Perencanaan dan Implementasi *Information Security Management System* Menggunakan *Framework* ISO/IEC 20071

Anggi Anugraha Putra[1)], Oky Dwi Nurhayati[2)], Ike Pertiwi Windasari [2)]
Program Studi Sistem Komputer Fakultas Teknik Universitas Diponegoro
Jalan Prof. Sudharto, Tembalang, Semarang, Indonesia
Anugraha.anggi@gmail.com

***Abstract* - Penerapan tata kelola Teknologi Informasi saat ini sudah menjadi kebutuhan dan tuntutan di setiap instansi penyelenggara pelayanan publik mengingat peran TI yang semakin penting bagi upaya peningkatan kualitas layanan sebagai salah satu realisasi dari tata kelola pemerintahan yang baik *(Good Corporate Governance)*. Dalam penyelenggaraan tata kelola TI, faktor keamanan informasi merupakan aspek yang sangat penting diperhatikan mengingat kinerja tata kelola TI akan terganggu jika informasi sebagai salah satu objek utama tata kelola TI mengalami masalah keamanan informasi yang menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*).**

***Information Security Management System (ISMS)* adalah seperangkat kebijakan berkaitan dengan manajemen keamanan informasi atau terkait dengan risiko TI. Prinsip yang mengatur di balik ISMS adalah bahwa organisasi harus merancang, menerapkan dan memelihara seperangkat kebijakan, proses dan sistem untuk mengelola risiko aset informasi mereka, sehingga memastikan tingkat risiko keamanan informasi yang dapat diterima. Dari perencanaan dan implementasi sistem manajemen keamanan informasi ini, dihasilkan daftar nilai risiko akhir aset-aset kritikal dan dokumen-dokumen tata kelola penunjang ISMS.**

Metode penelitian yang digunakan adalah studi kasus yang didalam hal ini, merupakan penelitian kualitatif. Adapun proses yang digunakan untuk mengukur tingkat kematangan dari tata kelola keamanan sistem informasi ini berdasarkan kerangka kerja ISO/IEC 27001. Dari kerangka tersebut kemudian dilakukan evaluasi terhadap objek kontrol yang dimiliki ISO/IEC 27001. Hasil yang didapat adalah peningkatan terhadap tata kelola keamanan sistem informasi. Kesimpulan dari penelitian ini adalah dibutuhkannya tata kelola keamanan sistem informasi agar IT dapat diandalkan untuk mencapai tujuan bisnis.

Kata kunci: Teknologi Informasi, Risiko, Keamanan Informasi, ISO/IEC 27001

I. PENDAHULUAN

Semakin meningkatnya pemanfaatan teknologi informasi dalam berbagai bidang maka resiko ancaman terhadap keamanan informasi juga terus meningkat. Dari berbagai sumber indikasi semakin meningkatnya ancaman terhadap keamanan informasi dapat dilihat baik dari jumlah maupun dari tingkat kecanggihannya. Kerugian finansial yang ditimbulkan sangat besar yang terjadi dalam berbagai bentuk seperti hilangnya pendapatan, besarnya biaya perbaikan, hilangnya data dan kepercayaan pelanggan serta bentuk-bentuk kerugian lain. Kenyataan ini mengharuskan pengguna teknologi informasi baik sebagai pribadi maupun institusi harus siap menghadapi ancaman keamanan informasi ini.

Keamanan informasi secara tidak langsung menjadi salah satu perhatian bagi perusahaan jika ingin melanjutkan bisnisnya. Oleh karena itu, perlu adanya standarisasi yang diterapkan atau diimplementasikan dalam perusahaan sebagai panduan yang memberikan arahan dalam menjaga aset penting seperti informasi yang dianggap sensitif bagi perusahaan tersebut.

ISO 27001 adalah suatu bentuk kerangka kerja standar internasional yang berisi tentang standar-standar dalam area keamanan informasi. ISO 27001 menyediakan kerangka kerja dalam lingkup penggunaan teknologi dan pengelolaan aset yang membantu organisasi memastikan bahwa keamanan informasi sudah efektif. Hal ini termasuk kemampuan akses data secara berkelanjutan kerahasiaan, dan integritas atas informasi yang dimilikinya.

Bank Pembangunan Daerah Sumatera Barat (Bank Nagari) adalah satu-satunya bank daerah yang berguna untuk meningkatkan perekonomian masyarakat khususnya di Sumatera Barat. Sebagai suatu lembaga keuangan yang cukup besar tentunya Bank Nagari menerapkan Teknologi Informasi sebagai salah satu cara untuk mencapai tujuan bisnis dari bank tersebut. Banyaknya jaringan yang terhubung dengan kantor pusat Bank, akan adanya dampak munculnya risiko keamanan data yang dapat mengancam Bank Nagari dalam kegiatan operasionalnya, sehingga perlu diadakan evaluasi atas keamanan informasi dengan indeks keamana informasi yang mengacu pada ISO 27001 untuk mengetahui kondisi terkini keamanan informasi yang kemudian dilanjutkan dengan membuat rekomendasi perbaikan terhadap keamanan informasi tersebut dengan harapan rekomendasi yang telah dibuat digunakan sebagai bahan pertimbangan dalam rangka upaya meningkatkan kualitas keamanan informasi agar dapat memberikan pelayanan yang lebih baik dan dapat diandalkan.

