalah dengan tahapan sebagai berikut : 1) Melakukan Studi awal, 2) Pengumpulan data, melalui kuesioner, wawancara dan pengamatan, 3) Melakukan pengolahan data terhadap data-data yang dihasilkan, terutama pada kuesioner dengan menggunakan indeks KAMI, 4) Analisa data, analisa dilakukan terhadap tingkat *maturity* ( kematangan ) yang dihasilkan dan 5) Membuat kesimpulan

sampel yang mengelola sistem informasi Perguruan Tinggi. Ketiga, sampel yang dipilih merupakan user/pengguna langsung dari sistem informasi Perguruan Tinggi.



Gambar 3 Langkah-langkah penelitian

- a. Studi Awal  
Dalam melakukan studi awal, penulis melakukan : pencarian materi, pembuatan draf kuesioner, serta mempelajari Sistem Informasi di UNPAK khususnya pada Fakultas MIPA.
- b. Pengumpulan Data  
Pada tahapan ini, penulis melakukan pengumpulan data yang diperoleh dengan cara wawancara, observasi dan pemberian kuesioner
- c. Pengolahan Data  
Pada tahapan ini, penulis melakukan pengolahan data dari kuesioner yang di isi oleh para responden dengan menggunakan Indeks KAMI, hasilnya berupa tingkat *maturity*. Proses pengolahan data menggunakan aplikasi Excel
- d. Analisa data  
Pada tahapan ini, penulis melakukan analisa data dari tingkat *maturity*.
- e. Kesimpulan dan Saran  
Pada tahap akhir penulis membuat kesimpulan dan saran dari semua proses penelitian yang dilakukan.

Penulis menggunakan metode dengan teknik *purposive sampling* yang merupakan bagian dari Sampling Non Probabilitas dalam pemilihan sampel. Dalam sampling non probabilitas tidak perlu dilakukan perhitungan tetapi hanya dengan dipilih ataupun dikira-kira. Sehingga melalui teknik *purposive sampling* ini, pemilihan sampel dilakukan berdasarkan tujuan dari penelitian dan pertimbangan-pertimbangan tertentu atau dengan kata lain sampel sengaja dipilih karena memiliki cirri-ciri khusus. Pertimbangan itu adalah, pertama sampel yang dipilih merupakan manajemen dari Perguruan Tinggi, kedua sampel yang dipilih merupakan

#### 4. HASIL PENELITIAN DAN PEMBAHASAN

Berdasarkan penelitian yang penulis lakukan maka diketahui bahwa Pengembangan Sistem Informasi baru diterapkan di Fakultas MIPA, dan lebih dikenal dengan istilah SIFA. Sedangkan untuk fakultas yang lain yang berada di Universitas Pakuan masih dilakukan secara manual dalam hal pengolahan datanya(pada saat penulis melakukan penelitian). SIFA atau Sistem Informasi Akademik Fakultas MIPA mulai diterapkan pada tahun 2007, dan hanya bisa digunakan secara lokal oleh *user* atau disebut dengan *intranet*. Mengenai masalah penerapan tata kelola teknologi informasinya sudah mulai diterapkan walaupun belum secara keseluruhan. Sehingga nantinya dari penerapan tata kelola teknologi informasinya tersebut dapat diketahui mengenai keamanan sistem informasinya. Hal ini nantinya dapat dilihat berdasarkan hasil evaluasi yang penulis lakukan. Asset merupakan sesuatu yang mempunyai nilai dan sangat berharga bagi kelangsungan hidup suatu organisasi ataupun instansi, sehingga harus dijaga dan dikelola dengan baik. Asset yang dimiliki oleh Fakultas MIPA dalam mengembangkan sistem informasinya antara lain :

