

EVALUASI TINGKAT KEAMANAN INFORMASI SEBAGAI UPAYA PENINGKATAN KEAMANAN SISTEM INFORMASI AKADEMIK DI SEKOLAH TINGGI TEKNIK QOMARUDDIN GRESIK MENGGUNAKAN INDEKS KEAMANAN INFORMASI

Nur Abidin¹⁾, Mohamad Hariyadi²⁾

^{1, 2)}Program Studi Teknik Informatika dan Program Studi Teknik Elektro Universitas Qomaruddin
e-mail: nurabidin@uqgresik.ac.id¹⁾, mohamadhariyadi@uqgresik.ac.id²⁾

ABSTRAK

Penelitian ini bertujuan untuk mengevaluasi keamanan sistem informasi akademik di Sekolah Tinggi Teknik Qomaruddin Gresik menggunakan indeks keamanan informasi (KAMI). Penggunaan Indeks keamanan informasi dikarenakan telah memenuhi kelengkapan dan kematangan yang sesuai dengan Standar Nasional Indonesia (SNI). Penelitian ini dilakukan dengan menggunakan metode survei, interview serta observasi langsung. Berdasarkan hasil evaluasi tersebut telah didapatkan tingkat kesiapan penerapan pengamanan sebesar 187 dari total 645, atau sekitar 28,99%. Sedangkan tingkat kematangannya I s/d I⁺.

Kata Kunci: Indeks Keamanan Informasi (KAMI), ISO/IEC 27001, Keamanan Sistem Informasi.

ABSTRACT

This study aims to evaluate the security of academic information systems in the Qomaruddin Gresik Technical High School using the information security index (KAMI). The use of the information security index is because it has met the completeness and maturity in accordance with the Indonesian National Standard (SNI). This research was conducted using survey methods, interviews and direct observation. Based on the results of the evaluation, it was found that the level of security application readiness was 187 out of a total of 645, or around 28.99%. While the maturity level is I to I⁺.

Keywords: Information Security Index (KAMI), Information Systems Security, ISO / IEC 27001.

I. PENDAHULUAN

Pentingnya teknologi informasi membuat teknologi informasi menjadi teknologi yang banyak diadopsi di hampir seluruh organisasi. Pengadopsian teknologi informasi digunakan mulai dari pekerjaan ditingkat operasional sampai dengan tingkat strategis untuk pengambilan keputusan. Pengadopsian tersebut memiliki tujuan untuk meningkatkan efisiensi serta sebagai keunggulan kompetitif bagi organisasi. Hal tersebut dapat tercapai jika dalam penerapannya disertai dengan pengelolaan yang baik sesuai dengan standar. Jika tidak, maka pengadopsian teknologi informasi dapat membahayakan bagi organisasi itu sendiri. Bahaya yang bisa saja terjadi salah satunya adalah kebocoran data akibat lemahnya keamanan informasi pada teknologi informasi tersebut[8].

Sekolah Tinggi Teknik Qomaruddin (STTQ) adalah sekolah tinggi teknik yang ada di Kabupaten Gresik. Sekolah Tinggi Teknik Qomaruddin memanfaatkan teknologi informasi untuk administrasi data pembelajaran perguruan tinggi. Data tersebut antara

lain; data dosen, data mahasiswa, data mata kuliah, data jadwal perkuliahan, data perencanaan studi, data perwalian, dan data hasil studi. Data-data tersebut diinput dan diproses oleh sebuah sistem informasi. Di Sekolah Tinggi Teknik Qomaruddin, sistem informasi yang bertugas untuk mengolah data-data tersebut adalah sistem informasi akademik (SIKAD). Di dalam SIKAD terdapat data sensitif berupa data nilai akademik hasil studi mahasiswa (KHS). Biro yang bertanggung jawab untuk mengelola sistem informasi akademik (SIKAD) di Sekolah Tinggi Teknik Qomaruddin adalah Biro Sistem Informasi (BSI). Terdapat dua divisi dalam BSI, Biro Pengembangan Sistem Informasi dan Pengolahan Data, dan Divisi Infrastruktur dan Jaringan.

Data dalam sebuah sistem informasi harus terjaga kerahasiaannya agar data tersebut terjamin kerahasiaannya, maka sistem informasi harus memiliki keamanan yang baik agar tidak terjadi masalah yang diinginkan. Menurut Matondang dan Kawan [6] keamanan merupakan salah satu aspek penting dari sebuah sistem informasi. Terjadinya masalah keamanan mengakibatkan kerugian. Kerugian-kerugian yang ditimbulkan oleh sistem yang

tidak aman, seperti; hilangnya data, perubahan data yang dilakukan oleh orang yang tidak memiliki hak, dan hilangnya hak akses terhadap sistem tentunya berdampak tidak baik bagi organisasi. Keamanan data menurut Fitriansyah dan Kawan [2] secara tidak langsung dapat memastikan keberlangsungan bisnis, mengurangi resiko serta dapat mengoptimalkan *return on investment* (ROI). Untuk dapat mengetahui tingkat keamanan sistem informasi, maka dibutuhkan sebuah evaluasi terhadap sistem informasi. Penelitian yang telah dilakukan oleh Abidin dan Saffana [7], dalam perencanaan strategis SI/TI di Sekolah Tinggi Teknik Qomaruddin Gresik yang menjadi prioritas utama strategi SI/TI adalah pentingnya penerapan keamanan sistem informasi.