II. DASAR TEORI

A. Keamanan Informasi

Keamanan informasi berkaitan dengan perlindungan aset berharga terhadap kehilangan, pengungkapan penyalahgunaan, atau kerusakan. Dalam konteks ini, "aset berharga" adalah informasi yang direkam, diproses, disimpan, dikirim atau diambil baik dari media elektronik atau non elektronik. Upaya perlindungan tersebut dimaksudkan untuk memastikan keberlanjutan bisnis, meminimalkan risiko yang mungkin terjadi dan memaksimalkan keuntungan yang didapat dari investasi dan kesempatan bisnis [12].

Di dalam upaya penanganan maupun pengendalian terhadap keamanan informasi, kiranya harus mempertimbangkan tiga aspek penting dalam keamanan

informasi yang akrab dengan kependekan CIA (*Confidentiality, Integrity, Availability*).

1. *Confidentiality* (kerahasiaan). Merupakan aspek yang memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang.
2. *Integrity* (integritas). Merupakan aspek yang menjamin tidak adanya pengubahan data tanpa seizin pihak yang berwenang, menajaga keakuratan dan keutuhan informasi.
3. *Availability* (ketersediaan). Merupakan aspek yang memberi jaminan atas ketersediaan data saat dibutuhkan, kapanpun dan dimanapun.

B. Indeks Keamanan Informasi (KAMI)

Indeks KAMI merupakan alat evaluasi untuk menganalisa tingkat kesiapan atau kematangan SMKI di Instansi pemerintah. Alat evaluasi ini disusun oleh Tim Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika. Indeks KAMI digunakan untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) 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[14].

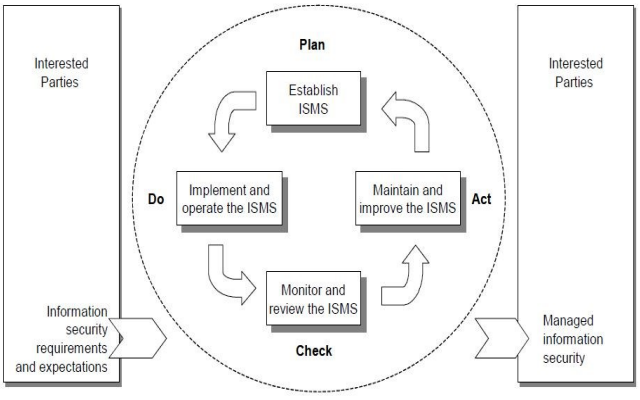
C. ISO 20071

ISO/IEC 27001 merupakan standar keamanan informasi yang menggantikan BS-7799:2 dan diterbitkan pada bulan Oktober 2005 oleh *International Organization for Standarization* dan *International Electrotechnical Commission.*

ISO 27001 berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan [14].

Standar ini mengadopsi "*Plan-Do-Check-Act*" (PDCA) model, yang digunakan untuk mengatur semua proses SMKI. Penerapan model PDCA juga akan mencerminkan prinsip-prinsip sebagaimana diatur dalam Pedoman OECD (2002) yang mengatur keamanan sistem informasi dan jaringan. Standar ini memberikan model untuk menerapkan prinsip-prinsip dalam pedoman yang mengatur penilaian risiko, desain keamanan dan implementasi, manajemen keamanan dan penilaian ulang [14].

Dalam model PDCA, keseluruhan proses SMKI dapat dipetakan seperti pada Gambar 1.



Gambar 1. Model PDCA yang diterapkan untuk proses SMKI (Sistem Manajemen Keamanan Informasi)

ISO 27001 memiliki sebelas klausul kontrol keamanan (*security control*), 39 objektif control (*control objectives*) dan 133 kontrol keamanan/control (*controls*). Sebelas klausul kontrol keamanannya adalah sebagai berikut [14]:

1. Kebijakan keamanan informasi
2. Organisasi keamanan informasi
3. Manajemen aset
4. Sumber daya manusia menyangkut keamanan informasi
5. Keamanan fisik dan lingkungan
6. Komunikasi dan manajemen operasi
7. Akses control
8. Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi
9. Pengelolaan insiden keamanan informasi
10. Manajemen kelangsungan usaha (*business continuity management*)
11. Kepatuhan

III. METODOLOGI PENELITIAN

A. Metodologi Penelitian

Penelitian ini merupakan jenis penelitian analisis deskriptif kuantitatif [16], dimana peneliti akan melakukan analisis dengan mendiskripsikan tingkat kematangan SMKI PT. Bank Pembangunan Daerah Sumatera Barat (Bank Nagari) berdasarkan skor atau nilai yang dihasilkan Indeks KAMI. Deskripsi yang dilakukan penulis didasarkan pada panduan dalam penggunaan indeks KAMI.

