Jurnal Computech & Bisnis, Vol. 14, No. 1, Juni 2020, 10-18
ISSN (print): 1978-9629, ISSN (online): 2442-4943

EVALUASI TATA KELOLA KEAMANAN TEKNOLOGI INFORMASI MENGGUNAKAN INDEKS KAMI UNTUK PERSIAPAN STANDAR SNI ISO/IEC 27001 (STUDI KASUS: STMIK MARDIRA INDONESIA)

Asep Ririh Riswaya[1], Ashwin Sasongko[2], Asep Maulana[3]
STMIK Mardira Indonesia[1], Universitas Langlangbuana Bandung[23]
aririhriswaya@gmail.com[1], ashwin.sasongko@gmail.com[2], siapok@yahoo.com[3]

Abstract

Today's technology is an important asset to support the business activities of institutions or institutions, STMIK Mardira Indonesia *is a higher education institution that requires technology for educational service facilities. Information technology security governance is useful for protecting assets while maintaining the sustainability of information technology services, several standards for governance have also been used to ensure the security of information technology assets,* SNI ISO / IEC 27001 *and* SNI ISO / IEC 27002 *are national standards that adopt from international standards in its activities require evaluation to determine governance readiness and the US index is used as an evaluation tool towards the standardization. The evaluation results in the electronics sector have a value of 21 which means the electronics sector in this institution is high according to the US Index 10 to 15 low, 16 to 34 high and 35 to 50 strategic. However, on the status of preparedness with a value of 117 which means that it is still not feasible for SNI ISO / IEC 27001 certification to be eligible for certification is a range of values 273 to 445. On the basis of some evaluation results obtained, governance is carried out in Annex A.5.1.1 Information security policy document, A.5.1.2 Review of the policies for information security, A.6.1.1 Information security roles and responsibilities, A.15.1.1 Information security policy for supplier relationships, A.16.1 Reporting information security events and weaknesses and Annex 16.1 .3 Reporting information security weaknesses.*

***Keywords**: Governance TI, Information Technology Security, SNI ISO / IEC 27001 and SNI ISO / IEC 27002.*

Abstrak

Teknologi masa kini menjadi aset penting untuk menunjang kegiatan bisnis intansi atau lembaga, STMIK Mardira Indonesia merupakan lembaga pendidikan tinggi yang membutuhkan teknologi untuk sarana layanan lembaga pendidikan. Tata kelola keamanan teknologi informasi berguna untuk melindungi aset juga menjaga keberlangsungan layanan teknologi informasi, beberapa standar untuk tata kelola juga telah digunakan untuk menjamin keamanan aset teknologi informasi, SNI ISO/IEC 27001 dan SNI ISO/IEC 27002 merupakan standar nasional yang mengadopsi dari standar internasional dalam kegiatan nya memerlukan evaluasi untuk menentukan kesiapan tata kelola dan indeks KAMI digunakan sebagai alat evaluasi menuju standarisasi tersebut. Hasil evaluasi pada bagian sektor elektronik memiliki nilai 21 yang artinya sektor elektronik di lembaga ini tinggi menurut Indeks KAMI 10 s.d 15 rendah, 16 s.d 34 tinggi dan 35 s.d 50 strategis. Namun pada status kesiapan berinilai 117 yang artinya masih tidak layak untuk tersertifikasi SNI ISO/IEC 27001 untuk cakupan layak sertifikasi adalah rentang nilai 273 s.d 445. Dengan dasar beberapa hasil evaluasi yang didapat maka tata kelola dilakukan pada Annex *A.5.1.1 Information security policy document, A.5.1.2 Review of the policies for information security, A.6.1.1 Information security roles and responsibilities, A.15.1.1 Information security policy for supplier relationships, A.16.1 Reporting information security events and weaknesses* dan *Annex 16.1.3 Reporting information security weaknesses*.

Kata Kunci: Tata Kelola Teknologi Informasi, Keamanan Teknologi Informasi, SNI ISO/IEC 27001 dan SNI ISO/IEC 27002

PENDAHULUAN

Pemanfaatan TI sangat berperan dalam segala sektor kehidupan, baik sektor penyelenggaraan pemerintah maupun swasta. Dalam penyelenggaraan layanan publik menurut Badan Standarisasi Nasional (BSN) memerlukan *good governance* yang akan menjamin transparansi, akuntabilitas, efisiensi, dan evektifitas layanan TI. Selain BSN ada pula peraturan menteri komunikasi dan informatika no. 41 tahun 2007 menjelaskan panduan umum tata kelola teknologi inforamsi dan komunikasi nasional,

menandakan bahwa tata kelola TI penting untuk menunjang penyelenggaraan layanan TI, walaupun pada tahun 2018 peraturan menteri no. 41 dicabut namun diatur ulan perbagian oleh peraturan-peraturan menteri lain nya.

Badan Standarisasi Nasional menetapkan pada tanggal 8 April 2016 SNI ISO/IEC 27001:2013 sebagai standar nasional dalam teknologi informasi, teknik keamanan, dan sistem manajemen keamanan informasi juga menetapkan terjemaahan standar nasional Indonesia adopsi identik standar *international organization for standarization* / *international electrotechnical commission* dalam bahasa Indonesia. Untuk mendapatkan ukuran terstandarisasi SNI ISO/IEC 27001:2013 Badan Siber dan Sandi Negara (BSSN) mengeluarkan aplikasi yang digunakan sebagai alat bantu untuk menganalisa dan mengevaluasi tingkat kesiapan (kelengkapan dan kematangan) penerapan SNI ISO/IEC 27001:2013 yaitu indeks KAMI (Keamanan Informasi).

