JURNAL SAINS DAN INFORMATIKA
RESEARCH OF SCIENCE AND INFORMATIC V5.I2

Vol.5No.2(2019)108-113 **p-issn : 2459-9549**
http://ejournal.kopertis10.or.id/index.php/sains **e-issn : 2502-096X**

Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi di LPPM AMIK Jayanusa

Isnardi
Manajemen Informatika, AMIK Jayanusa, is_adasaja@yahoo.com

Submitted: 21-11-2019, Reviewed: 22-11-2019, Accepted 28-11-2019
http://doi.org/10.22216/jsi.v5i2.4785

Abstract
Information Management is one aspect of Good University Governance, including the quality and security of information management. One effort that can be done to improve the quality of information security, is the implementation of tools to measure the level of maturity and completeness in information security called the Information Security Index (KAMI). The use of the US Index is also followed by the adoption of ISO 27001 as an international security standard that can help an organization ensure that the information security that is applied is effective. The information system used in LPPM AMIK Jayanusa has been threatened several times in the form of deface and others, after an improvement has been carried out an evaluation using the US index, the results of this study are the level of dependence of the use of electronic systems by 23 of the total score of 50 and into the category Height where the electronic system is an inseparable part of the work process that is running. The results of the assessment of the five areas that have been carried out are 248 out of 645 and are in the inappropriate category. Recommendations from this study can be used as material for consideration and evaluation for the LPPM AMIK Jayanusa in making improvements relating to information security mitigation.
Keywords : Information Systems Security, index KAMI, Risk Management

Abstrak
Pengelolaan Informasi merupakan salah satu aspek dalam Good University Governance, termasuk kualitas dan keamanan pengelolaan informasi. Salah satu upaya yang dapat dilakukan untuk meningkatkan kualitas dari keamanan informasi, adalah implementasi alat bantu untuk mengukur tingkat kematangan dan kelengkapan dalam keamanan informasi yang disebut dengan Indeks Keamanan Informasi (KAMI). Penggunaan Indeks KAMI ini juga diikuti dengan penerapan ISO 27001 sebagai standar keamanan internasional yang dapat membantu sebuah organisasi memastikan keamanan informasi yang diterapkan sudah efektif. Sistem Informasi yang di gunakan di LPPM AMIK Jayanusa pernah beberapa kali mendapatkan ancaman berupa *deface* dan lainnya, setelah di lakukan perbaikan di lakukan evaluasi dengan menggunakan indeks KAMI, Hasil penelitian ini adalah tingkat ketergantungan penggunaan sistem elektronik sebesar 23 dari total skor 50 dan masuk kedalam kategori Tinggi dimana sistem elektronik adalah bagian yang tidak terpisahkan dari proses kerja yang berjalan. Hasil penilaian kelima area yang telah dilakukan adalah sebesar 248 dari 645 dan berada pada kategori tidak layak. Rekomendasi dari penelitian ini dapat dijadikan sebagai bahan pertimbangan dan evaluasi bagi pihak LPPM AMIK Jayanusa dalam melakukan perbaikan yang berkaitan dengan mitigasi keamanan informasi.

Kata Kunci: Keamanan Sistem Informasi, indeks kami, Manajemen Resiko

1. Pendahuluan

Perkembangan teknologi informasi pada era digital saat ini semakin pesat, berbagai kemudahan dalam kehidupan bisa dinikmati hari ini yang sebelumnya tidak pernah terpikirkan. Seiring dengan itu kejahatan di dunia digital juga meningkat.Instansi Pemerintah maupun swasta sudah yang sudah dan akan menerapkan penggunaaan teknologi informasi dan sistem informasi mulai memperhatikan sistem keamanan teknologi informasi dan sistem informasi yang mereka gunakan karena fakta yang mengejutkan datang dari perusahaan monitoring internet Akamai yang mengungkap bahwa kejahatan internet di Indonesia meningkat dua kali lipat. Angka ini

menempatkan Indonesia di posisi pertama negara berpotensi menjadi target hacker, menggantikan Tiongkok. Dari 175 negara yang diinvestigasi, Indonesia berkonstribusi sebanyak 38 persen dari total sasaran trafik hacking di internet. Angka ini meningkat seiring dengan meningkatnya kecepatan internet di Indonesia(Ardiyanti, 2014)