B. Teknik Pengumpulan Data

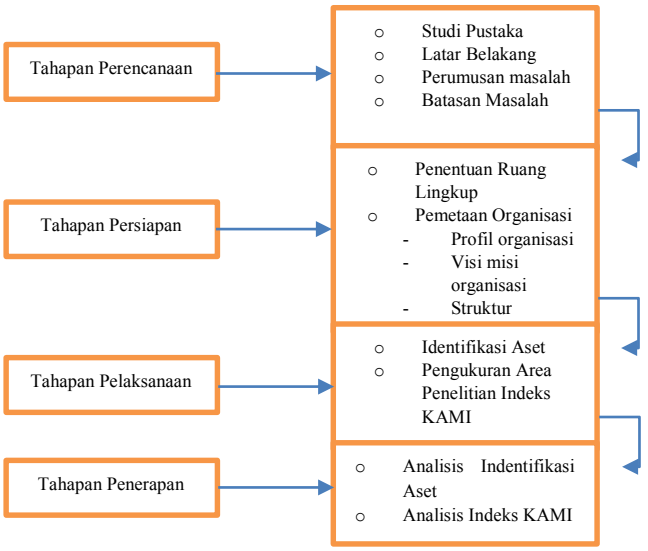
Studi kepustakaan diharapkan mampu menggali seluruh informasi yang terkait dengan permasalahan yang akan diteliti dan objek yang menjadi tujuan penelitian. Studi kepustakaan ini memberikan dasar bagi arah penelitian yang akan dilakukan serta menjadi awal pemikiran bagi setiap peneliti sehingga penelitian yang dilakukan dapat dijadikan acuan kembali dikemudian hari.

Selain itu, peneliti menggunakan kuesioner untuk mengumpulkan data-data terkait kesiapan Bank Nagari dalam menerapkan SMKI. Kuesioner yang akan digunakan peneliti adalah Indeks Keamanan Informasi (Indeks KAMI) versi 2.3 dari Kementerian Komunikasi dan Informatika dengan pertimbangan:

1. Karena dalam penyusunannya Indeks KAMI mengacu pada sumber yang sama dengan acuan dalam penyusunan KMK 479/2010, maka tingkat kesiapan atau kematangan yang menjadi *output* utama dari penggunaan indeks ini dapat digunakan disamakan dengan tingkat kesiapan/kematangan Bank Nagari dalam menerapkan ketentuan yang ada dalam KMK 479/2010.
2. Indeks KAMI telah digunakan Direktorat Keamanan Informasi Kementerian Komunikasi dan Informasi untuk mengukur tingkat kematangan SMKI pada sejumlah instansi dan perusahaan, oleh karenanya peneliti menganggap Indeks KAMI valid untuk digunakan dalam kepentingan penelitian ini, sehingga peneliti tidak perlu menyusun kuesioner khusus untuk tujuan pengukuran tingkat kesiapan dan kematangan SMKI di Bank Nagari.

C. Tahap Penelitian

Tahapan dari penelitian ini dijelaskan pada gambar 3.1 sebagai berikut:



Gambar 2. Tahapan Penelitian

IV. HASIL DAN PEMBAHASAN

Bagian ini membahas tentang proses implementasi sistem dan hasil pengujian terhadap aplikasi pada tugas akhir ini.

A. Hasil Identifikasi Aset

Setelah melakukan tahapan identifikasi aset di unit Divisi TI didapat 6 kategori aset beserta data-data aset yang dimiliki dan dapat dilihat pada tabel-tabel berikut.

Kategori aset yang pertama ditemukan dari tahapan identifikasi yaitu aset sumber daya manusia. Kategori dari aset sumber daya manusia yang terdapat di dalam sistem pengamanan informasi Bank Nagari ditunjukkan dalam Tabel 1 dibawah ini:

TABEL I
REGISTRASI ASET SUMBER DAYA MANUSIA (SDM)

No	Nama Aset
1.	Grup Strategi dan Kebijakan Sistem Informasi (IT Governance, Compliance, …)
2.	Grup Pengembangan dan Pemeliharaan Sistem Informasi (Application Development, Database Administrator, Business Analyst, Electronic Data Interchange, …)
3.	Grup Pengelolaan Operasional, Layanan, Sarana dan Aset Sistem Informasi (Help Desk, End User Support, Network Administration, System Administrator, Infrastructure / Operations Manager,…)

Selanjutnya aset yang didapat yaitu pada kategori aset data. Kategori dari aset data yang terdapat di dalam system pengaman informasi Bank Nagari ditunjukkan dalam Tabel 2 dibawah ini:

TABEL II
REGISTRASI ASET DATA

No	Nama Aset
1.	Data Transaksional Harian
2.	Data Identitas Nasabah
3.	Data Nominal Nasabah
4.	Password dan Username Staf
6.	Data office Divisi TI

Kategori aset selanjutnya yang didapat yaitu pada kategori aset sarana pendukung. Kategori dari aset sarana pendukung yang terdapat di dalam unit sistem informasi fakultas teknik ditunjukkan dalam Tabel 3 dibawah ini:

TABEL III
REGISTRASI ASET SARANA PENDUKUNG

No	Nama Aset
1.	Genset
2.	UPS
3.	AC

Selanjutnya aset yang didapat yaitu pada kategori aset fasilitas. Kategori dari aset fasilitas yang terdapat di dalam unit sistem informasi fakultas teknik ditunjukkan dalam tabel 4 dibawah ini:

TABEL IV
REGISTRASI ASET FASILITAS

No	Nama Aset
1.	Ruang penyimpanan server
2.	Rak server
3.	Rak aset data

Selanjutnya aset yang didapat yaitu pada kategori aset perangkat keras dan jaringan. Kategori dari aset perangkat keras dan jaringan yang terdapat di dalam unit sistem informasi fakultas teknik ditunjukkan dalam Tabel 5 dibawah ini:

TABEL V
REGISTRASI ASET PERANGKAT KERAS DAN JARINGAN

No	Nama Aset
1.	PC
2.	LCD TV
3.	Printer
4.	Scanner
5.	Monitor LCD
6.	Router
7.	Switch Layer 2
8.	Switch Layer 3
9.	Modem
10.	Akses Point
11.	Server

