ANALISIS TINGKAT KESIAPAN DAN KEMATANGAN IMPLEMENTASI ISO 27001:2013

by Wiyli Yustanti

Submission date: 02-Apr-2023 09:26AM (UTC+0700)
Submission ID: 2053151221
File name: 201-Article_Text-346-1-10-20181228.pdf (223.14K)
Word count: 3631
Character count: 23888

ANALISIS TINGKAT KESIAPAN DAN KEMATANGAN IMPLEMENTASI ISO 27001:2013 MENGGUNAKAN INDEKS KEAMANAN INFORMASI 3:2015 PADA UPT. PPTI UNIVERSITAS NEGERI SURABAYA

WIYLI YUSTANTI
Prodi Sistem Informasi, Jurusan Teknik Informatika, Universitas Negeri Surabaya, wiyliyustanti@unesa.ac.id

RAHADIAN BISMA
Prodi Sistem Informasi, Jurusan Teknik Informatika, Universitas Negeri Surabaya, rahadianbisma@unesa.ac.id

ANITA QOIRIAH
Prodi Teknik Informatika, Jurusan Teknik Informatika, Universitas Negeri Surabaya, anitaqoiriah@unesa.ac.id

AGUS PRIHANTO
Prodi Teknik Informatika, Jurusan Teknik Informatika, Universitas Negeri Surabaya, Jl. Ketintang, Surabaya, 602[illegible]donesia
agusprihanto@unesa.ac.id

Abstrak - Perguruan tinggi n[illegible] sebagai lembaga pemerintah harus menerapkan standar manajemen keamanan informasi sesuai dengan peraturan kementrian komunikasi dan informatika nomor 4 tahun 2016. Tujuan adanya pemenuhan terhadap standar ini adalah untuk memastikan bahwa tingkat keamanan informasi yang diterapkan telah memenuhi standar ISO 27001: 2013, dimana penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK) saat ini sebagian besar sudah menjadi kebutuhan dan tuntutan untuk setiap organisasi penyelenggara pelayanan publik. Dari hasil analisa data yang dikumpulkan didapatkan bahwa sistem elektronik yang digunakan dalam kegiatan operasiona di Universitas Negeri Surabaya sudah termasuk dalam kategori strategis, artinya bahwa sebagian besar kegiatan layanan operasional akademik maupun non akademik bertumpu pada sistem elektronik. Berdasarkan ukuran dalam indeks KAMI disimpulkan bahwa area pengelolaan resiko, kerangka kerja keamanan dan pengelolaan asset keamanan informasi masih rendah yaitu pada level I-II yang berarti masih perlu perbaikan untuk menuju kesiapan implementasi ISO 27001:2013.

Kata Kunci: Indeks KAMI; ISO 27001; keamanan Informasi; perguruan tinggi

Abstract - State universities as government institutions must implement the [illegible]mation security management standards in accordance with the regulation number 4/2016 of the Ministry of Communication and Informatics Republic of Indonesia. The purpose of fulfilling this standard is to

ensure that level of information security applied has met ISO 27001: 2013 standards, where the application of the management of Information and Communication Technology (ICT) today has largely become a need and demand for every public service provider organization. The analysis of the collected data found that the electronic system used in operational activities at the State Surabaya University was included in the strategic category, meaning that most the academic and non-academic operational vice activities were based on electronic systems. Based on the measurement of KAMI index, it is concluded that the area of risk management, information security ework and management of information security assets is still low, namely at level I-II which means that there is still a need to improve to get ready for implementation of ISO 27001: 2013.