Begitu juga dengan LPPM AMIK Jayanusa dimana penelitian ini di lakukan. Institusi ini adalah sebuah Perguruan Tinggi yang sudah mengelolah proses Pengajaran, Penelitian dan Pengabdian Kepada Masyarakat (Tridarma) menggunakan teknolgoi informasi. Pada penelitian ini dikhususkan padan Lembaga Penelitian dan Pengabdian Masyarakat di institusi ini, karena sudah menerapkan sistem informasi untuk pengolahan data penelitian dan pengabdian, di kampus tersebut, dalam penerapan sistem sudah terjadi beberapa kali serangan *Cyber* yang menyerang komputer *server* tempat implementasi sistemdi institusi ini.Hal tersebut tentu saja dapat mengganggu kelancaran proses tri darma di institusi ini, dimana dengan terjadinya serangan terhadap sistem yang dimiliki akan menyebabkan terkendalanya sistem yang ada dalam instutisi tersebut dan dapat menimbulkan kerugian dari sisi materil, oleh karena itu perlunya di terapkan keamanan informasi untuk menghindari adanya pencurian data dan hilangnya data secara sengaja maupun tidak sengaja. (Basyarahil, Astuti, & Hidayanto, 2017)

Keamanan data secara tidak langsung dapat memastikan kontinuitas bisnis, mengurangi resiko, mengoptimalkan *return on investment* dan mencari kesempatan bisnis. Semakin banyak informasi perusahaan yang disimpan, dikelola dan di-sharing maka semakin besar pula resiko terjadinya kerusakan, kehilangan atau tereksposnya data ke pihak eksternal yang tidak diinginkan(Fitriansyah & Budiarto, 2012)

Pemerintah Indonesia melalui Kementerian Komunikasi dan Informatika (Kemkominfo) telah menghimbau kepada seluruh instansi pemerintahan, baik itu pusat maupun daerah, sebagai badan penyelenggara layanan publik untuk meningkatkan kesadaran akan pentingnya keamanan informasi. Berbagai cara dilakukan untuk meningkatkan kesadaran bagi aparatur negara tentang keamanan informasi, mulai dari sosialiasasi maupun bimbingan teknis (bimtek). Sosialisasi yang dilakukan berisikan materi-materi tentang definisi, pengertian, kontrol-kontrol, persyaratan dokumentasi keamanan informasi dan contoh-contoh tindakan untuk mengamankan informasi. Sementara pada setiap bimbingan teknis, dijelaskan metode atau cara melakukan penilaian mandiri (*self assessment*) terhadap status keamanan informasi pada masing-masing instansi menggunakan alat bantu berupa perangkat penilaian yang bernama indeks Keamanan Informasi (KAMI). Alat evaluasi Indeks KAMI 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. Indeks KAMI dapat digunakan mengevaluasi tingkat kematangan, tingkat kelengkapan penerapan SNI ISO/IEC 27001 serta peta area tata kelola keamanan sistem informasi di suatu instansi dan standar komprehensif yang membantu institusi dalam mencapai tujuan dan menghasilkan nilai melalui tata kelola dan manajemen teknologi informasi yang efektif.(*Astri F. Manullang1 , Candiwan2 , Listyo Dwi Harsono3*, 2017). Pada penelitian ini dilihat/dievavaluasi kesiapan LPPM AMIK Jayanusa dalam penerapan keamanan sistem informasi dengan menggunakan indeks KAMI.

2. Tinjauan Pustaka/Penelitian Sebelumnya

Terdapat dua penelitian terdahulu tentang keamanan teknologi informasi yang dijadikan rujukan dalam penelitian ini. Adanya tinjauan terhadap beberapa penelitian terdahulu ini bertujuan agar dapat memberikan gambaran umum yang memberikan manfaat bagi pelaksanaan penelitian. Berikut uraian beberapa penelitian terdahulu yang digunakan sebagai acuan dalam penelitian ini.

