Implementasi Indeks KAMI di Universitas Sam Ratulangi

Muh. Faturachman Husin[1], Hans F. Wowor[2], Stanley D.S. Karouw[3]
Teknik Informatika Universitas Sam Ratulangi. Manado, Jl. Kampus Unsrat Bahu, Manado 95115
13021106108@student.unsrat.ac.id[1], hanswowor@unsrat.ac.id[2], stanley.karouw@unsrat.ac.id[3]

***Abstrak* – Informasi adalah aset organisasi yang sangat berharga. Oleh sebab itu informasi menjadi salah satu objek serangan untuk dieksploitasi. Tujuan utama keamanan sistem informasi adalah menjaga 3 (tiga) atribut yaitu kerahasiaan (confidentiality), keutuhan (integrity) dan ketersediaan (availability). Universitas Sam Ratulangi memiliki unit kerja yang mempunyai tugas dan kewajiban untuk mengelola dan memberikan informasi. perlu dilakukan evaluasi keamanan sistem informasi untuk mendapatkan gambaran kondisi kesiapan dan kematangan keamanan informasi. Indeks Keamanan Informasi disingkat KAMI adalah alat evaluasi yang dirilis oleh Kementerian Komunikasi dan Informasi yang berfungsi untuk menganalisa tingkat kesiapan pengamanan informasi di instansi pemerintah. Didapati Tingkat kematangan keamanan informasi di Universitas Sam Ratulangi masih tergolong rendah dan butuh perbaikan walaupun peran/tingkat ketergantungan akan Teknologi Informasi dan Komunikasi tergolong Tinggi. Disajikan pula saran perbaikan untuk kekurangan yang ditemukan di sistem manajemen keamanan informasi.**

Kata kunci: Keamanan Informasi, Indeks KAMI, UNSRAT.

I. PENDAHULUAN

Informasi adalah aset organisasi yang sangat berharga. Oleh sebab itu informasi menjadi salah satu objek serangan untuk dieksploitasi. [1] Indonesia *Cyber Security Report* yang diterbitkan oleh *ID-SIRTII* menemukan data jumlah total serangan pada tahun 2016 sebanyak 136.672.948 kali (terjadi peningkatan lebih dari 50% dari tahun 2015 jumlah total serangan hanya 89.691.783 serangan keamanan internet di Indonesia). Jenis serangan terbanyak adalah *DDOS*, dan serangan yang paling banyak terjadi pada bulan April 2016, yakni sebanyak 46.338.965 serangan. Sedangkan domain pemerintahan *go.id* yang menjadi *Host Phising* sebesar 17.73% dan id 13,64%. Berbagai bentuk trend serangan dan insiden ini menggunakan instrumen *cyberspace* sebagai saluran utama dalam melaksanakan tindakannya. [2] Salah satu kebijakan yang dapat diambil oleh organisasi untuk mengatasi gangguan keamanan informasi adalah dengan menerapkan Sistem Manajemen Keamanan Informasi (SMKI). Walaupun kenyataannya sampai saat ini belum atau bahkan tidak akan ada sebuah keamanan Sistem Informasi yang sempurna sehingga dapat 100% mengamankan Informasi dari segala gangguan [3].

Universitas Sam Ratulangi (UNSRAT) Sebagai instansi pendidikan belum menerapkan standarisasi untuk sistem informasi. Sebelum standarisasi diterapkan, perlu dilakukan evaluasi keamanan sistem informasi di unit kerja demi mendapatkan gambaran kondisi kesiapan dan kematangan keamanan informasi dengan menggunakan Indeks Keamanan Informasi [2].

Indeks KAMI sebagai alat yang disusun oleh Tim Direktorat Keamanan Informasi Kementerian Komunikasi dan Informatika untuk mengukur dan menganalisis tingkat kesiapan atau kematangan pengamanan informasi yang ada di suatu instansi [2]. Hasil pengukuran ini akan menghasilkan tingkat kematangan keamanan informasi di UNSRAT, yang nantinya akan dievaluasi dan digunakan sebagai referensi untuk meningkatkan tingkat keamanan informasi UNSRAT dimasa mendatang.

II. LANDASAN TEORI

2.1 Keamanan Informassi

Keamanan Informasi adalah terjaganya kerahasiaan (confidentiality), keutuhan (integrity) dan ketersediaan (availability) informasi [2]. Orang mungkin akan bertanya, mengapa "keamanan informasi" dan bukan "keamanan teknologi informasi" atau IT Security. Kedua istilah ini sebenarnya saling terkait, namun mengacu pada dua hal yang sama sekali berbeda. "Keamanan Teknologi Informasi" atau IT Security mengacu pada usaha usaha mengamankan infrastruktur TI dari gangguan-gangguan berupa akses terlarang serta utilisasi jaringan yang tidak diizinkan, sementara "keamanan informasi" fokus pada data dan informasi milik organisasi.

Pada konsep ini, usaha-usaha yang dilakukan adalah merencanakan, mengembangkan serta mengawasi semua kegiatan yang terkait dengan bagaimana data dan informasi bisnis dapat digunakan serta diutilisasi sesuai dengan fungsinya serta tidak disalahgunakan atau bahkan dibocorkan ke pihak - pihak yang tidak berkepentingan [3]. Berdasarkan penjelasan tersebut kemananan teknologi informasi‟ merupakan bagian dari keseluruhan aspek keamanan informasi‟. Karena teknologi informasi merupakan salah satu alat penting yang digunakan untuk mengamankan akses serta penggunaan dari data dan informasi organisasi. Jadi, teknologi informasi bukanlah satu-satunya aspek yang memungkinkan terwujudnya konsep keamanan informasi di organisasi.