Keywords: KAMI Index; ISO 27001; information security; higher education

1. Pendahuluan

Kementerian Komunikasi dan Informatika Republik Indonesia telah mengeluarkan peraturan nomor 4 Tahun 2016 tentang Sistem Manajemen Keamanan Informasi (SMKI) untuk semua organisasi pemerintahan. Perguruan tinggi negeri sebagai lembaga pemerintah harus menerapkan standar ini untuk memastikan tingkat keamanan informasinya telah memenuhi standar ISO 27001: 2013, dimana penerapan tata kelola Teknologi Informasi dan Komunikasi (TIK) saat ini sebagian besar sudah menjadi kebutuhan dan tuntutan untuk setiap organisasi penyelenggara pelayanan publik. Unit Pelaksana Teknis Pusat Pengembangan Teknologi Informasi (UPT. PPTI) Universitas Negeri Surabaya sebagai unit kerja yang bertanggung jawab terhadap keamanan informasi di Universitas memiliki tuntutan untuk segera mengimplementasikan standart ISO 27001:2013. Dalam pengukuran kesiapan implementasi manajemen sistem keamanan informasi tersebut, pemerintah telah menyiapkan perangkat yang disebut sebagai Indeks Keamanan Informasi (KAMI) yang berisi pengukuran terhadap tingkat urgensitas peran TIK dalam upaya peningkatan kualitas layanan, yakni sebagai proses lisasi dari tata kelola yang baik. Dalam pengeyelenggaraan tata kelola, faktor keamanan informasi merupakan aspek yang sangat diperhatikan. Kinerja tata kelola akan terganggu apabila informasi yang merupakan salah satu obyek utama pada tata kelola TIK mengalami masalah keamanan informasi yang menyangkut kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*). Berbeda dengan indeks keamanan informasi (KAMI) yang digunakan pada tahun sebelumnya yaitu dengan menggunakan Indeks KAMI 1:2012, dimana tidak ada instrument yang mengukur tingkat kekiritisan layanan sistem elektronik yang digunakan dalam sebuah organisasi. Pada penelitian ini akan diukur tingkat kategori sistem elektronik yang digunakan di Universitas Negeri Surabaya serta lima area pengeloaan keamanan informasi dalam hal tata kelola keamanan informasi, pengelolaan resiko keamanan informasi, kerangka kerja pengelolaan keamanan informasi, pengelolaan asset informasi serta penggunaan teknologi dalam keamanan informasi dalam hal mengukur kesiapan UPT. PPTI dalam menerapkan ISO 27001:2013 yang merupakan standart internasional yang mengatur tentang manajemen keamanan informasi.

Dengan demikian, fokus permasalahan yang diambil dalam penelitian ini adalah terkait dengan bagaimana tingkat kematangan dan kesiapan UPT. PPTI dalam hal

menerapkan ISO 27001:2013. Tujuannya adalah untuk mengetahui langkah-langkah apa yang harus dilakukan sehingga UPT. PPTI dapat memenuhi persyaratan yang dibutuhkan dalam standart manajemen keamanan informasi berbasis ISO 27001:2013.

2. ISO 27001 :13

ISO 27001 dirilis pada tahun 2013 berisi prinsip-prinsip dasar Sistem Manajemen Keamanan Informasi (SMKI) atau *Information Security Management Systems*. Pada standar ini termuat spesifikasi atau persyaratan yang harus dilaksanakan dalam membangun SMKI. Beberapa karkteristik standar ini ialah sifat independen terhadap produk TI (Teknologi Informasi), keharusan menggunakan pendekatan manajemen berbasis resiko, didesain untuk memastikan kontrol-kontrol keamanan yang dipilih mampu melindungi asset informasi dari berbagai resiko, dan memberi keyakinan tingkat keamanan bagi pihak-pihak yang berkepentingan.

Selain karakteristik-karakteristik yang telah disebutkan, standar ini juga memberikan pendekatan proses sebagai model bagi penetapan, penerapan, pengoperasian, pemantauan tinjau ulang (review), pemeliharaan dan peningkatan suatu SMKI. Pada akhirnya, proses tersebut mendorong pengguna untuk memprioritaskan:

a. Pemahaman persyaratan keamanan informasi organisasi dan kebutuhan terhadap kebijakan serta sasaran keamanan informasi.
b. Penerapan dan pengoperasian kontrol untuk mengelola risiko keamanan informasi dalam konteks risiko bisnis organisasi secara keseluruhan.
c. Pemantauan dan tinjau ulang kinerja dan efektivitas SMKI, dan
d. Peningkatan berkelanjutan berdasarkan pada pengukuran tingkat ketercapaian sasaran.

Standar ini mempunyai model *Plan-Do-Check-Act* (PDCA) sebagai garis besar pelaksanaan perancangan syarat untuk SMKI yang dapat dilihat pada tabel 1.