Selanjutnya aset yang didapat yaitu pada kategori aset perangkat lunak. Kategori dari aset perangkat lunak yang terdapat di dalam sistem pengamanan informasi Bank Nagari ditunjukkan dalam Tabel 6 dibawah ini:

TABEL VI
REGISTRASI ASET PERANGKAT LUNAK

No	Nama Aset
1.	Aplikasi Client Core Banking
2.	Aplikasi Client Card Management (Xcard dan XcardWeb)
3.	Aplikasi SKN – BI
4.	Aplikasi BI RTGS/BI SSSS
5.	Aplikasi Terminal Western Union
6.	Aplikasi SWIFT
7.	Aplikasi Siskohat
8.	Aplikasi CMS (Cash Management Security)
9.	Aplikasi AntiFraud
10.	Aplikasi Risk Base Audit (RBA)
11.	Loan Integrated Support System (LISS)
12.	Aplikasi Pelaporan BI (LHBU, LKPBU, LBBU, LBU, SID, DHN, APMK, dll)
13.	Aplikasi Web dan Email
14.	Aplikasi Server & Client OLIBS
15.	Aplikasi Switching
16.	Aplikasi SID
17.	Aplikasi Translink, Voyager

Tabel-tabel diatas merupakan aset yang didapat melalui tahapan identifikasi aset. Semua aset tersebut memiliki fungsi yang berbeda-beda dan semua aset tersebut mendukung proses kerja pada unit divisi teknologi informasi Bank Nagari. Setelah melakukan tahapan identifikasi aset dan telah didapat data-data yang diinginkan maka tahap selanjutnya adalah melakukan tahapan analisa risiko dari semua aset yang didapat.

B. Analisa Risiko

Tahapan analisa risiko merupakan tahap lanjutan setelah tahap identifikasi aset. Dari hasil identifikasi, semua aset yang teridentifikasi akan dilakukan analisa risiko dari aset tersebut guna mengetahui tinggi dan rendahnya kritikalitas aset tersebut bagi organisasi serta mengetahui kerawanan, dampak, ancaman dan seberapa kecenderungan ancaman itu terjadi bagi aset.

a. Identifikasi Risiko

Proses identifikasi risiko digunakan sebagai acuan dasar untuk mengetahui risiko yang ada pada suatu aset. Dalam identifikasi risiko digunakan cara menganalisa kritikalitas dan menghitung nilai kritikalitas pada aset tersebut. Analisa ini berguna untuk mengetahui tinggi dan rendahnya tingkat kritikalitas aset bagi organisasi.

Hasil analisa kritikalitas salah satunya dari aset sumber daya manusia dapat lihat pada Tabel 7. dibawah ini:

TABELVII
HASIL ANALITAS KRITIKALITAS PERANGKAT KERAS DAN JARINGAN

No	Nama Aset	C	I	A	Kritikalitas
1.	PC	H	H	H	Kritikal
2.	LCD TV	M	M	M	Tidak kritikal
3.	Printer	M	M	M	Tidak kritikal
4.	Scanner	M	M	M	Tidak kritikal
5.	Monitor LCD	M	M	M	Tidak kritikal
6.	Router	H	H	H	Kritikal
7.	Switch Layer 2	H	H	H	Kritikal
8.	Switch Layer 3	H	H	H	Kritikal
9.	Modem	H	H	H	Kritikal
10.	Akses Point	H	H	H	Kritikal
11.	Server	H	H	H	Kritikal

Dari hasil analisa yang dilakukan diketahui ada 34 aset yang berada pada kategori kritikal dan 8 aset berada pada kategori tidak kritikal. Tahap analisa kritikalitas ini merupakan tahap awal dari proses analisa risiko. Setelah melakukan identifikasi risiko berdasarkan kritikalitas pada aset selanjutnya akan dihitung nilai pada aset yang telah teridentifikasi. Penilaian yang dilakukan menggunakan rumus:

Asset Value = (Confidentiality + Integrity + Availability) / 3

Hasil penilaian aset perangkat keras dan jaringan ditunjukkan oleh Tabel 9 sebagai berikut.

TABEL VIII
NILAI PADA ASET PERANGKAT KERAS DAN JARINGAN

No	Nama Aset	C	I	A	Nilai aset
1.	PC	3	3	3	3
2.	LCD TV	2	2	2	2
3.	Printer	2	2	2	2
4.	Scanner	2	2	2	2
5.	Monitor LCD	2	2	2	2
6.	Router	3	3	3	3
7.	Switch Layer 2	3	3	3	3
8.	Switch Layer 3	3	3	3	3
9.	Modem	3	3	3	3
10.	Akses Point	3	3	3	3
11.	Server	3	3	3	3

b. Analisa Kecenderungan dan Dampak

Setelah dilakukannya tahapan identifikasi risiko berdasarkan kritikalitas pada aset dengan mengarah pada kriteria penilaian *confidentiality*, *integrity*, dan *availability*. Dari analisa awal itu didapat hasil sementara aset-aset mana saja yang memiliki kriteria "kritikal" dan "tidak kritikal. Selanjutnya akan dilakukan tahapan analisa selanjutnya dari penelitian ini dimana analisa dilakukan dengan menentukan deskripsi risiko untuk setiap kategori informasi berdasarkan ancaman *(Threat),* kerawanan *(Vulnerability)* dan dampak *(Effect)*.