2.2 Konsep *CIA*

CIA memiliki tiga fokus tujuan utama, yaitu *confidentiality*, *integrity*, *dan availability* [5]. Setiap komponen dalam *CIA* ini sangat berperan penting dalam kesempurnaan keamanan sistem informasi. Parameter dalam *CIA* ini digunakan untuk menentukan apakah suatu jaringan atau informasi dikatakan aman atau tidak.

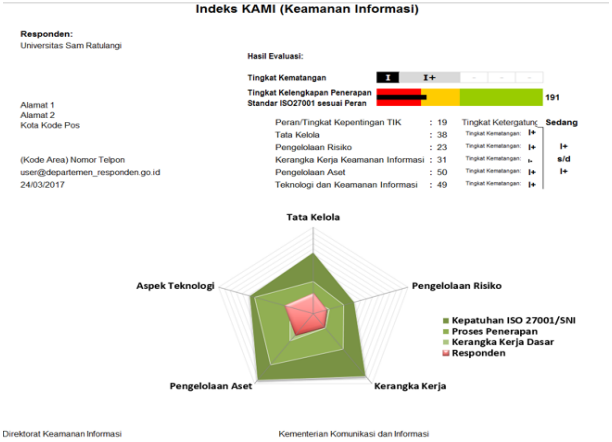
Confidentiality adalah bahwa informasi tidak tersedia atau diungkapkan kepada individu, entitas, atau proses yang tidak sah [5]. Misalnya pengungkapan informasi pada pihak tidak berhak secara lisan, surat elektronik, menyalin, mencetak dokumen, dan sebagainya. Kita tahu bahwa informasi adalah sebuah kekuatan, dan di era informasi ini, akses menuju sebuah informasi menjadi lebih penting lagi. Akses tidak berwenang yang terjadi pada informasi yang rahasia *(confidential)* dapat memiliki konsekuensi yang sangat serius, tidak hanya pada aplikasi keamanan nasional, tapi juga berlaku pada industri/pabrik dan komersial. Terdapat beberapa cara mekanisme proteksi *'confidentiality'* untuk system informasi, antara lain adalah teknik kriptografi dan control akses. Maka ancaman-ancaman seperti *malware, intruders*, jaringan yang tak aman, dan sistem administrasi yang lemah dapat diatasi.

Integrity adalah tindakan menjaga keakuratan dan kelengkapan asset [5]. Integritas suatu data bukan hanya benar, tetapi juga terpercaya. Sebagai contoh, jika sebuah informasi disalin ke dalam *USB* atau mengupload ke email, maka informasi tersebut bukan hanya tidak rahasia lagi, tetapi telah diragukan integritasnya. Sebab, jika sebuah file/data telah digandakan, maka akan terbuka kemungkinan risiko untuk diubah atau mengalami modifikasi. Terdapat beberapa mekanisme proteksi pada *'Integrity'*, yang dibagi menjadi dalam 2 kelompok, yaitu mekanisme pencegahan, seperti kontrol akses yang mencegah pemodifikasian informasi yang tak berwenang, selain itu ada teknik pendeteksian, dimana diadakan sebuah pendeteksian pemodifikasian informasi yang tak berwenan setelah mekanisme pencegahan gagal dilakukan. Control yang menjaga *'integrity'* termasuk prinsip antara lain *privilege* (hak), *separation* (pemisahan), dan *rotation* (perotasian) dalam pekerjaan.

Availability sebagai aset yang dapat diakses dan digunakan saat diminta oleh entitas yang berwenang [5]. Ketersediaan dapat diukur dengan sebagai contoh adalah dalam konteks bisnis memiliki *web portal* yang aman melawan serangan *Denial of Service (DOS)* atau bila ketersediaan infrastruktur komputer tidak dapat diyakini bekerja pada sistem organisasi, hal ini menyebabkan proses atau orang-orang tidak dapat bekerja pada saat itu. Jadi, *availability* juga merupakan hal yang penting disamping *confidentiality* dan *integrity*. Ancaman terhadap availability dikenal sebagai *denial of service* atau disingkat *DoS*. Musibah yang terjadi natural dan dibuat oleh manusia bisa mempengaruhi *availabilitas*. Maka, *disaster recovery planning* itu dibutuhkan untuk meminimalisir kehancuran/kehilangan data.

2.3 Indeks KAMI

Indeks KAMI adalah alat evaluasi untuk menganalisis tingkat kesiapan pengamanan informasi di instansi pemerintah [2]. Alat evaluasi ini tidak ditujukan untuk menganalisis kelayakan atau efektivitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi.



Gambar 1 Dashboard Indeks KAMI

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 SNI ISO/IEC 27001:2009. Hasil evaluasi indeks KAMI menggambarkan tingkat kematangan, tingkat kelengkapan penerapan SNI ISO/IEC 27001:2009 dan peta area tata kelola keamanan sistem informasi di instansi pemerintah.