Table 1. Model Tahapan Pelaksanaan SMKI dengan PDCA

Tahapan	Kegiatan
PLAN (Menetapkan SMKI)	Menetapkan kebijakan SMKI, sasaran, proses dan prosedur yang relevan untuk mengelola risiko dan meningkatkan keamanan informasi agar memberikan hasil sesuai dengan keseluruhan kebijakan dan sasaran.
DO (Implementasi dan Operasi SMKI)	Menerapkan dan mengoperasikan kebijakan SMKI, kontrol, proses dan prosedur-prosedur.
CHECK (Mengawasi dan melakukan tinjau ulang terhadap SMKI)	Mengkaji dan mengukur kinerja proses terhadap kebijakan, sasaran, praktek-praktek dalam menjalankan SMKI dan melaporkan hasilnya kepada manajemen untuk ditinjau efektivitasnya.
ACT (Memelihara dan meningkatkan SMKI)	Melakukan tindakan perbaikan dan pencegahan, berdasarkan hasil evaluasi, audit internal dan tinjauan manajemen tentang SMKI atau kegiatan pemantauan lainnya untuk mencapai peningkatan yang berkelanjutan.

Standart ISO 27001:2013 mensyaratkan penetapan sasaran kontrol dan kontrol-kontrol keamanan informasi yang termasuk dalam 11 prinsip, yaitu :

a. Kebijakan keamanan informasi
b. Organisasi keamanan informasi
c. Manajemen asset
d. Sumber daya manusia menyangkut keamanan informasi
e. Keamanan fisik dan lingkungan
f. Komunikasi dan manajemen operasi
g. Akses kontrol
h. Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi
i. Pengelolaan insiden keamanan informasi
j. Manajemen kelangsungan usaha (*business continuity management*)

Prinsip diatas didalam tataran pedoman pelaksanaannya di Indonesia telah diatur secara singkat dalam instrument yang disediakan oleh Kementrian Komunikasi dan Informatika dalam indikator yang disusun melalui Indeks KAMI.

3. Indeks Keamanan Informasi (KAMI)

Indeks KAMI (Keamanan Informasi) merupakan alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi pada suatu organisasi yang disusun oleh Direktorat Keamanan Informasi Kementerian Kominfo. Alat evaluasi ini tidak digunakan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada. Alat evaluasi ini merupakan perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan instansi (Tim Direktorat Keamanan Informasi – Kementerian Kominfo, 2011). Evaluasi terhadap kematangan dan kelengkapan keamanan informasi yang telah disesuaikan dengan standar ISO/IEC 27001:2013 (Ridho dkk, 2012). Metode penilaian Indeks KAMI dikelompokan menjadi 5 area antara lain:

a. Tata Kelola Keamanan Informasi – Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta Instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.
b. Pengelolaan Risiko Keamanan Informasi – Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.
c. Kerangka Kerja Keamanan Informasi – Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.
d. Pengelolaan Aset Informasi – Bagian ini mengevaluasi kelengkapan pengamanan terhadap aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut; dan
e. Teknologi dan Keamanan Informasi – Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi.

Penyusunan komponen tersebut dilakukan untuk mendapatkan evaluasi mandiri yang mudah ditanggapi dimana hasil evaluasi akan digunakan sebagai panduan pembenahan atau peningkatan tata kelola keamanan informasi Proses penilaian Juga akan dilakukan dengan 2 metode:

a. Jumlah (kelengkapan) bentuk pengamanan
b. Tingkat kematangan proses pengelolaan pengamanan informasi.

Untuk menilai tingkat kematangan penerapan pengamanan dan kategorisasi Indeks KAMI telah mengacu pada kerangka kerja COBIT (*Control Objective for Information and related Technology*) atau CMMI (*Capability Maturity Model for Integration*). Tingkat kematangan ini nantinya digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi di organisasi. Indeks KAMI telah mengelompokan menjadi 5 kategori tingkat kematangan sebagai berikut:

a. Tingkat 0- Tidak Diketahui (PASIF)
    1) Status kesiapan keamanan informasi tidak diketahui
    2) Pihak yang terlibat tidak mengkuti atau tidak melaporkan pemeringkatan Indeks KAMI.
b. Tingkat I- Kondisi Awal (REAKTIF)
    1) Mulai adanya pemahaman mengenai perlunya pengelolaan keamanan informasi.
    2) Penerapan langkah pengamanan masih bersifat reaktif, tidak teratur, tidak mengacu kepada keseluruhan risiko yang ada, tanpa alur komunikasi dan kewenangan yang jelas dan tanpa pengawasan.
    3) Kelemahan teknis dan non-teknis tidak teridentifikasi dengan baik.
    4) Pihak yang terlibat tidak menyadari tanggung jawab mereka.
c. Tingkat II- Penerapan Kerangka Kerja Dasar (AKTIF)
    1) Pengamanan sudah diterapkan walaupun sebagian besar masih di area teknis dan belum adanya keterkaitan langkah pengamanan untuk mendapatkan strategi yang efektif.
    2) Proses pengamanan berjalan tanpa dokumentasi atau rekaman resmi.
    3) Langkah pengamanan operasional yang diterapkan bergantung kepada pengetahuan dan motivasi individu pelaksana.
    4) Bentuk pengamanan secara keseluruhan belum dapat dibuktikan efektivitasnya.
    5) Kelemahan dalam manajemen pengamanan masih banyak ditemukan dan tidak dapat diselesaikan dengan tuntas oleh pelaksana maupun pimpinan sehingga menyebabkan dampak yang sangat signifikan.
    6) Manajemen pengamanan belum mendapatkan prioritas dan tidak berjalan secara konsisten.
    7) Pihak yang terlibat kemungkinan besar masih belum memahami tanggung jawab mereka.
d. Tingkat III- Terdefinisi dan Konsisten (PRO AKTIF)
    1) Bentuk pengamanan yang baku sudah diterapkan secara konsisten dan terdokumentasi secara resmi.
    2) Efektivitas pengamanan dievaluasi secara berkala, walaupun belum melalui proses yang terstruktur.
    3) Pihak pelaksana dan pimpinan secara umum dapat menangani permasalahan terkait pengelolaan keamanan pengendalian dengan tepat, akan tetapi beberapa kelemahan dalam sistem manajemen masih ditemukan sehingga dapat mengakibatkan dampak yang signifikan.

4) Kerangka kerja pengamanan sudah mematuhi ambang batas minimum standar atau persyaratan hukum yang terkait.
5) Secara umum semua pihak yang terlibat menyadari tanggungjawab mereka dalam pengamanan informasi.

e. Tingkat IV- Terkelola dan Terukur (TERKENDALI)
1) Pengamanan diterapkan secara efektif sesuai dengan strategi manajemen risiko
2) Evaluasi (pengukuran) pencapaian sasaran pengaman dilakukan secara rutin, formal dan terdokumentasi.
3) Penerapan pengamanan teknis secara konsisten dievaluasi efektivitasnya.
4) Kelemahan manajemen pengamanan teridentifikasi dengan baik dan secara konsisten ditindaklanjuti pembenahannya.
5) Manajemen pengamanan bersifat pro-aktif dan menerapkan pembenahan untuk mencapai bentuk pengelolaan yang efisien.
6) Insiden dan ketidakpatuhan (non-conformity) diselesaikan melalui proses formal dengan pembelajaran akar permasalahan.
7) Karyawan merupakan bagian yang tidak terpisahkan dari pelaksana pengamanan informasi.

f. Tingkat V- Optimal (OPTIMAL)
1) Pengamanan menyeluruh diterapkan secara berkelanjutan dan efektif melalui program pengelolaan risiko yang terstruktur.
2) Pengamanan informasi dan manajemen risiko sudah terintegrasi dengan tugas pokok instansi.
3) Kinerja pengamanan dievaluasi secara kontinyu, dengan analisisparameter efektivitas kontrol, kajian akar permasalahan dan penerapan langkah untuk optimasi peningkatan kinerja
4) Target pencapaian program pengamanan informasi selalu dipantau, dievaluasi dan diperbaiki.
5) Karyawan secara proaktif terlibat dalam peningkatan efektivitas pengamanan

4. Metode Penelitian

Tahapan penelitian yang dilakukan menggunakan langkah-langkah sebagai berikut :

a. Pengkajian ulang tingkat kelengkapan dan penetapan langkah perbaikan dan kematangan dari hasil penelitian sebelumnya mengenai tata kelola keamanan informasi dan pengelolaan resiko dalam keamanan informasi.
b. Tahap berikutnya adalah pendefinisian ruang lingkup penelitian. Ruang lingkup dapat dipilih sesuai dengan kepentingan penilaian Indeks KAMI. Pada tahap ini obyek penelitian dapat dipilih atau ditentukan lebih spesifik seperti penentuan divisi pada obyek penelitian yang akan didahukan sebagai pilot project penelitian. Ruang lingkup yang digunakan adalah semua area yang ada pada indeks KAMI. Area tersebut antara lain kategori sistem elektronik, tata kelola keamanan informasi, pengelolaan resiko keamanan informasi, kerangka kerja keamanan informasi, pengelolaan aset informasi dan teknologi serta keamanan informasi.