Jurnal pertama penelitian tentang Analisa Tingkat Kesiapan Penerapan Keamanan Teknologi Informasi Dalam Pelaksanaan *E-Government* Berbasis Indeks Keamanan Informasi (Kami) Studi Kasus Pemerintah Kota Kediri kesimpulan dari penelitian ini adalah Penerapan atau tingkat kematangan keamanan sistem di Pemerintah Kota Kediri masuk ke dalam katagori tidak layak, terutama di bidang pengelolaan resiko dengan nilai 18. Skor Maksimal dari Indeks KAMI adalah 588 dan Pemerintah Kota kediri berada di Skor 308. Dengan tingkat penggunaan Sistem Elektronik yang berada di level Tinggi. Dapat dikatakan sistem Keamanan yang digunakan di Pemerintah Kota Kediri tidak memadai. (Primakara, 2017)

Jurnal kedua Asesmen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (Kami) pada Institusi Xyz, Institusi XYZ adalah institusi yang mempunyai tugas menyelenggarakan urusan dibidang pemerintahan. Institusi XYZ menggunakan sistem informasi yang dapat diakses oleh pegawai kepemerintahan maupun masyarakat umum. Pada institusi XYZ terdapat bidang PUSDATIN (Pusat Data dan Informasi) yang berfungsi untuk mengelola layanan informasi kepada masyarakat maupun operasional sehari-hari dilingkungan institusi tersebut.

Informasi dikelola secara elektronik untuk mewujudkan *good governance* , sehingga terdapat keterbukaan informasi bagi masyarakat dan pertukaran informasi antar institusi yang saling terkoneksi. Data – data yang diproses pada bidang PUSDATIN terkoneksi

dengan jaringan *computer*. Kesimpulan yang dapat diperoleh dari penelitian ini adalah sebagai berikut:

- Hasil dari penilaian tingkat penggunaan Sistem Elektronik adalah sebesar 32 dari jumlah total keseluruhan sebesar 50. Hal ini menunjukkan bahwa institusi XYZ sudah masuk dalam kategori tinggi dalam penggunaan sistem elektronik yang berarti penggunaan sistem elektronik merupakan bagian yang tidak dapat terpisahkan dari proses kerja yang berjalan pada institusi XYZ.

Hasil skor keseluruhan berdasarkan penilaian kelima area dalam Indeks KAMI institusi XYZ memperoleh skor sebesar 153 dari total keseluruhan 645 dan berada pada level kematangan dimana kondisi ini merupakan kondisi awal penerapan keamanan informasi. Dalam hal ini Institusi XYZ belum layak dalam penerapan sistem manajemen keamanan informasi untuk melindungi aset yang dimiliki, sehingga masih rentan terhadap tindak kejahatan komputer yang dapat mengakibatkan terganggunya pelayanan sistem informasi di institusi XYZ. Adapun saran yang dapat penulis sampaikan terkait dengan sistem manajemen keamanan informasi untuk institusi XYZ dalam melindungi aset yang dimiliki adalah sebagai berikut: - Institusi XYZ harus meningkatkan sistem manajemen keamanan informasi karena tingkat Kategori Sistem Elektronik yang tinggi dan nilai aset yang dimiliki untuk mencegah atau menanggulangi tindak kejahatan komputer yang dapat mengakibatkan terganggunya pelayanan sistem informasi pada institusi XYZ. Pengelolaan keamanan informasi yang telah ada harus dilakukan perbaikan dan peningkatan kontrol keamanan dengan pembuatan kebijakan dan prosedur keamanan informasi yang sesuai dengan kondisi TI/SI institusi dengan memperhatikan kesiapan, sumber daya yang dimiliki untuk mendapatkan penerapan sistem manajemen keamanan informasi yang efektif dan efisien.