Hasil analisa kecenderungan dan dampak salah satunya dari aset perangkat keras dan jaringan ditunjukkan pada Tabel 10 sebagai berikut.

TABEL IX
HASIL ANALISA KECENDERUNGAN DAN DAMPAK ASET PERANGKAT KERAS DAN JARINGAN

Kategori Aset	Aset	Deskripsi Risiko			Kontrol yang ada saat ini	Risiko inheren	
		Kerawanan	Ancaman	Dampak		Nilai dampak	Nilai kecenderungan
Aset Perangkat keras dan Jaringan	PC	Kurang baiknya manajemen pengamanan dan hak akses fisik ruangan	PC dapat diakses oleh pihak yang tidak berwenang	Kegiatan terkait pengadaan secara elektronik terganggu	-perimeter gedung (kunci dan pembatas fisik) - Penerimaan tamu gedung	1	1
	LCD TV	Di letakkan di tempat umum yang dapat dilihat dan diakses oleh siapa saja	Rawan kehilangan	Tidak dapat memonitor jaringan dari layar LCD TV	-perimeter gedung (kunci dan pembatas fisik) - Penerimaan tamu gedung - petugas keamanan	1	1

Setelah menentukan nilai kecenderungan dan nilai dampak selanjutnya dilakukan perhitungan penilaian risiko akhir. Perhitungan ini didapat dengan menggunakan rumus:

Nilai Risiko = Nilai Dampak x Nilai Kecenderungan

Setelah melakukan penghitungan nilai risiko, hasil dari penilaian tersebut akan dibagi kedalam beberapa tingkatan kategori antara lain kategori rendah, sedang dan tinggi. Masing-masing tingkatan juga akan memiliki nilai yang tersendiri antara lain:

1. Nilai 0 - 5: Rendah
2. Nilai 6 – 11: Sedang
3. Nilai 12 – 16: Tinggi

Dari hasil penghitungan nilai risiko diatas jika dilihat berdasarkan persentase persebaran risiko maka nilai risiko pada kategori rendah berjumlah 89,75 % dan pada kategori sedang berjumlah 10,25 % dan dapat dilihat pada Gambar 3. berikut.

Gambar 3. Persentase nilai risiko

C. Pemetaan *Control Objective & Control*

Pemetaan *control objective & control* ini berdasarkan dari ISO 27001, dimana pada masing-masing aset akan dikontrol melalui klausul-klausul yang dimiliki oleh ISO 27001 guna mengurangi risiko yang ada pada masing-masing aset. Pengontrolan ini tidak terbatas pada aset yang bernilai tinggi ataupun rendah, tetapi lebih kepada semua aset yang telah teridentifikasi di awal. Karena setiap aset yang teridentifikasi memiliki fungsi dan peran yang saling mendukung satu sama lain dalam proses kerja unit sistem informasi fakultas teknik. Maka dari itu diperlukannya pengontrolan agar mengurangi risiko yang terjadi dikemudian harinnya. Adapun hasil pemetaan kontrol-kontrol tersebut dapat dilihat pada Tabel 11 berikut.

TABEL X
HASIL PEMETAAN KLAUSUL ISO 27001 TERHADAP ASET

kategori aset	aset	deskripsi risiko			kontrol yang ada saat ini	kontrol iso 27001
		kerawanan	ancaman	dampak		
aset perang-kat keras dan jaringan	pc	kurang baiknya manajemen pengaman-an dan hak akses fisik ruangan	pc dapat diakses oleh pihak yang tidak berwena-ng	kegiatan terkait pengadaan secara elektronik terganggu	-perimeter gedung (kunci dan pembatas fisik) - penerimaan tamu gedung	a.9.1 (area yang aman) a.10.7.1 (manajemen media yang dapat dipindahkan)
	lcd tv	di letakkan di tempat umum yang dapat dilihat dan diakses oleh siapa saja	rawan kehila-ngan	tidak dapat memonitor jaringan dari layar lcd tv	-perimeter gedung (kunci dan pembatas fisik) - penerimaan tamu gedung - petugas keamanan	a.9.1 (area yang aman) a.10.7.1 (manajemen media yang dapat dipindahkan)

D. Indeks KAMI

Pada bagian hasil dan pembahasan akan dijelaskan hal-hal terkait data penelitian, kegiatan assessment keamanan informasi menggunakan Indeks KAMI dan hasil yang diperoleh.

a. Data Pengukuran Indeks KAMI Pada Bank Nagari

Langkah pertama penggunaan indeks KAMI adalah dengan menjawab pertanyaan terkait kesiapan pengamanan informasi, responden diminta untuk mendefinisikan Peran TIK (atau Tingkat Kepentingan TIK) di Instansinya. Tujuan dari proses ini adalah untuk mengelompokkan instansi ke "ukuran" tertentu: Rendah, Sedang, Tinggi dan Kritis – Tabel 1. Setelah itu dilakukan pengukuran kesiapan keamanan informasi mulai dari tata kelola informasi, pengelolaan resiko keamanan informasi table, pengukuran kerangka kerja keamanan informasi table, pengukuran pengelolan aset informasi table, dan pengukuran teknologi dan keamanan informasi.

Berikut merupakan hasil responden dalam memdefeneisikan peran TIK pada Tabel 12.