c. Tahap berikutnya adalah pengambilan data untuk digunakan sebagai penilaian pengukuran dengan menggunakan indeks KAMI.
d. Selanjutnya adalah penilaian kelengkapan keamanan informasi. Penilaian dilakukan dalam indeks KAMI dilakukan dengan keseluruhan cakupan yang tercantum dalam standar ISO/IEC 27001:2013 yang disusun kedalam 5 area.
e. Tahapan terakhir dari penelitian ini adalah melakukan analisis dan pembahasan hasil kelengkapan keamanan informasi. Analisis ini meliputi hasil dari proses evaluasi yang telah dilakukan pada tahap evaluasi

5. Analisis dan Pembahasan

Sebelum melakukan proses evaluasi keamanan informasi di 5 area yang sudah diefinisikan dalam indeks KAMI. Perlu dijelaskan bahwa indeks KAMI yang digunakan pada tahun pertama telah mengalami perubahan yang cukup signifikan dengan perbedaan sebagai berikut:

Tabel 2. Perbandingan Indeks KAMI Versi 1 dan Versi 3

No	Versi 2	Versi 3
1	Peran TIK dalam Instansi (12 pertanyaan)	Kategori Sistem Elektronik (10 pertanyaan)
2	Tata Kelola Keamanan Informasi (20 pertanyaan)	Tata Kelola Keamanan Informasi (22 pertanyaan)
3	Pengelolaan Risiko Keamanan Informasi (15 pertanyaan)	Pengelolaan Risiko Keamanan Informasi (16 pertanyaan)
4	Kerangka Kerja Keamanan Informasi (28 pertanyaan)	Kerangka Kerja Keamanan Informasi (29 pertanyaan)
5	Pengelolaan Aset Informasi (34 pertanyaan)	Pengelolaan Aset Informasi (38 pertanyaan)
6	Teknologi dan Keamanan Informasi (24 pertanyaan)	Teknologi dan Keamanan Informasi (26 pertanyaan)
Total	**133 pertanyaan**	**141**

Dari table diatas dapat dilihat bahwa pengukuran kesiapan organisasi dalam menyiapkan ISO 27001 terkait dengan keamanan informasi, versi 3:2015 lebih detil dan memiliki pertanyaan lebih banyak. Untuk kategori sistem elektronik, hasil analisa data mengatakan bahwa ketergantungan UPT. PPTI terhadap sistem elektronik adalah strategis. Dimana nilai strategis adalah jika hasil pemgumpulan data memiliki nilai antara 35 dan 50. Data survey terkait kategori sistem elektronik mendapatkan nilai 40 (tabel 3).

Tabel 3. Indikator Pengkategorian Sistem Elektronik Organisasi

	Kategori Sistem Elektronik	Status
1,1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar	B

	Kategori Sistem Elektronik	Status
1,2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik	
	[A] Lebih dari Rp.10 Miliar	A
	[B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar	
	[C] Kurang dari Rp.1 Miliar	
1,3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu	
	[A] Peraturan atau Standar nasional dan internasional	A
	[B] Peraturan atau Standar nasional	
	[C] Tidak ada Peraturan khusus	
1,4	Menggunakan algoritma khusus untuk keamanan informasi dalam Sistem Elektronik	
	[A] Algoritma khusus yang digunakan Negara	A
	[B] Algoritma standar publik	
	[C] Tidak ada algoritma khusus	
1,5	Jumlah pengguna Sistem Elektronik	
	[A] Lebih dari 5.000 pengguna	A
	[B] 1.000 sampai dengan 5.000 pengguna	
	[C] Kurang dari 1.000 pengguna	
1,6	Data pribadi yang dikelola Sistem Elektronik	
	[A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya	
	[B] Data pribadi yang bersifat individu dan/atau data pribadi yang terkait dengan kepemilikan badan usaha	A
	[C] Tidak ada data pribadi	
1,7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi	
	[A] Sangat Rahasia	A
	[B] Rahasia dan/ atau Terbatas	
	[C] Biasa	
1,8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi	
	[A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik	A
	[B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung	
	[C] Proses yang tidak berdampak bagi kepentingan orang banyak	
1,9	Dampak dari kegagalan Sistem Elektronik	
	[A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara	
	[B] Tidak tersedianya layanan publik atau proses penyelenggaraan negara dalam 1 provinsi atau lebih	C
	[C] Tidak tersedianya layanan publik atau proses penyelenggaraan negara dalam 1 kabupaten/kota atau lebih	
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme)	
	[A] Menimbulkan korban jiwa	B
	[B] Terbatas pada kerugian finansial	
	[C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan merugikan finansial)	
	Skor penetapan Kategori Sistem Elektronik	**40**