Dari kedua jurnal tersebut evaluasi di lakukan di bidang pemerintahan dengan nilai evaluasi akhir Tidak layak, dan indeks KAMI yang di gunakan adalah versi 3.0. Tidak layak disini maksudnya dari sisi permasalahan kemanan bukan dari sisi teknologi dan sistem yang digunakan.

Pengertian Informasi

Informasi informasi adalah data yang diolah menjadi bentuk yang lebih berguna dan lebih berarti bagi penerimanya(Asmara, 2018)

Resiko Keamanan Informasi

Perkembangan teknologi yang pesat dan pola bisnis yang dinamis menyebabkan munculnya risiko keamanan informasi baru. Keterlibatan pihak ketiga dalam rantai pasok (*supply chain*) layanan suatu instansi/perusahaan menimbulkan risiko terkait keberadaan/keterlibatan pihak eksternal tersebut. Layanan berbasis infrastruktur awan (*Cloud*) memberikan peluang efisiensi dan peningkatan kinerja yang sangat signifikan bagi instansi/perusahaan, akan tetapi risiko terkait data yang berada pada pengendalian pihak ketiga (penyelenggara layanan) perlu dimitigasi. Sedangkan disahkannya peraturan terkait perlindungan data pribadi oleh banyak negara memerlukan kerangka kerja yang secara spesifik membahas bagaimana data pribadi yang ada/digunakan dalam instansi/perusahaan diamankan sesuai dengan persyaratan hukum. Butir-butir evaluasi kesiapan pengamanan yang disusun untuk setiap area merupakan persyaratan dasar yang bagi instansi/perusahaan yang terpapar risiko terkait ketiga area tersebut.Hasil penilaian evaluasi kesiapan Pengamanan Keterlibatan Pihak Ketiga, Pengamanan Layanan Infrastrukutur *Cloud* dan Perlindungan Data Pribadi disampaikan dalam bentuk *persentase* (%) dengan obyektif/sasaran pencapaian maksimal.

3. Metodologi Penelitian

3.1 Tahap pendahuluan

Tahapan pendahuluan ini ada beberapa langkah-langkah yang dijalankan, antara lain:

a. Perumusan masalah Tahapan ini digunakan untuk menentukan pokok permasalahan yang ditemukan dari perlakuan studi pendahuluan, yaitu untuk melihat kondisi sejauhmana kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi.

b. Penetapan tujuan dan batasan Setelah adanya perumusan masalah yang telah teridentifikasi dilakukan penetapan tujuan dan batasan dalam lingkup pengerjaan penelitian

c. Mengetahui kondisi kekinian yang berhubungan dengan keamanan informasi di LPPM AMIK Jayanusa. Langkah ini dilakukan untuk observasi pada kondisi kekinian yang berkaitan dengan keamanan informasi yang ada pada LPPM institusi ini yang meliputi kajian tentang permasalahan terkini yang terjadi, kelengkapan dokumentasi yang berkaitan dengan menjaga keamanan informasi, infrastruktur dan proses bisnis yang dilakukan organisasi dan hal-hal pendukung lainnya yang berkaitan dengan penelitian ini. Tahapan ini dilakukan dengan observasi secara langsung dan pengumpulan data dan informasi dari berbagai pihak yang terkait

d. Studi Lapangan

Melakukan pengamatan secara langsung terhadap objek yang muncul dalam studi kasus. Dalam hal ini

melingkupi hal-hal yang ada pada studi kasus LPPM institusi ini

e. Studi literature Digunakan untuk dasar dalam melakukan penelitian dengan cara mencari sumber-sumber pendukung yang berupa jurnal penelitian, buku, *e-book* yang berkaitan dengan keamanan informasi.

f. Pengumpulan data dokumen Langkah selanjutnya adalah pengumpulan data-data yang dibutuhkan baik itu berupa dokumen atau bukti pendukung lainnya. Temuan tersebut digunakan untuk mendukung pengerjaan penelitian.