TABEL XI
DATA PENGUKURAN PERAN DAN TINGKAT KEPENTINGAN TIK DALAM INSTANSI

Bagian I: Peran dan Tingkat Kepentingan TIK dalam Instansi				
Bagian ini memberi tingkatan peran dan kepentingan TIK dalam Instansi anda.				
Tingkat Kepentingan] Minim [0]; Rendah[1]; Sedang[2]; Tinggi[3]; Kritis [4]				
Jumlah Pertanyaan				12
Jawaban Bagian I				
Minim	Rendah	Sedang	Tinggi	Kritis
-	1	2	6	2
Skor Peran dan Tingkat Kepentingan TIK di Instansi				**31**

Dari Tabel 12 dapat dilihat untuk Skor Pengukuran Peran dan Tingkat Kepentingan TIK dalam Instansi dengan nilai 31 dari nilai maksimal area ini sebesar 48. Dari 12 pertanyaan pada area ini, 6 pertanyaan diantaranya direspon "Tinggi" oleh para responden.

TABEL XII
DATA PENGUKURAN KELENGKAPAN TATA KELOLA KEAMANAN INFORMASI

Bagian II: Tata Kelola Keamanan Informasi			
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
Jumlah Pertanyaan			20
Jawaban Bagian II			
Status pengamanan	Kategori Kontrol		
	1	2	3
Tidak Dilakukan	-	-	-
Dalam Perencanaan	-	2	1
Dalam Penerapan atau Diterapkan Sebagian	4	4	5
Diterapkan Secara Menyeluruh	4	-	-
Total Nilai Evaluasi Tata Kelola			**39**

Dari Tabel 13 dapat dilihat untuk Skor Pengukuran Kelengkapan Tata Kelola Keamanan Informasi dengan nilai 39 dari nilai maksimal area ini sebesar 114. Dari 20 pertanyaan pada area ini, 4 pertanyaan diantaranya direspon "Dalam Penerapan atau Diterapkan Sebagian" pada tahap 1 oleh responden.

TABEL XIII
DATA PENGUKURAN KEMATANGAN TATA KELOLA KEAMANAN INFORMASI

Status Penerapan	**Tingkat Kematangan**				**Total**
	II	**III**	**IV**	**V**	
Tidak Dilakukan	-	-	-	-	
Dalam Perencanaan	4		1		5
Dalam Penerapan/Diterapkan Sebagian	6	3	5	-	14
Diterapkan Secara Menyeluruh	1	-	-	-	1
Total	**11**	**3**	**6**		**20**

Sementara pada tabel 4.35 dari tingkat kematangan (Level II s.d. V), sebanyak 6 dari 11 pertanyaan pada Level II direspon "Dalam Penerapan/Diterapkan Sebagian", selain itu seluruh dari pertanyaan Level III juga diberi respon yang sama.

b. Hasil Pengukuran Indeks KAMI Pada Bank Nagari

Dari data pengukuran yang telah dilakukan menggunakan indeks KAMI diperoleh hasil yang mencakup peran TIK di Bank Nagari, serta tingkat kematangan masing-masing bagian keamanan informasi yang terdapat di Bank Nagari.

Untuk Bagian I pada Tabel 4.44 yaitu Peran dan Kepentingan TIK di Instansi menunjukkan bahwa TIK memegang peran yang penting di Bank Nagari, hal ini ditunjukkan oleh perhitungan indek KAMI, untuk bagian I Bank Nagari memiliki Skor 31 yang berarti Peran TIK di Bank Nagari **Tinggi** yang dapat dilihat pada Tabel 15.

TABEL XIV
HASIL PENGUKURAN PERAN/TINGKAT KEPENTINGAN TIK

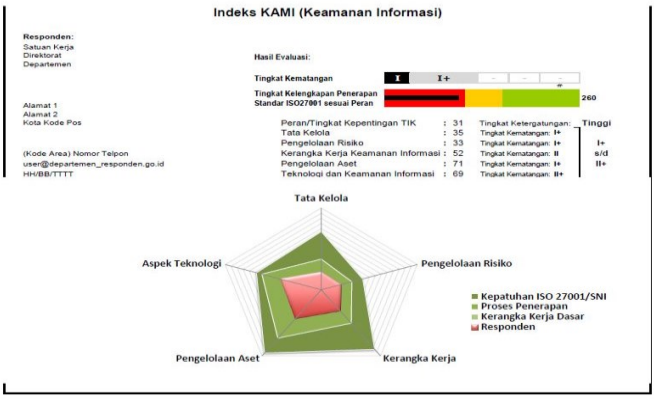
Bagian I Peran dan Tingkat Kepentingan TIK di Instansi		**Skor**
Skor	**Tingkat**	
0 – 12 13 – 24 25 – 36 37 – 48	[Rendah] [Sedang] [Tinggi] [Kritis]	31 **Tinggi**

Sementara untuk Bagian II, III, IV dan V dan VI digunakan untuk mengukur tingkat kematangan keamanan informasi di Bank Nagari. Hasil pengukuran dapat dilihat pada Tabel 16.