Bentuk evaluasi yang diterapkan dalam Indeks KAMI dirancang untuk dapat digunakan oleh instansi pemerintah dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya Tugas Pokok dan Fungsi yang ada. Data yang digunakan dalam evaluasi ini nantinya akan memberikan potret indeks kesiapan dari aspek kelengkapan maupun kematangan kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya.

Alat evaluasi ini kemudian bisa digunakan secara berkala untuk mendapatkan gambaran perubahan kondisi keamanan informasi sebagai hasil dari program kerja yang dijalankan, sekaligus sebagai sarana untuk menyampaikan peningkatan kesiapan kepada pihak yang terkait (stakeholders).

Penggunaan dan publikasi hasil evaluasi Indeks KAMI merupakan bentuk tanggungjawab penggunaan dana publik sekaligus menjadi sarana untuk meningkatkan kesadaran mengenai kebutuhan keamanan informasi di instansi pemerintah. Pertukaran informasi dan diskusi dengan instansi pemerintah lainnya sebagai bagian dari penggunaan alat evaluasi Indeks KAMI ini juga menciptakan alur komunikasi antar pengelola keamanan informasi di sektor pemerintah sehingga semua pihak dapat mengambil manfaat dari lesson-learned yang sudah dilalui.

Alat evaluasi Indeks KAMI ini secara umum ditujukan untuk digunakan oleh instansi pemerintah di tingkat pusat. Akan tetapi satuan kerja yang ada di tingkatan Direktorat Jenderal, Badan, Pusat atau Direktorat juga dapat menggunakan alat evaluasi ini untuk mendapatkan gambaran mengenai kematangan program kerja keamanan

informasi yang dijalankannya. Evaluasi ini dianjurkan untuk dilakukan oleh pejabat yang secara langsung bertanggung jawab dan berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya.

Penilaian dalam Indeks KAMI dilakukan dengan cakupan keseluruhan persyaratan pengamanan yang tercantum dalam standar ISO/IEC 27001:2009, yang disusun kembali menjadi 5 (lima) area di bawah ini:

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

Penyusunan kembali menjadi 5 (lima) komponen ini dilakukan untuk mendapatkan bentuk evaluasi mandiri yang mudah untuk ditanggapi dimana hasil evaluasinya sendiri nanti akan dapat digunakan sebagai panduan pembenahan atau peningkatan kinerja tata kelola keamanan informasi. Dalam setiap area, proses evaluasi akan membahas sejumlah aspek yang dibutuhkan untuk mencapai tujuan utama dari pengamanan di area tersebut.

Proses penilaian dilakukan melalui 2 (dua) metode. Metode pertama akan mengevaluasi sejauh mana instansi responden sudah menerapkan pengamanan sesuai dengan kelengkapan kontrol yang diminta oleh standar ISO/IEC 27001:2009. Untuk kelima area evaluasi, yang dimaksud sebagai kontrol dijelaskan secara singkat di bawah ini:

1) Tata Kelola Keamanan Informasi – Kontrol yang diperlukan adalah kebijakan formal yang mendefinisikan peran, tanggung-jawab, kewenangan pengelolaan keamanan informasi, dari pimpinan unit kerja sampai ke pelaksana operasional. Termasuk dalam area ini juga adalah adanya program kerja yang berkesinambungan, alokasi anggaran, evaluasi program dan strategi peningkatan kinerja tata kelola keamanan informasi.
2) Pengelolaan Risiko Keamanan Informasi – Bentuk tata kelola yang diperlukan adalah adanya kerangka kerja pengelolaan risiko dengan definisi yang eksplisit terkait ambang batas diterimanya risiko, program pengelolaan risiko dan langkah mitigasi yang secara reguler dikaji efektifitasnya.
3) Kerangka Kerja Keamanan Informasi – Kelengkapan kontrol di area ini memerlukan sejumlah kebijakan dan prosedur kerja operasional, termasuk strategi penerapan, pengukuran efektifitas kontrol dan langkah perbaikan.
4) Pengelolaan Aset Informasi – Kontrol yang diperlukan dalam area ini adalah bentuk pengamanan terkait keberadaan aset informasi, termasuk keseluruhan proses yang bersifat teknis maupun administratif dalam siklus penggunaan aset tersebut.
5) Teknologi dan Keamanan Informasi – Untuk kepentingan Indeks KAMI, aspek pengamanan di area teknologi mensyaratkan adanya strategi yang terkait dengan tingkatan risiko, dan tidak secara eksplisit menyebutkan teknologi atau merk pabrikan tertentu.

Detail bentuk pengamanan yang dibahas di masing-masing area dapat dipahami dari pertanyaan (kajian mandiri) yang disediakan di area tersebut. Metode yang kedua merupakan perluasan dari evaluasi kelengkapan dan digunakan untuk mengidentifikasi tingkat kematangan penerapan pengamanan dengan kategorisasi yang mengacu kepada tingkatan kematangan yang digunakan oleh kerangka kerja COBIT (Control Objective for Information and related Technology) atau CMMI (Capability Maturity Model for Integration). Tingkat kematangan ini nantinya akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi di Kementerian/Lembaga.

Pemetaan dan pemeringkatan akan dilakukan Tim yang ditetapkan Kementerian Komunikasi dan Informatika (KOMINFO) dan menjadi dasar bagi pemberian OPINI Kominfo tentang kondisi tata kelola keamanan informasi di Kementerian/Lembaga terkait.