Indeks KAMI (Keamanan Informasi) tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan kerangka kerja keamanan informasi, indeks kami dirilis pertama kali di tahun 2009 (indeks KAMI versi 1,0) kemudian digunakan untuk analisis tingkat kematangan pada tanggal 2 Juni tahun 2011 (indeks KAMI versi 2,0), untuk versi 2,1, versi 2,2 dan versi 2,3 di refisi kesalahan definisi rumusan penentuan tingkat kematangan yang berakhir di tanggal 19 April tahun 2012 untuk rumusan bernar capaian tingkat keamanan IV, pada tahun 2015 disesuaikan dengan ISO/IEC 27001:2013 dan menjadi versi 3,0 ditahun yang sama versi 3,1 dikeluarkan dengan pemisahan dua katagori, kemudian ditahun 2019 dikeluarkan oleh BSSN dengan Indeks Kami versi 4,0 dengan perbedaan bagian suplemen **[35]**.

Sekolah Tinggi Manajemen Informatika dan Komputer Mardira Indonesia (STMIK-MI) adalah sekolah tinggi swasta yang sedang berkembang, dimana STMIK-MI memiliki program studi teknik informatika yang berkaitan erat dengan TI, didalam lingkungan STMIK-MI sudah menggunakan pemanfaatan layanan TI dalam proses bisnisnya, penerapan penggunaan TI di STMIK-MI dijalankan dan dikendalikan oleh bagian Pusat Komputer dan Teknologi (PUSKOMTEK), salah satu tugas PUSKOMTEK adalah mengawasi, memelihara, memperbaiki dan mengembangkan sarana TI di STMIK-MI untuk keberlangsungan proses bisnis sekolah tinggi.

Keamanan informasi menjadi hal penting terutama bagi organisasi yang menggunakan layanan TI sebagai pendukung utama proses bisnisnya. Berdasarkan **[2]** menerangkan bahwa perlu adanya keamanan informasi untuk menjaga aset perusahaan seperti aset *software*, *database* dan *file server*, *mediastore*, *server* dan *workstation*, *network hardware*, *communication network*, *auxiliary equipment* dan aset personal. Keamanan informasi yang menjamin kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) aset-aset informasi yang ada.

Aset TI dilingkungan institusi STMIK-MI merupakan salah satu tanggung jawab PUSKOMTEK dimana aset-aset ini lah yang akan menjamin keberlangsungan layanan TI di STMIK-MI, diantara nya adalah perangkat komputer disetiap bagian, laboratorium komputer sarana pembelajaran, CCTV, Akses Point, Server data Sistem Informasi Manajemen Akademik dan Kemahasiswaan (SIMAK), jaringan intranet dan internet. Aset TI tersebut adalah yang menjadi sarana layanan TI bagi STMIK-MI dan semua itu berada dalam tanggung jawab PUSKOMTEK.

Selama ini PUSKOMTEK belum pernah melakukan analisa penyebab terjadinya permasalahan – permasalahan yang muncul terkait dengan gangguan teknologi informasi dan PUSKOMTEK tidak mengetahui sampai di mana tingkat keamanan teknologi informasi terhadap aset-aset yang dimilikinya. Oleh karena itu PUSKOMTEK membutuhkan kontrol keamanan teknologi informasi untuk menjaga keamanan aset-aset nya. Sedangkan analisa keamanan teknologi informasi dapat dilakukan dengan pemeriksaan keamanan sistem informasi dan Keamanan informasi ditujukan untuk menjaga aspek kerahasiaan (*Confidentiality*), keutuhan (*Integrity*) dan ketersediaan (*Availability*) dari Informasi (ISO/IEC 27001, 2013).

KAJIAN PUSTAKA

Tata kelola TI adalah struktur kebijakan atau prosedur dan kumpulan proses yang bertujuan untuk memastikan kesesuaian penerapan TI dengan dukungannya terhadap pencapaian tujuan institusi, dengan cara mengoptimalkan keuntungan dan kesempatan yang ditawarkan TI, mengendalikan penggunaan terhadap sumber daya TI dan mengelola resiko-resiko terkait TI.

Tatakelola teknologi informasi bukan bidang yang terpisah dari pengelolaan perusahan, melainkan merupakan komponen pengelolaan perusahaan secara keseluruhan, dengan tanggung jawab utama sebagai berikut:

1. Memastikan kepentingan stakeholder diikutsertakan dalam penyusunan strategi perusahaan.
2. Memberikan arahan kepada proses-proses yang menerapkan strategi perusahaan.
3. Memastikan proses-proses tersebut menghasilkan keluaran yang terukur.
4. Memastikan adanya informasi mengenai hasil yang diperoleh dan mengukurnya.
5. Memastikan keluaran yang dihasilkan sesuai dengan yang diharapkan

Di lingkungan yang sudah memanfaatkan Teknologi Informasi, tata kelola TI menjadi hal penting yang harus diperhatikan. Hal ini dikarenakan ekspektasi dan realitas seringkali tidak sesuai. Pihak shareholder perusahaan selalu berharap agar perusahaan dapat :

1. Memberikan solusi TI dengan kualitas yang bagus, tepat waktu, dan sesuai dengan anggaran.
2. Menguasai dan menggunakan TI untuk mendatangkan keuntungan.
3. Menerapkan TI untuk meningkatkan efisiensi dan produktifitas sambil menangani risiko TI.

Manfaat tata kelola TI adalah mengatur penggunaan TI, dan memastikan kinerja TI sesuai dengan tujuan/fokus utama area tata kelola TI.