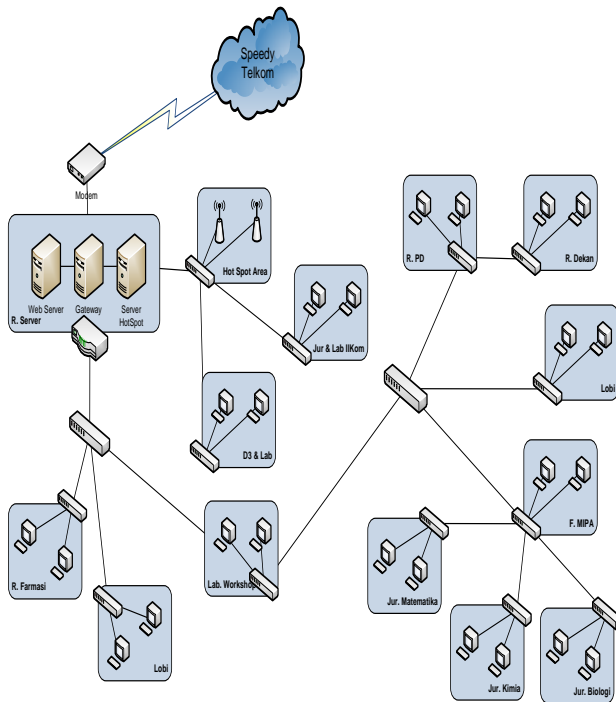
Tabel 5 Identifikasi Asset

No	Asset
<b>1. Asset Data dan Informasi</b>	
	Database Pengguna
	Dokumentasi Sistem Informasi
	File-file Pekerjaan Karyawan
<b>2. Aset Perangkat Lunak</b>	
	Sistem Operasi ( Ubuntu, Windows, Linux)
	Aplikasi Perkantoran ( MS.Office, Open Office )
	Aplikasi yang mendukung dalam web SIFA, antara lain PHP 5.1.4, Java Script ( AJAX ), CSS, XHTML
<b>3. Aset Perangkat Keras</b>	
	Server
	PC
	Printer
<b>4. Jaringan</b>	
	Gateway
	Hotspot
	Modem
	Perangkat Wireless LAN
	Kabel Jaringan

Sumber : Fakultas Ilmu Komputer UNPAK( 2010 )

snapshot index kesiapan atau kematangan dari kerangka kerja keamanan sistem informasi yang dijalankan. Setelah dilakukan perhitungan terhadap pengolahan data kuesioner maka didapat hasil sebagai berikut :

Infrastruktur Jaringan Yang Diterapkan di Fakultas MIPA UNPAK, adalah :



Sumber : Fakultas Ilmu Komputer UNPAK( 2010 )  
Gambar 4 Infrastruktur jaringan

Mengenai ancaman, yang sering terjadi adalah pemadaman listrik. Hal inilah yang membuat aset yang dimiliki seperti komputer sering mengalami kerusakan. Oleh karena itu pihak Fakultas MIPA UNPAK bekerja sama dengan PLN, mendirikan *tower* listrik sendiri untuk mengurangi resiko dan mengurangi kerugian yang disebabkan oleh seringnya terjadi pemadaman listrik. Selain itu, lokasi *server* yang berada di tempat yang kurang aman, yaitu di lantai bawah dan masih menjadi satu dengan tempat praktek mahasiswa, sehingga bisa menimbulkan hal-hal yang tidak diinginkan terjadi.

Dengan menggunakan Index KAMI, yang digunakan untuk mengukur tingkat kematangan (*Maturity*) kerangka kerja keamanan informasi dengan melihat penerapan tata kelola teknologi informasinya dimana telah memenuhi aspek keamanan berdasarkan ISO 27001, maka dalam Index KAMI terdiri 5 aspek yang perlu diketahui, antara lain Aspek Tata Kelola Keamanan Informasi, Pengelolaan Resiko Keamanan Informasi, Kerangka Kerja Pengelolaan Keamanan Informasi,

Pengelolaan Aset Informasi dan Teknologi Keamanan Informasi. Dari kelima aspek tersebut, akan dinilai kematangannya, berdasarkan 3 (tiga) kerangka penilaian, yaitu :

1. Kepatuhan ISO 27001
2. Proses Penerapan
3. Kerangka Kerja Dasar

Oleh karena itu, data-data yang telah penulis dapatkan, salah satunya melalui kuesioner, data-data tersebut akan diolah sehingga akan menghasilkan

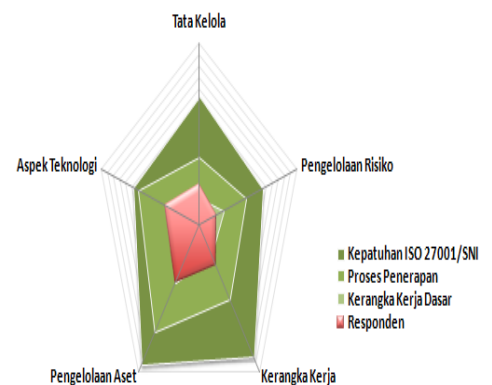
Responden: 3

Hasil Evaluasi:

Tingkat Kesiapan lembaga **Tidak Layak**

Tingkat Kematangan sesuai Standar ISM **227**

Peran/Tingkat Kepentingan TIK	: 22	Tingkat Ketergantun	Sedang
Tata Kelola	: 36		
Pengelolaan Fisiko	: 28		
Kerangka Kerja Keamanan Informasi	: 44		
Pengelolaan Aset	: 63		
Teknologi dan Keamanan Informasi	: 56		



Gambar 5 Hasil Evaluasi berdasarkan Indeks KAMI

Berdasarkan hasil evaluasi diatas, dapat dikatakan bahwa Fakultas MIPA UNPAK masih dalam tingkat kematangan 2, yaitu menuju ke proses penerapan. Aspek Pengelolaan Aset, Aspek Teknologi, Aspek Kerangka Kerja dan Aspek Tata kelola sudah dalam kerangka kerja dasar dan menuju ke proses penerapan, sedangkan Aspek Pengelolaan Resiko masih mendekati tingkat kematangan yang pertama, yaitu tahap kerangka kerja. Aspek Tata Kelola mulai mendekati tingkat kematangan kedua, yaitu proses penerapan, sedangkan aspek yang lainnya masih lumayan jauh untuk menuju ke proses penerapan. Walaupun demikian, dapat dikatakan bahwa Tingkat kesiapan atau kelengkapan Fakultas MIPA UNPAK terhadap proses penerapan tata kelola teknologi informasi berdasarkan hasil evaluasi diatas masih dalam kategori tidak layak. Hasil evaluasi diatas menunjukkan adanya kesenjangan antara hubungan satu aspek dengan aspek yang lainnya, sehingga belum dapat mencapai target yang diinginkan. Sebagai salah satu alasannya, karena belum adanya program kerja yang terstruktur untuk menangani masalah keamanan informasi dan belum adanya kesadaran begitu pentingnya akan kebutuhan keamanan terhadap sistem informasi yang sedang diterapkan sehingga mengakibatkan adanya kesenjangan, seperti :

1. Aspek Pengelolaan Informasi

- a. Kesenjangan:  
Tanggung jawab terhadap pengelolaan aset informasi belum dilakukan secara menyeluruh
  - b. Implikasi :  
Aset informasi tidak terpelihara dengan baik
  - c. Rekomendasi :  
Organisasi sebaiknya memastikan aset yang terhubung dengan sarana pengolah informasi mempunyai pemilik, klasifikasi *security* yang didefinisikan dan disetujui, dan pembatasan akses yang dikaji ulang secara periodik
2. Aspek Teknologi dan Keamanan Informasi
    - a. Kesenjangan:  
Manajemen keamanan jaringan belum di kaji secara berkala.
    - b. Implikasi:  
Terjadi kemungkinan Informasi di jaringan tidak terlindungi.
    - c. Rekomendasi :  
Organisasi sebaiknya memastikan jaringan diatur dan dikontrol secara memadai, untuk melindungi dari ancaman, dan untuk memelihara keamanan pada sistem dan aplikasi yang menggunakan jaringan, termasuk informasi yang melintas didalamnya.
3. Aspek Tata Kelola Teknologi Informasi
    - a. Kesenjangan :  
Pengaturan atau tata kelola teknologi informasi untuk internal organisasi belum dikembangkan secara keseluruhan.
    - b. Implikasi  
Pelanggaran keamanan informasi di organisasi,
    - c. Rekomendasi :  
Organisasi sebaiknya membuat pengaturan yang terkait:
      - 1) Mengkaji kembali penerapan tata kelola teknologi informasi yang sedang berlangsung
      - 2) Koordinasi aktivitas keamanan informasi dalam organisasi
      - 3) Pengaturan secara tertulis alokasi tanggung jawab terhadap aset-aset.
      - 4) Kontak dengan kelompok khusus atau spesialis keamanan.
      - 5) Pengkajian keamanan informasi oleh pihak independen dilakukan secara berkala

Secara umum interpretasi terhadap hasil evaluasi melalui kuesioner adalah adanya masih adanya kelemahan kontrol dalam proses pengelolaan datanya yang penting dan perlu diwaspadai, yang merupakan kerentanan bagi

### *Jurnal Paradigma vol XVI no.2 September 2014*

munculnya ancaman (*threat*) yang sangat memungkinkan (*probability*) akan berdampak (*impact*) serius bagi pencapaian kinerja di UNPAK ini. Berkaitan dengan hal itu, maka diperlukan langkah-langkah sebagai berikut:

1. Melakukan identifikasi ancaman (*threat*) terhadap data sebagai aset perusahaan dan dampak bisnis terkait dengan ancaman tersebut
2. Melakukan identifikasi terhadap kelemahan (*vulnerability*) yang dapat memicu terjadinya ancaman.