Indeks KAMI adalah perangkat untuk mengevaluasi penerapan tata kelola keamanan informasi yang dilakukan secara berkelanjutan, dan digunakan untuk memberikan gambaran kemajuan hasil penerapan secara berkala. Apabila terjadi perubahan pada infrastruktur atau unit kerja yang ada dalam lingkup awal evaluasi Indeks KAMI, pengkajian ulang bermanfaat untuk memastikan kelengkapan dan kematangan bentuk tata kelola yang diterapkan di awal. Untuk proyek pengadaan sistem aplikasi berskala besar dan strategis, Indeks KAMI dapat juga difungsikan sebagai checklist penerapan tata kelola bagi pengamanan sistem tersebut.

2.4 Penelitian Terkait

Terdapat beberapa penelitian sebelumnya yang menjadi tinjauan dalam keamanan informasi. Sebagai bahan tinjauan dalam penelitian ini akan dicantumkan beberapa hasil penelitian sebelumnya yang dilakukan oleh beberapa peneliti,

Moch. Rashid Ridho (2012) [6]. Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan SNI ISO/IEC 27001:2009 Studi Kasus: Bidang Aplikasi dan Telematika Dinas Komunikasi Dan Informatika Surabaya. Perbedaan penelitian ini dengan

penelitian saya terletak pada studi kasus yang diambil. Pada penelitian ini mengambil studi kasus di Bidang Aplikasi dan Telematika Dinas Komunikasi Dan Informatika Surabaya. Sedangkan pada penelitian saya mengambil studi kasus di Universitas Sam Ratulangi.

Tedi Agoan, Hans F. Wowor dan Stanley Karouw (2017) [7]. Analisa Tingkat Kematangan Teknologi Informasi Pada Dinas Komunikasi Dan Informatika Kota Manado Menggunakan *Framework COBIT 5 Domain Evaluate, Deirect, Monitor (EDM) dan Deliver, Service, and Support (DSS)*. Perbedaan penelitian ini dengan penelitian saya terletak pada alat ukur yang digunakan. Pada penelitian ini menggunakan alat ukur yaitu *COBIT 5*.

Brian Gamaliel, Yaulie Rindengan dan Stanley Karouw (2017) [8]. Pengukuran Tingkat Keselarasan Tata Kelola Teknologi Informasi Menggunakan *Cobit 5* Pada Pemerintah Sulawesi Utara. Universitas Sam Ratulangi. Manado, Indonesia. Perbedaan penelitian ini dengan penelitian saya terletak pada alat ukur yang digunakan. Pada penelitian ini menggunakan alat ukur yaitu *COBIT 5*. Sedangkan pada penelitian saya menggunakan alat ukur yaitu INDEKS KAMI. Persamaan penelitian ini dengan penelitian saya adalah melakukan penelitian tentang audit atau analisa.

Mufti Rizal and Yudho Giri Sucahyo (2013) [9]. *A Study on the Preparedness of Information Security Framework Area based on the Assessment of Information Security Index in Ministry of XYZ.* Perbedaan penelitian ini dengan penelitian saya terletak pada alat ukur yang digunakan. Pada penelitian ini menggunakan alat ukur yaitu COBIT 4.1. Sedangkan pada penelitian saya menggunakan alat ukur yaitu INDEKS KAMI. Edit Prima, Yudho G. Sucahyo, and Zainal A. Hasibuan (2013) [10]. *Mapping the Certification Authority for e-Government Procurement System into eGovAMAN Framework*. Pada penelitian ini menjelaskan tentang kerangka kerja untuk melakukan audit pada keamanan informasi di pemerintahan Indonesia.

Adi Muhajirin (2012) [12]. Kajian Tingkat Kematangan Sistem Manajemen Keamanan Informasi Studi Kasus: Suku Dinas Komunikasi dan Informatika Jakarta Selatan. Program Pascasarjana Magister Ilmu Komputer, Sekolah Tinggi Manajemen Informatika dan Komputer Nusa Mandiri (STMIK Nusa Mandiri) Jakarta. Informasi merupakan aset yang sangat berharga bagi sebuah lembaga baik lembaga pemerintah maupun swasta termasuk dalam hal ini adalah Sudin Kominfomas Jakarta Selatan yang merupakan salah satu instansi Pemerintah. Maka dari itu pengamanan informasi sangat perlu untuk dilakukan. Sumber daya yang memadai dan cukup harus dialokasikan untuk melindungi aset informasi melalui penyelenggaraan kebijakan keamanan sistem informasi yang terukur sesuai dengan standard yang ada. Indeks KAMI merupakan suatu alat evaluasi yang digunakan untuk menganalisa tingkat kesiapan pengamanan informasi di Instansi Pemerintah. Berdasarkan hasil penelitian didapatkan hasil bahwa tingkat kesiapan pengamanan informasi di Kominfomas Jakarta Selatan berada pada tingkat kematangan dua yaitu masih berada pada tingkat proses penerapan.