Tata kelola Keamanan informasi adalah himpunan tanggung jawab dan prakter yang dilakukan oleh dewan dan manajemen eksekutif dengan tujuan memberikan arahan strategis, memastikan bahwa risiko dikelola secara tepat dan memverifikasi bahwa sumber daya perusahaan itu digunakan secara bertanggung jawab. Tujuan utama pelaksanaan tata kelola keamanan informasi adalah untuk melindungi asset yang paling berharga dari sebuah organisasi. Identifikasi asset informasi merupakan faktor penentu keberhasilan untuk implementasi yang efisien dan keamanan informasi diperusahaan (Insitute Governance IT, 2001: Deloitte Touche Tohmatsu) **[24]**. Menurut Kementerian Komunikasi dan Informatika Keamanan Informasi bagi penyelenggara Pelayanan Publik **[25]**,

International Standards Organization (iso) adalah badan penetap standar internasional yang terdiri dari wakil-wakil dari badan standarisasi nasional setiap negara. Didirikan pada 23 Februari 1947, ISO menetapkan standar-standar industrial dan komersial dunia. ISO merupakan lembaga nirlaba internasional, pada awalnya dibentuk untuk membuat dan memperkenalkan standardisasi internasional untuk apa saja. Standar yang sudah kita kenal antara lain standar jenis film fotografi, ukuran kartu telepon, kartu ATM Bank, ukuran dan ketebalan kertas dan lainnya.

Dalam menetapkan suatu standar tersebut mereka mengundang wakil anggotanya dari 130 negara untuk duduk dalam Komite Teknis (TC), Sub Komite (SC) dan Kelompok Kerja (WG). Peserta ISO termasuk satu badan standar nasional dari setiap negara dan perusahaan-perusahaan besar. ISO bekerja sama dengan Komisi Elektroteknik Internasional (IEC) yang bertanggung jawab terhadap standardisasi peralatan elektronik.

Sejak tahun 2005, International Organization for Standardization (ISO) atau Organisasi Internasional untuk Standarisasi telah mengembangkan sejumlah standar tentang *Information Security Management Systems* (ISMS) atau Sistem Manajemen Keamanan Informasi (SMKI) baik dalam bentuk persyaratan maupun panduan.

ISO 27000 diterbitkan pda tahun 2009 untuk memberikan gambaran tentang standar ISO 27000 serta dasar konseptual secara umum. Terdapat 46 keamanan informasi dasar yang didefinisikan dalam dalam "*Term and Condition*" ISO 27000. Keamanan informasi didasarkan dari perusahaan yang bisnis prosesnya tergantung dengan infrastruktur IT yang rentan terhadap kegagalan dan gangguan. Sama halnya dengan standar teknologi informasi yang lain, ISO 27000 merujuk pada siklus PDCA (*Plan – Do – Check – Action*), siklus yang terkenal dari manajemen mutu **[27]**.

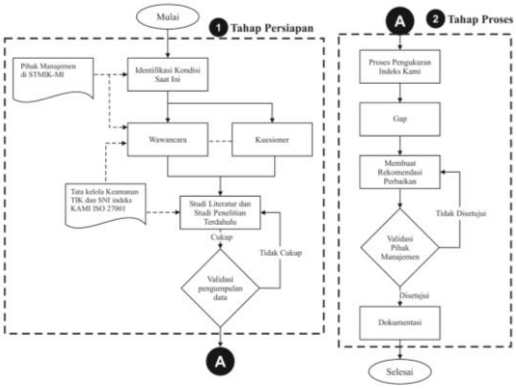
ISO/IEC 27002 adalah seperangkat standar dan prosedur yang berkaitan dengan keamanan dan kontrol informasi yang memungkinkan bisnis untuk menerapkan keamanan yang tepat **[26][27]**. Standar ini sebagian besar dilengkapi dengan ISO/IEC 27001 yang merinci tugas manajerial seperti penilaian risiko dan meninjau keamanan. Dilain pihak, ISO/IEC 27002 banyak berbicara tentang aspek Kontrol, Sementara itu, ISO/IEC 27001 merupakan standard internasional yang paling banyak digunakan

untuk *information security management*. Sampai dengan akhir 2009, lebih dari 12.000 organisasi di seluruh dunia telah memiliki sertifikasi ISO/IEC 27001. ISO/IEC 27001 digunakan untuk melindungi *confidentiality*, *integrity* dan *availability* dari informasi. ISO/IEC 27001 bukan merupakan *technical standard* yang menjelaskan ISMS ke dalam *technical detail*, dan tidak hanya fokus pada IT tetapi juga aset penting lainnya di dalam organisasi. ISO/IEC 27001 fokus pada *business process* dan *business asset*, pengurangan resiko 22 terhadap informasi yang bernilai tinggi bagi organisasi. Informasi tersebut dapat terkait ataupun tidak terkait dengan TI, dapat berbentuk ataupun tidak berbentuk format digital. Persyaratan yang harus diterapkan untuk dokumentasi ISMS, dijelaskan dalam standar melalui penetapan konten penting, dokumen yang diperlukan serta spesifikasi dan struktur pemantauan untuk manajemen dokumen.

Indeks keamanan informasi (Indeks KAMI). Indeks KAMI merupakan salah satu alat untuk mengevaluasi dan menganalisis tingkat kesiapan atau kematangan SMKI. Alat evaluasi ini disusun oleh Tim Direktorat Keamanan Informasi Kementrian Komunikasi dan Informatika. Indeks ini digunakan untuk memberikan gambaran kondisi kematangan dari kerangka kerja keamanan informasi. Indeks ini mengevaluasi semua area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang memenuhi aspek keamanan pada SNI ISO/IEC 27001:2013 dan pada tahun 2019 indeks KAMI versi 4.0 di terbitkan oleh Badan Siber dan Sandi Negara (BSSN)