TABEL XV
HASIL PENGUKURAN BAGIAN-BAGIAN KEAMANAN INFORMASI

Indeks KAMI	**Skor**	**Tingkat kematangan**
Bagian II: Tata Kelola Keamanan Informasi	39	I+
Bagian III: Pengelolaan Risiko Keamanan Informasi	33	I+
Bagian IV: Kerangka Kerja Pengelolaa Keamanan Informasi.	96	II
Bagian V: Pengelolaan Aset Informasi	75	II
Bagian VI: Teknologi dan Keamanan Informasi	70	II+
Total Skor (II+III+IV+V+VI)	**313**	**I+ s/d II+**

Pada Gambar 4.2 Menunjukkan hasil pengukuran Bagian IV, V, dan VI menunjukkan bawa tingkat kematangan keamanan informasi di Bank Nagari berada pada Level II dan II+ yaitu **Penerapan Kerangka Kerja Dasar,** sementara untuk bagian II, dan II berada pada tingkat kematangan keamanan informasi di Bank Nagari masih berupa **Kondisi Awal.**

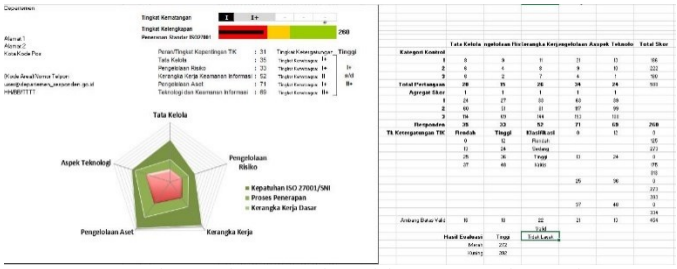


Gambar 4. Tingkat Kematangan Indeks KAMI Bank Nagari

Sehingga hasil akhir dari pengukuran keamanan informasi menggunakan indeks KAMI untuk Bank Nagari mendapatkan kesimpulan bahwa kemanan informasi yang terdapat pada Bank Nagari masih **Perlu Perbaikan**, seperti pada Tabel 4.46, dan diagram radar pada Gambar 17.

TABEL XVI
KESIMPULAN INDEKS KAMI BANK NAGARI

Skor Bagian I			**Skor Bagian II+III+IV+V+VI**		**Kesimpulan**
0	12	Rendah	0	124	Tidak Layak
			125	272	Perlu Perbaikan
			273	588	Baik/Cukup
13	24	Sedang	0	174	Tidak Layak
			175	312	Perlu Perbaikan
			313	588	Baik/Cukup
25	36	Tinggi	0	272	Tidak Layak
			273	392	**Perlu Perbaikan**
			393	588	Baik/Cukup
37	48	Kritis	0	333	Tidak Layak
			334	453	Perlu Perbaikan
			454	588	Baik/Cukup



Gambar 5. Diagram Radar Indeks KAMI Bank Nagari

Hasil ini dapat memberikan gambaran kepada para pengambil keputusan sebagai bahan evaluasi diri untuk dapat membuat perencanaan untuk perbaikan, sehingga secara bertahap diharapkan dapat memenuhi standar ISO 27001 dan selanjutnya institusi siap untuk di sertifikasi ISO 27001 *Information Security Managemen System* (ISMS).

E. Rekomendasi Keamanan Informasi Untuk Bank Nagari

Hasil pengukuran kemananan informasi menggunakan indeks KAMI untuk Bank Nagari menunjukkan tingkat kematangan keamanan informasi I+ s/d II+. Sementara untuk mendapatkan kesiapan sertifikasi ISO/IEC 27001, tingkat kematangan kemanan informasi minimal berada pada level III (Terdefinisi dan Konsisten). Adapun hal-hal yang dapat direkomendasi untuk meningkatkan tingkat kematangan informasi di Bank Nagari adalah sebagai berikut:

1. Bagian I Peran dan Tingkat kepentingan TIK [Tinggi]: Perlunya perencanaan pada anggaran untuk keamanan informasi, guna meningkatkatkan hal-hal terkait operasional dan monitoring kegiatan keamanan informasi.
2. Bagian II Tata Kelola Keamanan Informasi [I+] → [III]: Perlunya perencanaan dan pendokumentasian yang jelas kepada fungsi dan tanggung jawab pengelola kemanan informasi serta tindakan-tindakan pengembangan berkelanjutan terkait tata kelola keamanan informasi.
3. Bagian III Pengelolaan Resiko Keamanan Informasi [I+] → [III]: Perlunya pendokumentasiaan rencana-rencana terkait resiko keamanan informasi, kerangka kerja penanganan resiko keamanan informasi yang terdefinisi dan tindakan-tindakan yang berkelenjutan, dalam penanganan hal-hal terkait resiko keamanan informasi.
4. Bagian IV Kerangka Kerja Pengelolaan Keamanan Informasi [II] → [III]: Perlunya pendokumentasian yang jelas (terdefinisi) terhadap kerangka kerja (kebijakan dan prosedur) keamanan informasi serta melakukan uji coba dan monitoring kerangka kerja keamanan informasi secara berkelanjutan.
5. Bagian V Pengelolaan Aset Keamanan Informasi [II] → [III] : Perlunya perencanaan pengolaan aset keamanan informasi yang lebih terdefinisi dan terkomentasi, prosedur dan kebijakan mengenai operasional aset keamanan dan perlu diperjelas fungsi dan peranannya dari aset keamanan informasi, serta melakukan evaluasi / monitoring berkala mengenai keberadaan dan fungsi aset keamanan informasi tersebut
6. Bagian VI Teknologi dan Keamanan Informasi [II+] → [III]: Perlu adanya dokumentasi yang jelas (terdefinisi) terkait kelengkapan, evaluasi dan efektifitas penggunaan teknologi, monitoring yang dilakukan secara berkala guna mendapatkan infomasi secara menyeluruh terhadap keamanan informasi di instansi.