III. METODOLOGI PENELITIAN

Tabel 1 Alur Penelitian

NO	TAHAPAN	INPUT	PROSES	OUTPUT
1	Persiapan	Telaah Dokumen bisnis	Studi Literatur	Identifikasi Masalah UNSRAT
2	Desain Penelitian	Identifikasi Organisasi	Penilaian INDEKS KAMI	Kuisioner/ Wawancara
				Batasan Masalah
3	Pengumpulan Dan Analisa Data	Populasi dan Sampel	Analisis Tingkat Kapabilitas	Nilai Tingkat Kematangan
		Analisis Data Kuisioner		Saran Rekomendasi
4	Penyusunan Laporan	Saran Rekomendasi	Studi Literatur	Laporan Hasil Penelitian
				Kesimpulan Dan Saran
				Presentasi Hasil Penelitian

Pada bab ini menjelaskan alur penelitian dimana terdapat rincian tentang bahan atau materi, alat, urutan langkah-langkah yang dibuat secara sistematis, logis sehingga dapat dijadikan pedoman yang jelas dan mudah untuk menyelesaikan permasalahan, analisis hasil dan kesulitan-kesulitan yang dihadapi. Urutan langkah-langkah penelitian dapat dilihat pada tabel 1.

Tahapan persiapan, peneliti melakukan telaah dokumen bisnis dan studi literature yaitu dokumen Renstra TIK UNSRAT dan dokumen hasil auditsistem informasi juga melakukan pencarian dasar-dasar teori dan penemuan dari penelitian yang telah dilakukan sebelumnya. Teori-teori yang terkait dengan permasalahan penelitian Indeks KAMI dan penelitian yang menggunakan Indeks KAMI versi lainnya atau penelitian yang menggabungkan beberapa model evaluasi akan saya pelajari dan di rangkum secara singkat sesuai dengan kebutuhan penelitian ini. Keluaran yang di dapatkan dari tahap persiapan yaitu identifikasi permasalahan TIK yang ada di universitas sam ratulangi.

Pada tahapan desain penelitian, peneliti melakukan identifikasi organisasi dan penilaian INDEKS KAMI. Identifikasi organisasi berisi tentang visi, misi, struktur organisasi, rencana strategis UNSRAT tentang TIK Dan laporan hasil audit. Indeks KAMI adalah perangkat untuk mengevaluasi penerapan tata kelola keamanan informasi yang dilakukan secara berkelanjutan, dan digunakan untuk memberikan gambaran kemajuan hasil penerapan secara berkala. Apabila terjadi perubahan pada infrastruktur atau unit kerja yang ada dalam lingkup awal evaluasi Indeks KAMI, pengkajian ulang bermanfaat untuk memastikan kelengkapan dan kematangan bentuk tata kelola yang diterapkan di awal. Keluaran yang di dapatkan dari tahap desain penelitian yaitu kuisioner, wawancara dan Batasan masalah yang dibutuhkan agar pembahasan mengarah pada tujuan dan tidak meluas.

Pada tahapan pengumpulan dan Analisa data, peneliti menentukan populasi, sampel dan Teknik analisis data yang diperlukan. Populasi dalam penelitian ini adalah seluruh Pengelola dan Pengguna Layananan TIK Universitas Sam Ratulangi baik itu dosen, mahasiswa, dan karyawan. Jumlah populasi untuk penelitian ini adalah 24.379 orang. Jumlah populasi tersebut berdasarkan jumlah rata-rata pengguna yang menggunakan layanan TIK UNSRAT. Cara pengambilan sampel pada penelitian ini adalah dengan

menggunakan accidental sampling. Accidental sampling adalah pengambilan sampel pada saat penelitian tersebut dilakukan. Sampel ini adalah beberapa informan yang berada di lokasi pada saat penelitian berlangsung. Jumlah sampel yang penulis ambil adalah 30 orang informan. Keluaran dari tahap ini adalah nilai tingkat kematangan dan saran rekomendasi untuk tingkat kelengkapan pengamanan dan tingkat kematangan pengamanan.

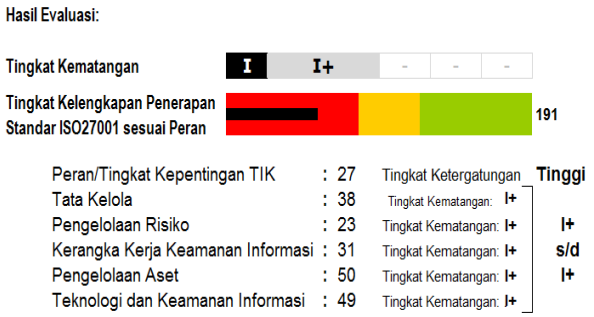
Pada tahap yang terakhir yaitu penyusunan laporan, peneliti memasukan saran rekomendasi dan studi literature. Keluaran dari tahapan ini yaitu laporan hasil penelitian, kesimpulan, saran dan presentasi hasil penelitian.

IV. HASIL DAN PEMBAHASAN

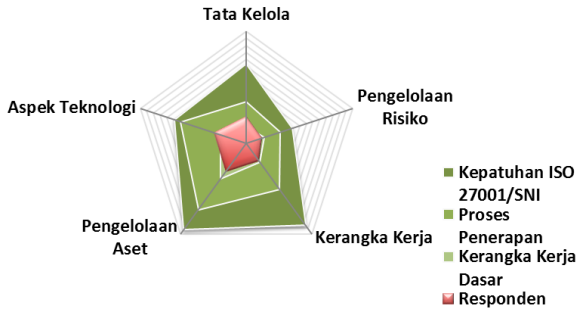
Implementasi Indeks KAMI di UNSRAT, menggunakan Indeks KAMI versi 2.3. Dalam alat ukur tersebut, terdapat 131 (seratus tiga puluh satu) pertanyaan yang dibagi menjadi 6 bagian. Pada Bagian I, informan diminta untuk mendefinisikan Peran TIK (Tingkat Kepentingan TIK) di unit masing-masing. Selain itu, informan juga diminta untuk mendeskripsikan infrastruktur TIK yang ada dalam satuan kerjanya secara singkat. Bagian II s.d. Bagian VI berisikan sejumlah pertanyaaan terkait Tingkat Kematangan keamanan informasi. Rekapituasi dan pengolahan data hasil observasi dapat dilihat pada tabel 2.