METODOLOGI

Metodologi penelitian adalah sekumpulan peraturan, kegiatan dan prosedur yang digunakan oleh suatu disiplin ilmu. Metodologi juga merupakan analisis teoritis mengenai suatu cara atau metode. Pada bagian ini bertujuan untuk memaparkan konsep penelitian secara umum dan mengacu pada standar pengukuran indeks KAMI versi 4.0 dan SNI ISO/IEC 27001:2013. Data sekunder yang penulis gunakan dalam penelitian ini diperoleh melalui literatur atau studi pustaka seperti buku, jurnal, prosiding dan laman. Tahapan-tahapan pada penelitian ini dapat dilihat pada Gambar berikut dibawah ini:



Gambar I.1 Tahapan Penelitian

HASIL DAN PEMBAHASAN

Dalam pengukuran dengan indeks KAMI membutuhkan responder yang tepat dimana responden tersebut berada pada bagian manajemen atas, disini pengukuran yang dilakukan adalah di lemabaga pendidikan STMIK-MI yang telah menggunakan teknologi informasi sebagai layanan juga sarana proses bisnis. Adapun beberapa responden yang menjadi sumber dari pengukuran tata kelola teknologi informasi adalah :

Tabel I.1 Data Responden Indek KAMI

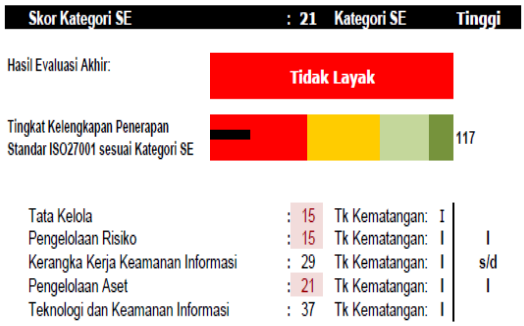
No	Jabatan
1	Ketua STMIK Mardira Indonesia
2	Wakil Ketua II
3	Kepala Bagian Umum dan Administrasi (BAU)
4	Kepala PUSKOMTEK
5	Staff PUSKOMTEK

Hasil pengukuran dengan menggunakan indeks KAMI adalah menunjukan bahwa skor katagori sistem elektronik yakni 21 yang artinya skor tersebut berada pada tingkatan tinggi dalam kata lain bahwa di STMIK-MI menggunakan sistem elektronik dengan ketergantungan yang cukup banyak, berikut cakupan skor dari katagori sektor elektronik di tabel I.2. :

Tabel I.2 Nilai Sektor Elektronik **[35]**

KATEGORI SISTEM ELEKTRONIK			
Rendah		Skor Akhir	
10	15	0	174
		175	312
		313	535
		536	645
Tinggi		Skor Akhir	
16	34	0	272
		273	455
		456	583
		584	645
Strategis		Skor Akhir	
35	50	0	333
		334	535
		536	609
		610	645

Sedangkan untuk bagian berikutnya yakni pada tata kelola keamanan TIK bernilai 15 dalam kecukupan untuk standar ISO masih bernilai kurang mencukupi karena nilai standar adalah 126 pada tahap tata kelola keamanan TIK. Untuk selanjutnya adalah pada bagian pengelolaan resiko didapat nilai 15 sedangkan nilai standar ISO adalah 72 untuk maksimum skor pengelolaan resiko, bagian kerangka kerja keamanan informasi didapat 29 sedangkan minimum skor nya 159 dibagian pengelolaan aset didapat 21 sedangkan untuk skor maksimumnya 159 selanjutnya pada bagian teknologi dan kemanan informasi didapat skor 37 dan skor minimum nya adalah 168 dan yang terakhir bagian suplemen bernilai 0 karena STMIK-MI tidak menggunakan jasa perusahaan lain pada sektor sistem elektronik-nya.
Dari penilaian dengan indeks kami menarik kesimpulan bahwa STMIK-MI masih belum layak tersertifikasi ISO sesuai dengan hasil evaluasi indesk KAMI, maka dari itu penulis merekomendasikan tata kelola keamanan teknologi informasi untuk tahapan awal menuju sertifikasi ISO. Berikut tabel – tabel dan diagram hasil evaluasi dengan indeks KAMI pada STMIK-MI dijelaskan sebagai berikut:



Gambar I.2 Tingkat Kelengkapan Penerapan Keamanan TI

Berikut hasil jawaban dari tebaran kuesioner dengan indeks KAMI perbagian:

Tabel I.3 Penilaian Bagian II Tata kelola

Status Penerapan	Tingkat Kematangan			
	II	III	IV	V
Tidak dilakukan	5	1	1	0
Dalam Perencanaan	8	2	4	0
Dalam penerapan/diterapkan sebagian	0	0	1	0
Diterapkan menyeluruh	0	0	0	0

Tabel I.4 Penilaian Bagian III Pengelolaan Risiko

Status Penerapan	Tingkat Kematangan			
	II	III	IV	V
Tidak dilakukan	1	1	0	0
Dalam Perencanaan	9	1	2	2
Dalam penerapan/diterapkan sebagian	0	0	0	0
Diterapkan menyeluruh	0	0	0	0

Tabel I.5 Penilaian Bagian IV Kerangka kerja Keamanan TI

Status Penerapan	Tingkat Kematangan			
	II	III	IV	V
Tidak dilakukan	2	1	0	1
Dalam Perencanaan	9	12	1	3
Dalam penerapan/diterapkan sebagian	0	0	0	0
Diterapkan menyeluruh	0	0	0	0

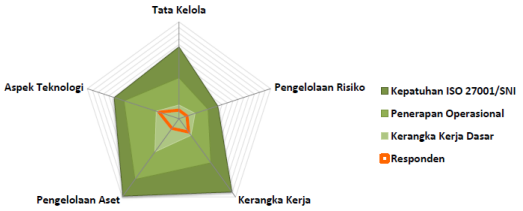
Tabel I.6 Penilaian Bagian V Pengelolaan Aset