V. KESIMPULAN DAN SARAN

Bagian ini menjelaskan kesimpulan dan saran dari hasil penelitian dan pembahasan.

A. Kesimpulan

Berdasarkan hasil penelitian yang dilakukan dalam perencanaan dan implementasi standar keamanan sistem informasi menggunakan standar ISO/IEC 27001, maka dapat disimpulkan hal-hal sebagai berikut:

1. Pelaksanaan pengukuran identifiaksi aset berdasarkan ISO 20071 menghasilkan identifikasi ruang lingkup aset yang kemudian dilakukan analisis risiko terhada aset. Langkah analisis risiko keamanan informasi dilakukan dengan melakukan penilaian tingkat kritikalitas pada aset dan kemudian melakukan analisis kecenderungan dan dampak dengan menentukan deskripsi risiko dari setiap kategori informasi berdasarkan ancaman *(Threat),* kerawanan *(Vulnerability)* dan dampak *(Effect)*.
2. Berdasarkan hasil analisa kritikalitas aset yang mengacu pada kriteria kerahasiaan (*confidentialty*), keutuhan (*integrity*), dan ketersediaan (*availability),* dari seluruh aset yang diidentifikasi terdapat 34 aset memiliki tingkat kritikalitas pada kategori "kritikal" dan 8 aset pada kategori "tidak kritikal".
3. Dengan indeks KAMI, dapat diukur tingkat kematangan keamanan informasi di Bank Nagari yang mencakup Peran TIK, Tata kelola, resiko, kerangka kerja, aset dan teknologi keamanan informasi. Hasil yang diperoleh adalah bahwa tingkat kematangan keamanan informasi Bank Nagari berada pada level I+ s/d II+, dimana untuk mendapatkan sertifikasi ISO/IEC 27001 level keamanan informasi adalah minimal pada level III.

B. Saran

Dari penelitian yang telah dilakukan, dapat diberikan beberapa saran sebagai berikut:

1. Disarankan bagi peneliti untuk proses pengidentifikasi dokumen-dokumen yang dibutuhkan hendaknya dibahas lebih mendetail dengan diskusi dengan pihak-pihak terkait sehingga dapat lebih mengerti proses manajemen keamanan informasi dari tempat penelitian.
2. Dalam penelitian ini hanya berfokus pada standar keamanan informasi ISO/IEC 27001. Diharapkan dalam penelitian berikutnya disertakan juga perbandingan manajemen keamanan informasi antara ISO, COBIT dan standar keamanan informasi yang lain agar hasil lebih optimal.

DAFTAR PUSTAKA

[1] J. K. G. Pavlov, "*Information Security Management System In Organization*," *Trakia Journal of Sciences,* p. 25, 2011.

[2] A. Rezakhani, "*Standardization of all Information Security Management Systems*," *International Journal of Computer Applications,* p. 4, 2011.

[3] I. Afrianto, "Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI - SNI ISO/IEC 27001:2009 Studi Kasus Perguruan Tinggi X," pp. 43-48, 2015.

[4] J. P. L. A. A. E. Kenneth C. Laudon, *Management Information System, England: Pearson Eduacation* LTD, 20013.

[5] E. Turban, *Improving Strategic and Operational Performance*, United States of America: Times Ten Roman, 2011.

[6] J. Karimi, "*Impact Of Competitive Strategy And Information Technology Maturity On Firm' Strategic Response to Globalization*," *Journal of Management Information Systems,* pp. 55-88, 1996.

[7] P. D. M. Goeken, *Best Practice Referenzmodelle der IT Governance*, Fritzlar, Germany: School of Finance & Management angefertigt, 2011.

[8] D. A. Harrison, *The Application of the Theory of Reasoned Action to Senior Management and Strategic Information Systems*, Texas: University of Texas at Arlington, 1993.

[9] E. Sunjaya, "Pengaruh Tipologi Strategi Kompetitif dan Kematangan Teknologi Informasi Terhadap Respon Strategik Manajer," p. 13, 2010.

[10] W. Priatna, "Pengaruh Kmatangan, Kinerja dan Pemanfaatan Teknologi Informasi Terhadap Implementasi SI di SMK Negeri Jakarta Timur dengan Model Cobit Framework," pp. 121-123, 2013.

[11] A. Setiawan, "Pengaruh Kematangan, Kinerja dan Perkembangan Teknologi Informasi di Perguruan Tinggi Swasta Yogyakarta dengan Model Cpnit Framework," pp. 3-8, 2008.

[12] N. A. Widodo, "Perancangan Audit Internal Sistem Manajemen Keamanan Informasi (SMKI) Berdasarkan Standar ISO/IEC 27001:2005 Di PT. Bpr Karyajatnika Sadaya.," pp. 2-3, 2012.

[13] M. Anchar, "Strategi Keamanan Informasi Perusahaan Media Cetak/Online Menggunakan Tinjuan Information Security Management System (ISMS)," pp. 16-17, 2010.

[14] Tim Direktorat Keamanan Informasi, Panduan Penerapan Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik, Jakarta: Kominfo, 2011.

[15] Schweizer Norm, "*Information technology - Security techniques - Information security management systems -Requirements," ISO/IEC 27001 International Standard*, Switzerland, 2013.

[16] Sugiyono, Metode Penelitian Kuantitatif Kualitatif dan R&D, Bandung: Alfabeta, 2012.