Dengan adanya kelemahan kontrol dalam pengelolaan datanya maka dapat berdampak *negative* pada :

1. Tidak optimalnya penggunaan data atau informasi
2. Tidak adanya kepastian bahwa data atau informasi kritis dan sensitive organisasi tidak dapat diakses oleh pihak yang berhak
3. Tidak adanya jaminan kepatuhan teknologi informasi pada hukum dan peraturannya yang telah ditetapkan.

Adapun indikasi dari fenomena diatas :

1. Kejadian ketidakmampuan untuk memulihkan data kritis untuk proses bisnis
2. Ketidakpuasan pengguna terhadap ketersediaan data
3. Seringnya terjadi insiden ketidakpatuhan pada hukum yang diakibatkan permasalahan manajemen penyimpanan.

Oleh karena itu, hal ini bisa dijadikan sebagai acuan bagi pimpinan untuk melakukan pembenahan ataupun penentuan prioritas yang harus dilakukan terlebih dahulu, demi menjaga keamanan sistem informasi yang sedang dijalankan sehingga apa yang menjadi tujuan akhir dari penerapan tata kelola teknologi informasi ini dapat sesuai seperti yang diinginkan. Dengan penerapan tata kelola teknologi informasi ini diharapkan masalah keamanan sistem informasi maupun masalah penyampaian informasi melalui SIFA bisa diperbaiki, yang menjadi kekurangannya bisa segera dicarikan solusinya sehingga tidak mengganggu kinerja yang lainnya.

## **5. KESIMPULAN**

Berdasarkan hasil penelitian yang penulis lakukan pada Universitas Pakuan Bogor khususnya di Fakultas MIPA, maka disimpulkan sebagai berikut :

1. Pengelolaan pengembangan sistem informasi yang diterapkan di Fakultas MIPA UNPAK, dilakukan dengan menggunakan *intranet* maupun internet untuk membantu para pengguna dalam memperoleh informasi yang di harapkan, dan pada saat ini pengembangan sistem informasi dilakukan secara terus menerus untuk mendapatkan hasil yang maksimal.
2. Berdasarkan dari hasil evaluasi yang dilakukan dengan menggunakan Indeks KAMI, maka



diperoleh hasil kematangan penerapan tata kelola teknologi informasi yang masih berada pada tingkat kematangan kedua, yaitu dalam tahap proses penerapan kerangka kerja dasar, sehingga dibutuhkan adanya suatu perbaikan untuk meningkatkan kesadaran akan kebutuhan teknologi informasi. Kondisi kesiapan atau kelengkapan dan kematangan tata kelola teknologi informasi di Fakultas MIPA UNPAK masih dalam kategori tidak layak, sehingga dibutuhkan suatu kebijakan yang baru, yang mengatur mengenai masalah teknologi informasi terutama dalam hal keamanan informasinya.

3. Evaluasi terhadap kebijakan penerapan tata kelola teknologi informasi perlu dilakukan secara periodik, untuk mengetahui sejauh mana peningkatannya terutama dalam hal keamanan sistem informasi yang telah dilakukan, semakin meningkat atau menurun. Kebijakan yang diambil harus dipahami sebagai suatu aset penting yang melindungi sistem informasi yang dimiliki oleh Fakultas MIPA UNPAK serta dapat menjaga asset yang lainnya.
4. Hasil penelitian ini menunjukkan bahwa tingkat kematangan penerapan tata kelola teknologi informasi masih berada di tingkat kematangan kedua, yang mana data yang diperoleh telah diolah dengan menggunakan Indeks KAMI.