Kategori Sistem Elektronik		Status
	Tingkat Ketergantungan	Strategis

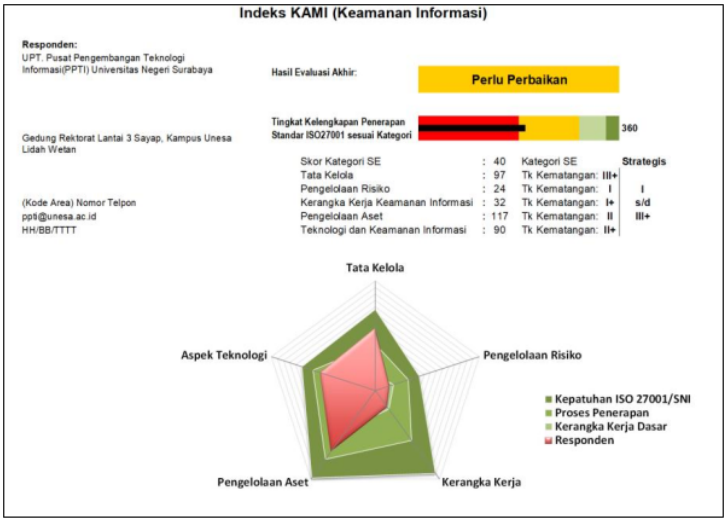
Secara umum, sistem manajemen keamanan informasi UPT.PPTI masih perlu perbaikan, artinya sebagian dari dokumen kontrol yang wajib disediakan agar terkonfirmasi dengan standart ISO 27001:2013 tidak bias dipenuhi saat ini. Titik rekomendasi dari aspek yang harus diperbaiki dapat dilihat pada tabel 4.

Tabel 4. Tingkat kematangan terhadap implemtasi ISO 27001

	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Aspek Teknologi
Tingkat II					
Status	II	No	I+	II	II
Tingkat III					
Validitas	Yes	No	No	No	Yes
Status	III	No	No	No	II+
Tingkat IV					
Validitas	Yes	No	No	No	No
Status	III+	No	No	No	No
Tingkat V					
Validitas	No	No	No	No	No
Status	No	No	No	No	No
Status Akhir	III+	I	I+	II	II+
	6	**1**	**2**	**3**	**4**

Dari tabel tersebut tampak, bahwa area kritis yang perlu mendapatkan perhatian adalah terkait dengan pengelolaan resiko keamanan informasi, kerangka kerja keamanan informasi dan pengelolaan asset keamanan informasi. Untuk meningkatkan kesiapan terhadap aspek ini, maka perlu dibuat dokumentasi dan prosedur baku yang dapat menjamin bahwa pengelolaan keamanan informasi di UPT. PPTI Unesa telah terpenuhi dan berjalan dengan baik. Rekomendasi kebutuhan dokumen untuk meningkatkan tingkat kematangan dan kesiapan dalam impelementasi SMKI berbasis ISO 27001:2013 dapat dilihat pada tabel 5.

Makna dari strategis dalam hal ini adalah bahwa TIK sudah menjadi kebutuhan penting dalam organisasi universitas. Selanjutnya hasil analisa dari 5 area tata kelola keamanan informasi dapat di peroleh seperti gambar 1.



Gambar 1. Dashboard Hasil Pengukuran Kesiapan dan Kematangan SMKI berbasis Indeks KAMI 3:2015

6. Penutup

Dari hasil penelitian secara keseluruhan, bahwa area yang harus mendapatkan perbaikan lebih khusus adalah aspek pengelolaan resiko keamanan informasi, kerangka kerja keamanan informasi dan pengelolaan asset keamanan informasi. Ketiga area masih dalam kategori I sampai II yang artinya secara kelengkapan dan kematangan masih banyak yang harus diperbaiki.