3.2 Tahap Evaluasi

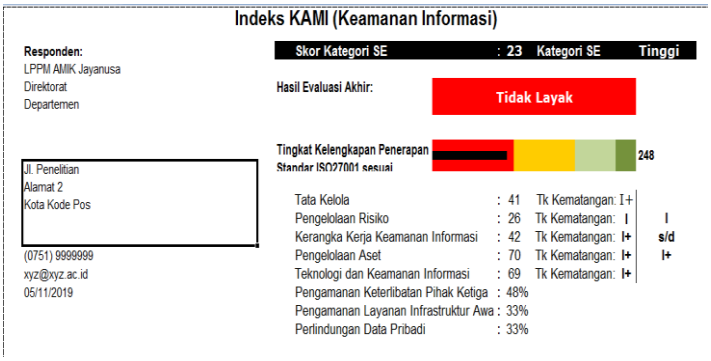
Mengkaji penetapan peran atau tingkat kepentingan TIK Langkah awal yang dilakukan untuk melakukan penilaian menggunakan indeks KAMI adalah dengan melakukan klasifikasi terlebih dahulu terhadap peran TIK didalam instansi tersebut

3.3 Menilai kelengkapan keamanan informasi dan mengkaji hasil indeks KAMI

4. Hasil dan Pembahasan

Pada penerapan indeks kami hal pertama yang dinilai disini adalah :

a. Tingkat ketergantungan kategori sistem elektronik, dimana pada skor akhir di dapatkan hasil 23, yang artinya tingkat ketergantungan LPPM instiutsi ini terhadap penggunaan teknologi tinggi.
b. Tata Kelola keamanan Informasi, Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi. Pada bagian ini LPPM institusi ini dengan skor 41, yang berarti Tidak Valid.
c. Pengelolaan Resiko Keamanan, Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi. Pada bagian ini LPPM institusi ini memperoleh nilai 26 yang artinya Tidak Valid.
d. Kerangka Kerja Pengelolaan Informasi, Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya. Pada bagian ini LPPM institusi ini memperoleh nilai 42 artinya Tidak Valid.
e. Pengelolaan Aset Informasi, Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut. Pada bagian ini LPPM institusi ini memperoleh nilai 70, yang artinya Tidak Valid.
f. Teknologi dan Keamanan Informasi, Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi. Pada bagian ini institusi ini memperoleh nilai 69 yang artinya tidak Valid.
g. Suplemen, Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi. Pada bagian ini LPPM institusi ini memperoleh nilai pada masing-masingnya rata-rata bernilai 1 dan 2, artinya bernilai dalam perencanaan atau dalam penerapan/penerapan sebahagian.
h. Dari keseluruhan penilaian diatas dapat diambil kesimpulan bahwa hasil evaluasi akhir penilaian resiko keamanan menggunakan indeks KAMI versi 4.0 bahwa LPPM institusi ini, **Tidak Layak** untuk kondisi kesiapan (kelengkapan dan kematangan) **kerangka kerja keamanan informasi** tetapi Sangat layak untuk Sistem informasi yang di gunakan seperti terlihat pada laporan berikut ini :



Gambar 4.1: Hasil penilaian Evaluasi akhir

Sedangkan hasilnya juga bisa dilihat dalam bentuk grafik seperti berikut ini

Gambar 4.2 : Grafik hasil evaluasi akhir

5. Kesimpulan

Kesimpulan yang dapat diperoleh dari penelitian ini adalah terkait penilaian manajemen keamanan informasi pada LPPM institusi AMIK Jayanusa dengan menggunakan Indeks Keamanan Informasi (KAMI) versi 4.0 adalah sebagai berikut:

a. Implementasi atau tingkat kematangan keamanan sistem di LPPM institusi ini sesuai dengan hasil penelitian ini masuk ke dalam katagori **tidak layak**, terlihat dari hasil penilaian tingkat penggunaan Sistem Elektronik adalah sebesar 23 dari jumlah total keseluruhan sebesar 45. Hal ini menunjukkan bahwa institusi ini sudah masuk dalam kategori tinggi dalam penggunaan sistem elektronik yang berarti penggunaan sistem elektronik merupakan bagian yang tidak dapat terpisahkan dari proses kerja yang berjalan pada LPPM institusi ini.
b. Hasil evaluasi akhir berdasarkan penilaian kelima area dalam Indeks KAMI4.0, di LPPM AMIK Jayanusa memperoleh skor sebesar 248 total keseluruhan dan berada pada level kematangan I+ dimana kondisi ini merupakan kondisi awal penerapan keamanan informasi. Dalam hal ini Institusi ini belum layak dalam penerapan sistem manajemen keamanan informasi tentu saja hal ini akan membuat institusi ini, harus berbenah dalam meningkatkan kesiapan keamanan supaya proses bisnis tidak terganggu dengan adanya berbagai gangguan yang bisa muncul seiring perkembangan teknologi yang semakin pesat. Adapun saran yang dapat peneliti sampaikan terkait dengan sistem manajemen keamanan informasi untuk LPPM institusi ini dalam melindungi aset yang dimiliki adalah sebagai berikut:
    a. LPPM AMIK JAyanusa harus meningkatkan sistem manajemen keamanan informasi karena tingkat Kategori Sistem Elektronik yang tinggi (Semua proses sudah terkomputerisasi) dan nilai aset yang dimiliki untuk mencegah atau menanggulangi tindak kejahatan komputer yang dapat mengakibatkan terganggunya pelayanan sistem informasi pada institusi ini.
    b. Pengelolaan keamanan informasi yang telah ada harus dilakukan perbaikan dan peningkatan kontrol keamanan dengan pembuatan kebijakan dan prosedur keamanan informasi yang sesuai dengan kondisi TI/SI institusi dengan memperhatikan kesiapan, sumber daya yang dimiliki untuk mendapatkan penerapan sistem manajemen keamanan informasi yang efektif dan efisien
    c. Indeks KAMI sebaiknya digunakan 2X dalam setahun sebagai alat untuk melakukan tinjauan ulang kesiapan keamanan informasi di LPPM institusi ini sekaligus untuk mengukur keberhasilan inisiatif perbaikan yang diterapkan, dengan pencapaian tingkat kelengkapan atau kematangan tertentu.
    d. Sebaiknya indeks KAMI juga di implementasian di bidang lainnya, sehingga akan tercipta teknologi informasi dan sistem informasi yang sangat kuat di bidang keamanan.
    e. Keamanan informasi, adalah awal dari keamanan proses bisnis yang lainnya di zaman digital ini, maka dalam membangun infrastruktur teknologi informasi dan sistem informasi, harus dijadikan masalah nomor satu yang menjadi perhatian pimpinan, pengguna dan pengembang.

UCAPAN TERIMA KASIH

Ucapan terima kasih saya sampaikan kepada Pimpinan LPPM AMIK Jayanusa dan teman-teman yang membantu proses penyelesaian penelitian ini dan terbitnya jurnal ini. Semoga jurnal ini bermanfaat bagi peneliti lain maupun pihak yang membutuhkan.

6. Daftar Rujukan

[1]. Ardiyanti, H. (2014). Cyber-security dan tantangan pengembangannya di indonesia. *Politica*, *5*(1), 95–110.
[2]. Asmara, R. (2018). JURNAL J – CLICK. *J-Click*, *5*(2), 320–336.
[3]. *Astri F. Manullang1 , Candiwan2 , Listyo Dwi Harsono3*.

(2017). JIEET: Volume 01 Nomor 02, 2017 (Journal Information Engineering and Educational Technology).

[4]. Basyarahil, F. A., Astuti, H. M., & Hidayanto, C. (2017). *Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya*. *6*(1).

[5]. Fitriansyah, A., & Budiarto, H. (2012). *Tata kelola keamanan informasi berbasis iso/iec 27001:2005*. *VIII*(2), 18–32.

[6]. Primakara, S. (2017). *Keamanan Teknologi Informasi Dalam Pelaksanaan E-Government Berbasis Indeks Keamanan Informasi (Kami) Studi Kasus Pemerintah Kota Kediri*. 21–27.