Saran yang ingin penulis sampaikan dalam penelitian ini antara lain :

1. Sebaiknya Fakultas MIPA UNPAK melakukan evaluasi kembali dalam hal penerapan tata kelola teknologi informasinya sehingga perencanaan dan perancangan kebijakan keamanan informasi dapat lebih baik lagi, serta membentuk program kerja yang jelas dan terstruktur, dan mensosialisasikan akan pentingnya tata kelola teknologi informasi dengan baik bagi instansi.
2. Melakukan evaluasi secara berkala terhadap kerangka kerja keamanan informasi sehingga bisa melihat adanya perubahan kondisi keamanan informasi yang sedang diterapkan.
3. Memberikan rekomendasi yang diperlukan khususnya untuk aspek tata kelola teknologi informasi, pengelolaan resiko keamanan informasi, kerangka kerja dasar keamanan informasi, pengelolaan asset keamanan informasi serta teknologi keamanan informasi
4. Perlu kembali diingat bahwa proses pembuatan dan pemberlakuan kebijakan dalam tata kelola teknologi informasi bagi organisasi adalah suatu proses yang tidak mengenal henti maka jangan pernah untuk berhenti pada satu keadaan dan jangan mudah menyerah. Lakukan perencanaan dan pembuatan SOP yang jelas, sehingga dapat menjaga asset-asset yang dimiliki oleh lembaga.
5. Meningkatkan kebutuhan akan infrastruktur yang mendukung dalam pengembangan sistem informasi,

*Jurnal Paradigma vol XVI no.2 September 2014* baik *hardware*, *software* maupun *softskill* yang dimiliki oleh setiap karyawan sehingga bisa meningkatkan kinerjanya dan dapat mencapai tujuan yang diinginkan.

6. Hasil penelitian ini dapat dilanjutkan dengan cakupan yang lebih luas dan dapat menggunakan metode ataupun pendekatan yang lain, sesuai dengan kasus yang diambil.

## 6. DAFTAR PUSTAKA

Andy, Jones and Debi,Ashenden.(2005).*Risk Management for Computer Security*. Elsevier Inc.

Arifin, Zainal.(2009).*Evaluasi Pembelajaran*. Bandung : PT. Remaja Rusdakarya

Arikunto, Suharsimi.(2008).*Dasar- Dasar Evaluasi Pendidikan*. Jakarta : Bumi Aksara

Birowo, Cahyono Tri.(2006).*Kajian Manajemen Resiko Teknologi Informasi Berdasarkan COBIT Framework dan ISO 27001 : Studi Kasus Pada Pusat Sistem Informasi dan Teknologi Keuangan Departemen Keuangan*.Jakarta:Universitas Indonesia

Depkominfo.(2008). *Indeks KAMI*. Jakarta.

Depkominfo.(2009).Aprisma.Jakarta.

Fauzi, Rokhman.(2007).*Perancangan dan Implementasi Manajemen Keamanan Sistem Informasi Berbasis Standar ISO/IEC 17799, ISO/IEC 27001 Dan Analisa Resiko Metode Octave-S*. Bandung : Institut Teknologi Bandung

Gaol, Chr. Jimmy.(2008).*Sistem Informasi Manajemen : Pemahaman dan Aplikasi*.Indonesia :Gramedia Widiasarana

Hall, Jon G.(2008).*Framework for IT Management ISO 27001 Chapter*. SMF Van Haren Publishing.

Irawan.(2007).*Penelitian Kualitatif&Kuantitatif Untuk Ilmu-Ilmu Sosial*.Jakarta : Departemen Ilmu Administrasi Fakultas Ilmu Sosial dan Ilmu Politik Universitas Indonesia

ISO/IEC 17799:2005 (E).(2005).*Information Technology–Security Techniques–Code of Practice for Information Security Management*. Geneva: International Standards Organization.

Kurnia, Aries Fajar.(2006).*Perencanaan Kebijakan Keamanan Informasi Berdasarkan Information Security Management System ( ISMS ) ISO 27001 Studi Kasus Bank XYZ*.Jakarta : Universitas Indonesia

Maesya, Aries.(2010). Personal Interview.

McLeod, Raymond dan Schell, Jr. Goerge.(2008).  
*Sistem Informasi Manajemen*.Jakarta : Salemba Empat

Mursito, Danan.(2008).*Evaluasi Kinerja Sistem Manajemen Keamanan Informasi Menggunakan ISO 17799 Studi Kasus Departemen Pertanian Republik Indonesia*. Jakarta : Universitas Indonesia

Patrick, F.Sullivan.(2008).*Standard to Develop ISO 27001 for Chief Privacy Officers*.JWB Group International Information Assurance.

Sugiyono.(2009).*Metode Penelitian Kuantitatif Kualitatif dan R&D*.Bandung : Alfabeta.

Surendro, Kridanto.(2009).*Implementasi Tata Kelola Teknologi Informasi*.Bandung: Informatika.