Tabel 2 Skor Area Evaluasi UNSRAT

AREA	SKOR
Peran TIK dalam Instansi	27
Tata Kelola Keamanan Informasi	38
Pengelolaan Risiko Keamanan Informasi	23
Kerangka Kerja Pengelolaan Keamanan Informasi	31
Pengelolaan Aset Informasi	50
Teknologi dan Keamanan Informasi	49



Gambar 2 Hasil Evaluasi Keamanan UNSRAT



Gambar 3 Diagram Radar Hasil Penilaian SMKI

Berdasarkan informasi pada Gambar 2 dapat disimpulkan bahwa :

1) Peran/Tingkat Kepentingan TIK di Universitas Sam Ratulangi berada pada level Tinggi (Skor: 27).
2) Sementara dari tingkat kelengkapan penerapan SMKI, Universitas Sam Ratulangi berada pada level "Tidak Layak", area "Merah" dengan total skor 191, yang merupakan jumlah dari seluruh skor rata-rata di setiap area Keamanan Informasi yang dievaluasi.

Tingkat kelengkapan penerapan SMKI juga dapat dilihat pada gambar 3 di atas, diagram berwarna merah muda merupakan kondisi SMKI Universitas Sam Ratulangi berdasarkan hasil pengisian kuesioner oleh para informan. Dapat dicermati bahwa:

1) Dari kelima area keamanan informasi yang diamati, tampak bahwa Universitas Sam Ratulangi telah memiliki Aspek Teknologi dan Tata Kelola yang jauh lebih baik dibanding area keamanan lainnya (paling mendekati standar yang ditetapkan dalam Proses Penerapan).
2) Pada Area Kerangka Kerja mencapai Kerangka Kerja Dasar. kecuali pada Area Pengelolaan Aset dan Pengelolaan Risiko tampak bahwa Universitas Sam Ratulangi tergolong tidak mencapai kerangka kerja dasar ini sangat perlu diperbaiki untuk meningkatkan pengamanan informasi.

Tingkat kelengkapan SMKI Universitas Sam Ratulangi berdasarkan hasil pengumpulan data Indeks KAMI menunjukkan pada area merah pada bar chart gambar 2 Pencapaian ini memberikan petunjuk bahwa SMKI yang ada memerlukan perbaikan pada sejumlah aspek.

Prioritas perbaikan aspek-aspek tersebut berdasarkan diagram radar gambar 3 dan persentase capaian skor informan pada tabel 2 adalah Kerangka Kerja Pengelolaan Keamanan Informasi, Tata Kelola Keamanan Informasi, Pengelolaan Aset Informasi, Teknologi Keamanan Informasi, dan Pengelolaan Risiko Keamanan Informasi.

Skor Kerangka kerja mempunyai nilai 31 dengan tingkat keamanan mencapai I+. Dari total 20 pertanyaan yang diajukan pada area ini, 0 diantaranya direspon "Tidak Dilakukan", 22 (85%) diantaranya direspon "Dalam Perencanaan", 4 (15%) diantaranya direspon "Dalam penerapan/Diterapkan Sebagian", dan sisanya 0 diantaranya direspon "Diterapkan Secara Menyeluruh". Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area ini, UNSRAT perlu melakukan perbaikan di antaranya:

1) Kebijakan dan prosedur keamanan informasi harus disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya.
2) Kebijakan keamanan informasi harus ditetapkan secara formal, dipublikasikan kepada pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkan.
3) Menyediakan mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk

penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya.
4) Menyediakan mekanisme untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait.
5) Kebijakan dan prosedur keamanan informasi yang ada harus merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi.
6) Mencantumkan pelaporan insiden, menjaga kerahasiaan, haki, tata tertib penggunaan dan pengamanan asset.
7) Membuat konsekwensi dari pelanggaran kebijakan keamanan informasi yang sudah didefinisikan, dikomunikasikan dan ditegakkan.
8) Membuat prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi.
9) Menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi security patch, alokasi tanggung jawab untuk memonitor adanya rilis security patch baru, memastikan pemasangannya dan melaporkannya.
10) Menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul.
11) Menerapkan kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (business continuity planning) yang mendefinisikan persyaratan/konsideran keamanan informasi, termasuk penjadwalan uji-cobanya.
12) Melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada.