Ucapan Terima Kasih (*Acknowledgments*)

Ucapan terimakasih yang sebesar-besarnya kami persembahkan untuk Kementrian Ristekdikti yang telah memberikan dana penelitian dalam skema penelitian desentralisasi untuk penelitian terapan unggulan perguruan tinggi selama dua tahun yaitu 2017 dan 2018.

Daftar Pustaka

Afrianto, Irawan, and Taryana Suryana (2015). "Pengukuran dan Evaluasi Keamanan Informasi Menggunakan Indeks KAMI-SNI/ISO/IEC 27001: 2013 Studi Kasus Perguruan Tinggi X." Ultima Infosys 6.1 ,2015: 43-49

Afrianto, Irawan, Taryana Suryana, and Sufa'atin Lnu (2015). "Pengukuran Keamanan Informasi Pada Aplikasi dan Sistem Informasi Pendukung Akademik Menggunakan Standar SNI ISO/IEC 27001: 2013." Prosiding Saintiks FTIK Unikom 1

Ardiyana, Yuda, D. S. Ririn Dwi Agustin, And D. S. Rita Rijayanti (2017). Analisis Tingkat Kematangan Keamanan Informasi Pt Mustika Petrotech Indonesia Dengan Menggunakan Indeks KAMI. Diss. Fakultas Teknik.

Basyarahil, Firzah Abdullah (2017). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 2700: 2013 Pada Direktorat Pengembangan Teknologi Dan Sistem Informasi (DPTSI) ITS Surabaya. Diss. Institut Teknologi Sepuluh Nopember.

Brewer, David (2013), An Introduction to ISO/IEC 27001: 2013. BSI Standard Limited,

Disterer, Georg (2013). "ISO/IEC 27000, 27001 and 27002 for information security management." Journal of Information Security 4.02, 92.

Heryatna, Dian Erman. Pengukuran Dan Evaluasi Keamanan Informasi Menggunakan Indeks Kami (2017),Studi Kasus: LPSE Kabupaten Bandung Barat, Diss. Fakultas Teknik.

Hidayati, Nur (2014). "Kajian Tata Kelola IT Berdasarkan Indeks KAMI Pada Universitas Pakuan Bogor." Paradigma 16.2 ,90-100.

Humphreys, Edward. Implementing the ISO/IEC 27001: 2013 ISMS Standard. Artech House, 2016.

ISO/IIEC 2700, Information technology--Security techniques -- Information security management systems -- Overview and vocabulary, 4th edition, 15th Feb 2016

ISO/IEC 27001:2013, Information technology -- Security techniques -- Information security management systems – Requirements, https://www.iso.org/standard/54534.html, retrieved on 29th April 2017.

Marco, Robert (2016). "Indeks Penilaian Tingkat Kematangan (Maturity) IT Governance Pada Manajemen Keamanan Layanan Teknologi Informasi." Data Manajemen Dan Teknologi Informasi (Dasi) 17.2,76-82.

Pardo, César, Francisco J. Pino, and Félix Garcia (2016). "Towards an Integrated Management System (IMS), harmonizing the ISO/IEC 27001 and ISO/IEC 20000-2 Standards." International Journal of Software Engineering and Its Applications 10.9 ,217-230.

Putra, Endi Lastyono, Bekti Cahyo Hidayanto, and Hanim Maria Astuti (2014). "Evaluasi Keamanan Informasi Pada Divisi Network of Broadband PT. Telekomunikasi Indonesia Tbk. Dengan Menggunakan Indeks Keamanan Informasi (KAMI)." Jurnal Teknik ITS 3.2, A228-A233.

Putra, Anggi Anugraha, Oky Dwi Nurhayati, and Ike Pertiwi Windasari (2016). "Perencanaan dan Implementasi Information Security Management System Menggunakan Framework ISO/IEC 20071." Jurnal Teknologi dan Sistem Komputer 4.1, 60-66.