Status Penerapan	Tingkat Kematangan			
	II	III	IV	V
Tidak dilakukan	12	8	0	0
Dalam Perencanaan	17	1	0	0
Dalam penerapan/diterapkan sebagian	0	0	0	0
Diterapkan menyeluruh	0	0	0	0

Tabel 4.7 Penilaian Bagian VI Teknologi dan keamanan TI

Status Penerapan	Tingkat Kematangan			
	II	III	IV	V
Tidak dilakukan	0	0	0	0
Dalam Perencanaan	14	11	1	0
Dalam penerapan/diterapkan sebagian	0	0	0	0
Diterapkan menyeluruh	0	0	0	0

Dari hasil evaluasi dari indeks KAMI maka dapat digambarkan di tingkat kelengkapan penerapan keamanan TIK dengan gambar diagram radar seperti berikut:



Gambar I.3 Diagram Radar Tingkat Kelengkapan Penerapan Keamanan TI

Berdasarkan hasil penilaian dari indeks kami maka terdapat selisih atau gap untuk dapat mencapai kesiapan tatakelola keamanan TI di STMIK-MI, selisih atau gap yang didapat dapat dilihat dari tabel selisih penilaian kesiapan tata kelola sesuai dengan indeks KAMI versi 4.0 tahun 2019.

Tabel I.8 Selisih atau Gap Bagian II: Tata Kelola Keamanan Informasi

Keterangan	Skor	Gap
Jumlah pertanyaan Tahap 1	8	48-15 = 33
Jumlah pertanyaan Tahap 2	8	
Jumlah pertanyaan Tahap 3	6	
Batas Skor Min untuk Skor Tahap Penerapan 3	48	
Total Skor Tahap Penerapan 1 & 2	15	
Status Peniliaian Tahap Penerapan 3	Tidak Valid	

Tabel I.9 Selisih atau Gap Bagian III: Pengelolaan Risiko Keamanan Informasi

Keterangan	Skor	Gap
Jumlah pertanyaan Tahap 1	10	36-15 = 21
Jumlah pertanyaan Tahap 2	4	
Jumlah pertanyaan Tahap 3	2	
Batas Skor Min untuk Skor Tahap Penerapan 3	36	
Total Skor Tahap Penerapan 1 & 2	15	
Status Peniliaian Tahap Penerapan 3	Tidak Valid	

Tabel I.10 Selisih atau Gap Bagian IV: Kerangka Kerja Pengelolaan Keamanan Informasi

Keterangan	Skor	Gap
Jumlah pertanyaan Tahap 1	12	64 – 29 = 35
Jumlah pertanyaan Tahap 2	10	
Jumlah pertanyaan Tahap 3	7	
Batas Skor Min untuk Skor Tahap Penerapan 3	64	
Total Skor Tahap Penerapan 1 & 2	29	
Status Peniliaian Tahap Penerapan 3	Tidak Valid	

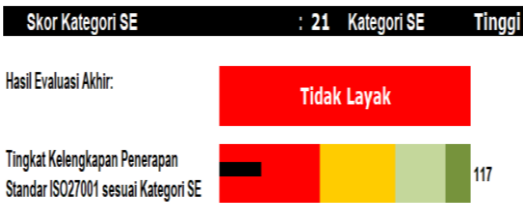
Tabel I.11 Selisih atau Gap Bagian V: Pengelolaan Aset Informasi

Keterangan	Skor	Gap
Jumlah pertanyaan Tahap 1	24	88 – 21 = 67
Jumlah pertanyaan Tahap 2	10	
Jumlah pertanyaan Tahap 3	4	
Batas Skor Min untuk Skor Tahap Penerapan 3	88	
Total Skor Tahap Penerapan 1 & 2	21	
Status Peniliaian Tahap Penerapan 3	Tidak Valid	

Tabel I.12 Selisih atau Gap Bagian VI: Teknologi dan Keamanan Informasi

Keterangan	Skor	Gap
Jumlah pertanyaan Tahap 1	14	68 – 34 = 34
Jumlah pertanyaan Tahap 2	10	
Jumlah pertanyaan Tahap 3	2	
Batas Skor Min untuk Skor Tahap Penerapan 3	68	
Total Skor Tahap Penerapan 1 & 2	34	
Status Peniliaian Tahap Penerapan 3	Tidak Valid	

Dari selisih yang didapat dengan bagian II sampai dengan VI terlihat jelas selisih yang didapat cukup banyak dan tidak ada satupun bagian yang masuk ke katagori Valid, dikarenakan sektor elektronik bernilai tinggi maka nilai skor akhir agar dapat tercukupi untuk terstandarisasi SNI ISO/IEC 27001 adalah 273 dan status kesiapan berada pada status pemenuhan kerangka kerja dasar. Sedangkan skor akhir pada evaluasi indeks KAMI di STMIK-MI adalah bernilai 117, Penilaian kesiapan untuk standar SNI ISO/IEC 27001 dapat dilihat digambar berikut :



Gambar 4.4 Skor Akhir Hasil Evaluasi di STMIK-MI

Dari hasil evaluasi indeks KAMI terdapat nilai – nilai yang belum mencukupi untuk tersertifikasi SNI ISO/IEC 27001 maka penulis mengambil rekomendasi untuk STMIK-MI harus membuat dokumen tata kelola keamanan TIK dengan *Control Objective* SNI ISO/IEC 27002 yang merupakan sebuah dokumen tata kelola keamanan TIK.