Skor pengelolaan resiko keamanan informasi dengan nilai 23. Dari total 15 pertanyaan yang diajukan pada area ini, 0 diantaranya direspon "Tidak Dilakukan", 8 (53%) diantaranya direspon "Dalam Perencanaan", 7 (47%) diantaranya direspon "Dalam penerapan/Diterapkan Sebagian", dan sisanya 0 diantaranya direspon "Diterapkan Secara Menyeluruh". Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area ini, UNSRAT perlu melakukan perbaikan di antaranya:

1) Membuat kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan.
2) Membuat kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap Instansi.
3) Menetapkan ambang batas tingkat risiko yang dapat diterima.
4) Mendefinisikan kepemilikan dan pihak pengelola (custodian) aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut.
5) Menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi).
6) Memantau status penyelesaian langkah mitigasi risiko secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya.
7) Melakukan evaluasi terhadap penyelesaian langkah mitigasi yang sudah diterapkan untuk memastikan konsistensi dan efektifitasnya.
8) Mengkaji ulang secara berkala profil risiko berikut bentuk mitigasinya untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru.

Skor tata kelola dengan nilai 38. Dari total 20 pertanyaan yang diajukan pada area ini, 0 diantaranya direspon "Tidak Dilakukan", 8 (40%) diantaranya direspon "Dalam Perencanaan", 8 (40%) diantaranya direspon "Dalam penerapan/Diterapkan Sebagian", dan sisanya 4 (20%) diantaranya direspon "Diterapkan Secara Menyeluruh". Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area ini, UNSRAT perlu melakukan perbaikan di antaranya:

1) Mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi.
2) Menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi.
3) Pengelola keamanan informasi harus menerapkan dan menjamin kepatuhan pengamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (aparat keamanan).
4) Mendefinisikan dan mengalokasikan tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (business continuity dan disaster recovery plans).

Skor pengelolaan aset Keamanan informasi dengan nilai 50. Dari total 34 pertanyaan yang diajukan pada area ini, 1 (3%) diantaranya direspon "Tidak Dilakukan", 22 (65%) diantaranya direspon "Dalam Perencanaan", 11 (32%) diantaranya direspon "Dalam penerapan/Diterapkan Sebagian", dan sisanya 0 diantaranya direspon "Diterapkan Secara Menyeluruh". Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area ini, UNSRAT perlu melakukan perbaikan di antaranya:

1) Membuat Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.
2) Mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi Instansi dan keperluan pengamanannya.
3) Menyediakan tingkatan akses yang berbeda dan matrix yang merekam alokasi akses.
4) Menyediakan pengelolaan perubahan terhadap sistem (termasuk perubahan konfigurasi) yang diterapkan secara konsisten.
5) Menyediakan pengelolaan konfigurasi yang diterapkan secara konsisten.

6) Membuat proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi.
7) Mendefinisikan tanggung jawab pengamanan informasi secara individual untuk semua personil.
8) Membuat Tata tertib pengamanan dan penggunaan aset Instansi terkait HAKI, Peraturan pengamanan data pribadi.
9) Menetapkan waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data.
10) Membuat Prosedur penghancuran data/aset yang sudah tidak diperlukan
11) Membuat Prosedur kajian penggunaan akses (user access review) dan langkah pembenahan apabila terjadi ketidak sesuaian (non-conformity) terhadap kebijakan yang berlaku.
12) Menerapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis dan dapat mencegah upaya akses oleh pihak yang tidak berwenang.
13) Membuat proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik.
14) Membuat peraturan pengamanan perangkat komputasi milik Instansi apabila digunakan di luar lokasi kerja resmi (kantor).
15) Menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai untuk konstruksi ruang penyimpanan perangkat pengolah informasi penting.
16) Membuat proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting.
17) Membuat mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga.
18) Membuat peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya (misalnya larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll).

Skor teknologi keamanan informasi dengan nilai 49. Dari total 24 pertanyaan yang diajukan pada area ini, 2 (8%) diantaranya direspon "Tidak Dilakukan", 7 (29%) diantaranya direspon "Dalam Perencanaan", 15 (63%) diantaranya direspon "Dalam penerapan/Diterapkan Sebagian", dan sisanya 0 diantaranya direspon "Diterapkan Secara Menyeluruh". Untuk meningkatkan tingkat kelengkapan penerapan SMKI di area ini, UNSRAT perlu melakukan perbaikan di antaranya:

1) Melindungi dengan lebih dari 1 lapis pengamanan layanan TIK (sistem komputer) yang menggunakan internet.
2) Menganalisis kepatuhan penerapan konfigurasi standar yang ada secara rutin.
3) Menganalisis semua log secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik).
4) Menerapkan standar dalam menggunakan enkripsi.
5) Menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya.

V. PENUTUP

5.1 Kesimpulan

Berdasarkan penelitian yang dilakukan di Universitas Sam Ratulangi Manado untuk mengukur Tingkat Keamanan Informasi dengan Menggunakan Indeks (KAMI) maka dapat diambil kesimpulan dari tugas Akhir ini adalah:

1) Tingkat kematangan keamanan informasi di Universitas Sam Ratulangi masih tergolong rendah dan butuh perbaikan walaupun peran/tingkat ketergantungan akan TIK tergolong Tinggi. Pada aspek Teknologi dan Tata Kelola jauh lebih baik dibanding area keamanan lainnya. Hal sebaliknya terjadi pada Area Pengelolaan Aset dan Pengelolaan Risiko yang skornya masih rendah.
2) Skor akhir Indeks KAMI di Universitas Sam Ratulangi adalah 191 dari 588 skor maksimum atau 32.48%. Dengan skor ini, Universitas Sam Ratulangi tergolong Tidak cukup untuk mencapai standar keamanan yang baik.