Saputra, Dedi, And Oryza Gilang(2016). "Evaluasi Keamanan Informasi Pada Sma Islam Al-Azhar (SMAIA) 4 Kemang Pratama Berdasarkan Indeks Keamanan Informasi (KAMI) SNI ISO/IEC 27001: 2013." Jurnal Khatulistiwa Informatika 4.1

Siga, Mustaqim, Tony Dwi Susanto, and Bekti Cahyo Hidayanto (2014). "Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi Pada Kantor Wilayah Ditjen Perbendaharaan Negara Jawa Timur." Sesindo 2014

Syarif, Rifqi Akmal, And Agung Nugroho (2016). "Analisis Tingkat Kematangan Sistem Manajemen Keamanan Informasi Direktorat Jenderal Perbendaharaan Diukur Dengan Menggunakan Indeks Keamanan Informasi (Studi Kasus: Aplikasi SPAN)." Info Artha 4.4, 69-80.

Tim Direktorat Keamanan Informasi (2011), Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik (in Bahasa)

Winda, Kusumaningrum Septilia(2016), "Evaluasi Tingkat Kelengkapan Dan Kematangan Sistem Keamanan Informasi Berdasarkan Indeks Kami Pada Divisi Sampling Dan Pengujian Bbpom Kota Semarang." Skripsi, Fakultas Ilmu Komputer

ANALISIS TINGKAT KESIAPAN DAN KEMATANGAN IMPLEMENTASI ISO 27001:2013

ORIGINALITY REPORT

15%	12%	3%	4%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Mercu Buana Student Paper	1%
2	mediacenter.malangkota.go.id Internet Source	1%
3	doaj.org Internet Source	1%
4	Submitted to Universitas Hasanuddin Student Paper	1%
5	Jesus Maiz - Apellaniz. "A Galactic O Star Catalog", The Astrophysical Journal Supplement Series, 03/2004 Publication	1%
6	ejournal.unesa.ac.id Internet Source	1%
7	rimbaalammakmur.co Internet Source	1%
8	repository.uksw.edu Internet Source	1%

9	Hendry Fajar Yoseviano, Astari Retnowardhani. "The use of ISO/IEC 27001: 2009 to analyze the risk and security of information system assets: case study in xyz, ltd", 2018 International Conference on Information Management and Technology (ICIMTech), 2018 Publication	<1 %
10	jdih.sumutprov.go.id Internet Source	<1 %
11	Submitted to Sriwijaya University Student Paper	<1 %
12	Submitted to Syiah Kuala University Student Paper	<1 %
13	Submitted to Universitas 17 Agustus 1945 Surabaya Student Paper	<1 %
14	Submitted to Fakultas Ekonomi Universitas Indonesia Student Paper	<1 %
15	jurnal.ugm.ac.id Internet Source	<1 %
16	mutuinstitute.com Internet Source	<1 %
17	repository.unri.ac.id Internet Source	<1 %

18	ijc.ilearning.co Internet Source	<1 %
19	repository.lppm.unila.ac.id Internet Source	<1 %
20	repository.unikom.ac.id Internet Source	<1 %
21	s-space.snu.ac.kr Internet Source	<1 %
22	www.bakrietelecom.com Internet Source	<1 %
23	www.dpr.go.id Internet Source	<1 %
24	www.indotelko.com Internet Source	<1 %
25	acstrainingcenterindonesia.blogspot.com Internet Source	<1 %
26	qdoc.tips Internet Source	<1 %
27	Andrea Szőke. "Extenzív zöldtetők, és azokon alkalmazott egyes Sedum fajok komplex értékelése", Corvinus University of Budapest, 2016 Publication	<1 %
28	documents.mx Internet Source	<1 %

29	eprints.binus.ac.id Internet Source	<1 %
30	eprints.stainkudus.ac.id Internet Source	<1 %
31	jepa.ub.ac.id Internet Source	<1 %
32	mrchoiruddin.wordpress.com Internet Source	<1 %
33	perumahan.pu.go.id Internet Source	<1 %
34	repositorio.ufpe.br Internet Source	<1 %
35	repository.radenintan.ac.id Internet Source	<1 %
36	zombiedoc.com Internet Source	<1 %
37	ejurnal.tunasbangsa.ac.id Internet Source	<1 %
38	Tina Tri Wulansari, Dody Novandi. "Evaluation of Information Security Management Using the KAMI Index Framework", 2022 International Conference of Science and Information Technology in Smart Administration (ICSINTESA), 2022 Publication	<1 %

39	ejournal.uin-suka.ac.id Internet Source	<1%

Exclude quotes	Off	Exclude matches	Off
Exclude bibliography	On		