Dari hasil selisih skor yang didapat dari evaluasi indeks KAMI penulis menjelaskan dan merekomendasikan kedalam *control objective* ISO, yang nantinya akan dibuat dokumen tata kelola keamanan guna meningkatkan keamanan teknologi informasi di STMIK-MI, dokumen tata kelola keamanan ini bisa menjadi acuan bagi STMIK-MI guna pengembangan keamanan TI di lingkungan STMIK-MI, berikut penjelasan rekomendasi yang penulis sajikan dalam bentuk tabel-tabel dibawah ini:

Tabel I.13 Rekomendasi Bagian II Tata Kelola Keamanan TI

NO	Kondisi Saat ini	Rekomendasi	Annex A reference
1	Ketua dan wakil ketua 2 tidak bertanggungjawab terhadap pelaksanaan keamanan TI dan Penetapan Kebijakan keamanan TI yang secara prinsip dan resmi	Dari hasil tebaran indeks KAMI ke tujuh pertanyaan ini berada dalam jawaban tidak diterapkan dalam artian belum adanya ketentuan ataupun penjelasan secara khusus dari pihak STMIK-MI maka dari itu direkomendasikan di dalam SNI ISO/IEC 27001 dengan Annex A.5.1.1 yakni terkait dengan kebijakan Keamanan TI dan Annex A.6.1.1 tentang Organisasi Keamanan TI	*A.5.1.1 Information security policy document*
2	Belum terdefinisinya standar kompetensi dan keahlian terkait pelaksana keamanan TI		
3	Belum menerapkan program sosialisasi dan peningkatan pemahaman pada keamanan TI dan kepatuhannya bagi semua pihak terkait		
4	Belum menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan TI		
5	Belum mengidentifikasikan data pribadi yang digunakan dalam proses kerja		*A.6.1.1 Information security roles and responsibilities*
6	Belum mealokasikan dan mendefinisikan tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*)		
7	Belum mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya		

Tabel I.14 Rekomendasi Bagian III Pengelolaan Risiko Keamanan TI

NO	Kondisi Saat ini	Rekomendasi	Annex A reference
1	Belum mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi	Dari hasil evaluasi indeks KAMI dibagian ke 3 tentang pengelolaan risiko, secara keseluruhan telah direncanakan, namun ada dua pernyataan yang belum direncanakan oleh STMIK-MI yank ni belum adanya program kerja risiko keamanan secara terdokumentasi dan belum dilakukan secara berkala maka direkomendasikan dengan Annex 16.1.3 yakni pelaporan kelemahan keamanan TI	*Annex 16.1.3 Reporting information security weaknesses*
2	Tidak ada pengawasan terhadap penyelesaiah langkah mitigasi risiko secara berkala guna memastikan kemajuan kerja		

Tabel I.15 Rekomendasi Bagian IV Kerangka Kerja Pengelolaan Keamanan TI

NO	Kondisi Saat ini	Rekomendasi	Annex A reference
1	Belum memiliki strategi penerapan keamanan TI yang dilakukan sebagai bagian dari rencana kerja organisasi	Dari Hasil evaluasi indeks KAMI beberapa sudah direncanakan namun ada empat pernyataan yang belum terencanakan untuk rekomendasi kontrol keamanan yang direkomendasikan yakni Annex A.5.1.1,	*A.5.1.1 Information security policy document*
2	Tidak mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko		*A.6.1.1 Information security roles and responsibilities*
3	Belum merealisasikan penerapan keamanan TI sebagai pelaksanaan program kerja organisasi		*A.5.1.2 Review of the policies for information security*
4	Belum adanya evaluasi secara periodik mengenai tingkat kepatuhan keamanan TI		

Tabel I.16 Rekomendasi Bagian V Pengelolaan Aset Informasi

NO	Kondisi Saat ini	Rekomendasi	Annex A reference
1	Tidak memiliki dan menerapkan kontrol keamanan sebagai tindak lanjut dari proses penerapan mitigasi risiko dan didalam pertanyaan evaluasi bagian ini dinyatakan tidak dilakukan semua	Dari hasil evaluasi dengan indeks KAMI menyatakan bahwa STMIK-MI secara garis besar belum memiliki kontrol keamanan yang berguna untuk mitigasi risiko dengan pernyataan itu direkomendasikan ke dalam Annex A.16.1 tentang manajemen keamanan insiden keamanan TI	*Annex A.16.1 Reporting information security events and weaknesses*

Tabel I.17 Rekomendasi Bagian VI Suplemen

NO	Kondisi Saat ini	Rekomendasi	Annex A reference
1	Pada saat evaluasi bagian suplemen ini tidak di isi sama sekali dikarenakan STMIK-MI memang belum menggunakan jasa eksternal untuk katagori sistem elektronik	Dikarenakan STMIK-MI belum menggunakan jasa eksternal pada sistem elekronik nya, maka untuk rekomendasi awal adalah hanya tentang penjelasan Suplemen itu sendiri dan rekomendasi pada Annex A.15.1.1 bertujuan untuk informasi tentang suplemen apabila nanti akan dilakukan	*Annex A.15.1.1 Information security policy for supplier relationships*

KESIMPULAN

Sektor elektronik di STMIK-MI yang di evaluasi dengan Indeks KAMI memiliki nilai akhir 21 dalam artian menurut Indeks KAMI skor ini masuk pada nilai tinggi sedangkan rentang nilai rendah dari 10 sampai 15, tinggi dari 16 sampai 34 dan strategis dari 35 sampai 50. Dengan demikian kriteria kesiapan dan kematangan tata kelola keamanan teknologi informasi sesuai Indeks KAMI minimal harus bernilai 273 untuk kondisi awal penerapan tata kelola keamanan teknologi informasi karena untuk rentang nilai tidak layak 0 sampai 272, pemenuhan kerangka kerja 273 sampai 455, cukup baik 456 sampai 583 dan baik 584 sampai 645 dan di STMIK-MI bernilai 117 atau berstatus tidak layak.