5.2 Saran

Berikut adalah saran yang dapat disampaikan dalam tugas akhir ini untuk menjawab sejumlah tantangan yang harus dihadapi terkait penerapan SMKI sebagai berikut:

1) Melaksanakan sejumlah program peningkatan awareness pimpinan dan pejabat tentang arti penting SMKI, baik dari sisi aturan maupun penerapannya, seperti program sosialisasi, internalisasi, workshop, seminar dan pelatihan terkait keamanan informasi dengan melibatkan pihak yang terkait dengan harapan bahwa pengembangan SMKI dapat menjadi bagian dari Rencana Strategis.
2) Menyempurnakan SOP di lingkungan Universitas Sam Ratulangi untuk mendukung peralihan proses bisnis dari *paper-based* menjadi *technology-based* administration sekaligus untuk menumbuhkembangkan budaya pendokumentasian data dan informasi di lingkungan Universitas Sam Ratulangi.
3) Membuat Bentuk pengamanan secara keseluruhan walaupun belum dapat dibuktikan efektivitasnya.
4) Langkah yang wajib dilakukan untuk naik ke tingkat selanjutnya:
   a. Menerapkan Pengamanan walaupun sebagian besar di area teknis dan membuat langkah pengamanan untuk mendapatkan strategi yang efektif.
   b. Proses pengamanan berjalan walaupun tanpa dokumentasi atau rekaman resmi.
   c. Langkah pengamanan operasional sudah diterapkan walaupun bergantung kepada pengetahuan dan motivasi individu pelaksana.

DAFTAR REFERENSI

[1] KOMINFO. (2017). "Audisi Pertama "*Born to Protect*", Jaring Bakat Cyber Security Indonesia". Diambil dari: *https://kominfo.go.id/content/detail/10363/audisi-pertama-born-to-protect-jaring-bakat-cyber-security-indonesia/0/berita_satker*

[2] Direktorat Keamanan Informasi, Kementerian Komunikasi dan Informatika. (2011). "Panduan Penerapan Tata Kelola Keamanan Informasi bagi Penyelenggara Pelayanan Publik". Jakarta, Indonesia.

[3] Infosecurity. (2011). Infosecurity – "*Many small businesses lack basic information security practices". Diambil kembali dari Info Security Magazine: http://www.infosecurity-magazine.com/view/18774/manysmall-businesses-lack-basic-information-security-practices/*

[4] IBISA. (2011). "Keamanan Sistem Informasi". Andi. Yogyakarta. Indonesia.

[5] Badan Standarisasi Nasional, (2009). "ISO IEC 27001 Teknologi Informasi – Teknik Keamanan – Sistem Manajemen Keamanan Informasi – Prasyaratan". Jakarta, Indonesia.

[6] Rashid Ridho, (2012). "Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan SNI ISO/IEC 27001:2009 Studi Kasus: Bidang Aplikasi dan Telematika Dinas Komunikasi Dan Informatika Surabaya". Institut Teknologi Sepuluh Nopember (ITS), Surabaya, Indonesia.

[7] Tedi Agoan, Hans F. Wowor dan Stanley Karouw, (2017). "Analisa Tingkat Kematangan Teknologi Informasi Pada Dinas Komunikasi Dan Informatika Kota Manado Menggunakan Framework COBIT 5 Domain Evaluate, Deirect, Monitor (EDM) dan Deliver, Service, and Support (DSS)". Universitas Sam Ratulangi. Manado, Indonesia.

[8] Brian Gamaliel, Yaulie Rindengan dan Stanley Karouw, (2017). "Pengukuran Tingkat Keselarasan Tata Kelola Teknologi Informasi Menggunakan *Cobit 5* Pada Pemerintah Sulawesi Utara". Universitas Sam Ratulangi. Manado, Indonesia.

[9] Mufti Rizal and Yudho Giri Sucahyo. (2013). "*A Study on the Preparedness of Information Security Framework Area based on the Assessment of Information Security Index in Ministry of XYZ*". Universitas Indonesia Jakarta, Indonesia.

[10] Edit Prima, Yudho G. Sucahyo, dan Zainal A. Hasibuan. (2013). "*Mapping the Certification Authority for e-Government Procurement System into eGovAMAN Framework*". Universitas Indonesia. Jakarta, Indonesia.

[11] Adi Muhajirin. (2012). "Kajian Tingkat Kematangan Sistem Manajemen Keamanan Informasi Studi Kasus: Suku Dinas Komunikasi Dan Informatika Jakarta Selatan". STMIK Nusa Mandiri. Jakarta, Indonesia.

SEKILAS TENTANG PENULIS

Saya bernama Muh. Faturachman Husin dan merupakan anak tunggal dari pasangan Aulia Husin dan Zuraidah Sukur, lahir di Ambon pada tanggal 3 Oktober1995. Asal daerah Ternate.

Saya mulai menempuh pendidikan di sekolah dasar SD Pertiwi 1 Ternate (2000 - 2007). Kemudian melanjutkan studi tingkat pertama di SMPN 1 Ternate (2007 - 2010) dan selanjutnya saya menempuh pendidikan tingkat atas di SMAN 1 Ternate (2010 - 2013).

Setelah itu, di tahun 2013 saya melanjutkan pendidikan ke salah satu perguruan tinggi yang berada di Manado yaitu Universitas Sam Ratulangi Manado, dengan mengambil Program Studi S-1 Teknik Informatika di Jurusan Elektro Fakultas Teknik.