Pada penilaian kesiapan dan kematangan keamanan teknologi informasi di STMIK-MI, ada beberpa bagian penilaian dan didapat hasil masing – masing nilai yakni bagian II tata kelola 15, bagian III pengelolaan risiko 15, bagian IV kerangka kerja keamanan informasi 29, bagian V Pengelolaan aset 21, bagian VI teknologi dan keamanan informasi 37 dan bagian VII suplemen 0. Keseluruhan rata – rata berada pada tingkat I (satu) kebawah dalam arti belum layak SNI ISO/IEC 27001 menurut penilaian Indeks KAMI.

Terlihat dari hasil evaluasi dengan Indeks KAMI yang diadopsi dari SNI ISO/IEC 27001 bahwa nilai bagian II dan III yakni bagian tata kelola dan pengelolaan risiko berada pada nilai paling bawah, maka tata kelola keamanan teknologi informasi harus dilakukan.

Pembuatan dokumen keamanan TI yang sesuai dengan beberapa kekurangan dari hasil evaluasi dengan Indeks KAMI yang berstatus belum ada atau belum diterapkan, maka dokumen keamanan TI merujuk ke *control objective* yang sesuai dengan beberapa status yang tidak diterapkan berubah menjadi dalam perencanaan, sehingga nilai skor akhir bisa bertambah menjadi status kesiapannya perlu perbaikan atau sudah mempunyai kerangka dasar bahkan bisa berstatus baik sesuai dengan SNI ISO/IEC 27001 dan SNI ISO/IEC 27002.

REFERENSI

[1] Rahardjo, Budi. 2005. Keamanan Sistem Informasi Berbasis Internet. Bandung: PT. Insan Indonesia.

[2] R. S. Rozas and R. Sarrno, “SiPKoKI ISO 27001: Sistem Pemilihan Kontrol Keamanan Informasi Berbasis ISO 27001”, in *Seminar Nasional Pascasarjana XI*, Surabaya, 2011.

[3] Rosmiati, dkk, 2016. *"A Maturity Level Framework for Measurement of Information Security Performance"* in *International Journal of Computer Applications Volume 141 – No.8, May 2016. Yogyakarta.*

[4] Suprianto Aji, 2007. "Prinsip dan Siklus Hidup Keamanan Informasi" Jurnal Teknologi Informasi DINAMIK Volume XII, No.2, Juli. Universitas Stikubank Semarang.

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

[6] Wibowo Aldi Satriani, dkk. 2016."KOMBINASI FRAMEWORK COBIT 5, ITIL DAN ISO/IEC 27002 UNTUK MEMBANGUN MODEL TATA KELOLA TEKNOLOGI INFORMASI DI PERGURUAN TINGGI". Seminar Nasional Teknologi Informasi dan Komunikasi. UGM. Yogyakarta.

[7] Agustino Dedy Panji. 2017."Analisa Manajemen Keamanan Informasi Pada Infrastruktur TI di STMIK STIKOM Bali". Konferensi Nasional Sistem & Informatika. STMIK STIKOM. Bali.

[8] Febrianto Ferry, Dana Indra Sensuse. 2017. "EVALUASI KEAMANAN INFORMASI MENGGUNAKAN ISO/IEC 27002: STUDI KASUS PADA STIMIK TUNAS BANGSA BANJARNEGARA". Jurnal Ilmiah Informasi Komputer, Akuntansi dan Manajemen Nomor II th.2017. Universitas AMIKOM. Yogyakarta.

[9] Endang Kurniawan, dan Imam Riadi. 2018."ANALISIS TINGKAT KEAMANAN SISTEM INFORMASI AKADEMIK BERDASARKAN STANDAR ISO 27002: 2013 MENGGUNAKAN SSE-CMM". Penelitian untuk mengetahui tingkat keaman informasi dalam sistem informasi akademik. UII. Yogyakarta.

[10] Fauzi, Rokhman. 2018."IMPLEMENTASI AWAL SISTEM MANAJEMEN KEAMANAN INFORMASI pada UKM MENGGUNAKAN KONTROL ISO/IEC 27002". Jurnal Teknologi Rekayasa. Universitas Telkom. Bandung.

[11] Indra, Dheni, dkk. 2017."Pembuatan Dokumen Sop Keamanan Aset Informasi Yang Mengacu Pada Kontrol Kerangka Kerja ISO 27002: 2013 (Studi Kasus : CV Cempaka Tulungagung)". JURNAL TEKNIK ITS. Kampus ITS Sukolilo. Surabaya.

[12] Rutanaji, Dicky, dkk. 2017."ISO 27001 Sebagai Metode Alternatif Bagi Perancangan Tata Kelola Keamanan Informasi". Prosiding Seminar Nasional XII Rekayasa Teknologi Industri dan Informasi. UGM. Yogyakarta.

[13] Putra Anggi Anugraha, dkk. 2016.″Perencanaan dan Implementasi *Information Security Management System* Menggunakan Framework ISO/IEC 20071″. Diponegoro. Semarang.

[14] Putra Mardi Yudhi, dan Tjahjadi, Djajasukma. 2018. "Evaluasi Keamanan Informasi Pada Perguruan Tinggi Bina Insansi Berdasarkan Indeks Keamanan Informasi SNI ISO/IEC 27001". Jurnal Penelitian Ilmu Komputer, System Embedded dan Logic. STMIK Bina Insani. Bekasi.

[15] R Lailatul Fitriana, dkk. 2014. "Pembuatan Panduan Tata Kelola Pada Bidang Keamanan Informasi dan Pemulihan Bencana Berbasis COBIT 4.1 dan ISO 27002". Seminar Nasional Sistem Informasi Indonesia. ITS. Surabaya.

[16] Nugroho Budi, dan Junaedi Lukman. "Pengembangan Tata Kelola Personil TI Menggunakan COBIT 4.1 dan ISO/IEC 27002". Tata Kelola TI. UPN. Jawa Timur.

[17] Basir Azhar, dkk. 2019. "*Enterprise Architecture Planning* Sistem Informasi Akademik Dengan TOGAF ADM". Jurnal Sains Komputer dan Informatika. Universitas Ahmad Dahlan. Yogyakarta.

[18] Yunis Roni, dan Surendro Kridanto. 2010. "Implementasi *Enterprise Architecture* Perguruan Tinggi". Seminar Nasional Aplikasi Teknologi Informasi

[19] Purnomo Lukman Hadi Dwi, dan Tjahyanto Aris. 2010. "Perancangan Model Tata Kelola Ketersediaan Layanan TI Menggunakan Framework COBIT pada BPK-RI". Seminar Nasional Informatika 2010. UPN. Yogyakarta

[20] Dewi Indah Kusuma, dkk. 2015. "Usulan Manajemen Risiko Berdasarkan Standar SNI ISO/IEC 27001:2009". Studi Informatika. UIN. Jakarta

[21] Sihotang Hengki Tamando, dan Sagala Jijon Raphita. 2015. "Penerapan Tata Kelola Teknologi Informasi dan Komunikasi Pada Domain *ALIGN, PLAN*

and ORGANISE (APO) dan MONITOR, EVALUATE and ASSESS (MEA) dengan Menggunakan Framework COBIT 5". Jurnal Manajemen dan Informatika Komputer Pelita. STMIK Pelita Nusantara Medan. Sumatera Utara.

[22] Wella, dan Tampi Anathasia. 2017. "Tingkat Kapabilitas Tata Kelola TI Pusat Teknologi Informasi dan Komunikasi". Melakukan Pengukuran Tingkat Kapabilitas tata kelola TI di PTI Universitas Sam Ratulangi. UMN. Tangerang.

[23] Pratiwi Wilda Ayu. 2019. "Perancangan Sistem Manajemen Keamanan Informasi Bedasarkan Standar ISO 27001:2013 Pada KOMINFO Provinsi Jawa Timur". Fakultas Teknologi dan Informatika. STMIK Surabaya. Surabaya.

[24] Rastogi, R & Von Solms, R. 2006. *Information Security Governance a Re-definition*. IFIP International Federatiian for Information Processing, Volume 193/2006, Springer Boston. 9

[25] Tim Direktorat Kemanan Informasi. 2011. Tata Kelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik. Direktorat Keamanan Infromasi. Direktorat Jendral Aplikasi Informatika Kementerian Komunikasi dan Informatika Republik Indonesia.

[26] www.isoindonesiacenter.com

[27] ISO/IEC. 2005. *"Information Technology-Security Techniques-Code of Practice for Information Security Management ISO/IEC 17799 (27002):2005"*. Switzerland. Diakses dari www.iso27001security.com [Juni 2019]

[28] Musda, 2017. *An Introductory Overview Of ITIL V3* (Terjemahan ITIL V3).

[29] Richardus Eko Indrajit, "Kebijakan Keamanan Informasi". Diakses dari https://www.academia.edu/14326531/Kebijakan_Keamanan_Informasi [Juni 2019]

[30] QAPI. 2006. *"Guidance for Performing Failure Mode and Effects Analysis with Performance Improvement Projects"*. cms.gov. diakses dari https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/QAPI/downloads/GuidanceForFMEA.pdf [Agustus 2019]

[31] Lipol, L. S., Haq, J., 2011. *"Risk Analysis Method: FMEA/FMECA in the Organizations"*. International Journal of Basic & Applied Sciences. Diakses dari https://www.sciencedirect.com/science/article/pii/S2212567115012745 [Oktober 2019]

[32] Manajemen Risiko diakses dari https://www.iso.org [Agustus 2019]

[33] Sukmadinata, S. N. 2005. "Metode Penelitian". PT Remaja Rosdakarya. Bandung. Diakses dari http://a-research.upi.edu/operator/upload/t_pd_0908073_chapter3.pdf [Oktober 2019]

[34] Buku Profil Akademik. 2013. "Profil STMIK Mardira Indonesia". Bandung STMIK Mardira Indonesia.

[35] Badan Siber dan Sandi Negara Republik Indonesia. Diakses dari https://bssn.go.id/indeks-kami/ [Agustus 2019]

[36] PERATURAN MENTERI KOMUNIKASI DAN INFORMATIKA. 2007. "Panduan Umum Tata Kelola Teknologi Informasi dan Komunikasi Nasional". Jakarta. MENTERI KOMUNIKASI DAN INFORMATIKA diakses dari https://jdih.kominfo.go.id/produk_hukum/unduh/id/450/t/peraturan+menteri+komunikasi+dan+informatika+nomor+41permkominfo112007+tanggal+19+november+2007 [November 2019]

[37] Menteri Komunikasi dan Informatika. 2016. Peraturan Menteri Komunikasi dan Informatika Tentang Sistem Pengamanan Informasi. Jakarta diakses dari https://jdih.kominfo.go.id/produk_hukum/unduh/id/532/t/peraturan+menteri+komunikasi+dan+informatika+nomor+4+tahun+2016+tanggal+11+april+2016 [November 2019]

[38] SNI ISO 27001:2009 Teknologi informasi - Teknik keamanan – Sistem Diakses dari http://sispk.bsn.go.id/SNI/DaftarList# [November 2019]

[39] SNI ISO/IEC 27002:2014/Corr. 1:2016 Teknologi informasi Teknik keamanan Petunjuk praktik kendali keamanan informasi (RALAT 1) (ISO/IEC 27002:2013/Cor 1:2014, IDT) Diakses dari http://sispk.bsn.go.id/SNI/DaftarList# [November 2019]