Berdasarkan latar belakang tersebut, maka penelitian yang akan dilakukan terkait dengan kesiapan penerapan keamanan sistem informasi serta penilaian tingkat kematangan penerapannya. Untuk dapat melakukan evaluasi keamanan sistem informasi agar berjalan baik, maka dibutuhkan suatu standar yang digunakan untuk melakukan evaluasi tersebut. Standar yang digunakan dalam penelitian ini adalah indeks KAMI yang sesuai dengan standar SNI ISO/IEC 27001. Indeks KAMI merupakan alat bantu untuk menganalisa dan mengevaluasi tingkat kesiapan (kelengkapan dan kematangan) yang telah distandarisasi Badan Standar Nasional Indonesia (SNI) dan digunakan oleh Badan Siber dan Sandi Negara (BSSN) [1]. Hasil evaluasi dalam penelitian ini dijadikan referensi atau acuan untuk implementasi keamanan sistem informasi akademik (SIKAD) di Sekolah Tinggi Teknik Qomaruddin.

II. LANDASAN TEORI

A. Sistem Informasi

Sistem informasi adalah suatu sistem buatan manusia yang secara umum terdiri atas sekumpulan komponen berbasis komputer dan manual yang dibuat untuk menghimpun, menyimpan, dan mengolah data serta menyediakan informasi keluaran kepada pemakai [4]. Informasi-Informasi yang dihasilkan dari pengolahan data pada sebuah sistem memiliki peranan penting dalam pengelolaan sebuah organisasi. Menurut Raharjo [8], Informasi merupakan aset yang sangat berharga sehingga perlu dijamin keamanan oleh setiap organisasi. Setiap bagian dalam organisasi bergantung pada informasi yang dimiliki. Informasi tersebut diolah dari berbagai sumber yang ada, baik internal maupun eksternal organisasi. Kemudian disebarluaskan kepada setiap bagian organisasi sesuai dengan peruntukannya.

B. Sistem Informasi Akademik

Sistem Informasi Akademik adalah sebuah sistem yang dirancang untuk melakukan pengolahan data

akademik [13]. sistem informasi ini bertujuan untuk dapat membantu pelaksanaan pendidikan, sehingga perguruan tinggi dapat memberikan layanan informasi kepada mahasiswa dengan baik dan efektif melalui jaringan internet.

C. Keamanan Informasi

Menurut Yuliani dan Kawan [15] mendefinisikan keamanan informasi adalah informasi yang diterima harus dari sumber yang sebenarnya atau asli. Sedangkan menurut Whitman dan Mattord [14] di dalam bukunya mendefinisikan keamanan informasi merupakan usaha untuk melindungi komputer dan non peralatan komputer, fasilitas, data, dan informasi dari penyalahgunaan oleh orang yang tidak bertanggung jawab. Beberapa aspek yang perlu diperhatikan dalam usaha untuk mengamankan data [14] diantaranya:

1. *Physical Security* adalah keamanan informasi yang memfokuskan pada strategi untuk mengamankan individu atau anggota organisasi, aset fisik, dan tempat kerja dari berbagai ancaman meliputi bahaya kebakaran, akses tanpa otorisasi, dan bencana alam.
2. *Personal Security* adalah keamanan informasi yang berhubungan dengan keamanan personal. Biasanya saling berhubungan dengan ruang lingkup "*physical security*".
3. *Operation Security* adalah keamanan informasi yang membahas bagaimana strategi suatu organisasi untuk mengamankan kemampuan organisasi tersebut untuk beroperasi tanpa gangguan.
4. *Communications Security* adalah keamanan informasi bertujuan mengamankan media komunikasi, teknologi komunikasi, serta apa yang ada di dalamnya. Serta kemampuan untuk memanfaatkan media dan teknologi komunikasi untuk mencapai tujuan organisasi.
5. *Network Security* adalah keamanan informasi yang memfokuskan pada bagaimana pengamanan peralatan jaringan, data organisasi, jaringannya dan isinya, serta kemampuan untuk menggunakan jaringan tersebut dalam memenuhi fungsi komunikasi data organisasi.

D. International Standards Organization (ISO)

Menurut Kementerian Komunikasi dan Informatika, keamanan informasi bagi penyelenggara pelayanan publik adalah badan penyetap standar internasional yang terdiri dari wakil-wakil dari badan standardisasi nasional setiap negara. Didirikan pada 23 Februari 1947, *International Standards Organization* (ISO) menetapkan standar-standar industrial dan komersial dunia. Sejak tahun 2005, *International Organization for Standardization* (ISO) atau Organisasi Internasional untuk Standardisasi telah

mengembangkan sejumlah standar tentang *Information Security Management Systems* (ISMS) atau Sistem Manajemen Keamanan Informasi (SMKI) baik dalam bentuk persyaratan maupun panduan. Adapun beberapa standar di seri ISO menurut [11] adalah sebagai berikut:

1. ISO 27000: dokumen definisi-definisi keamanan informasi yang digunakan sebagai istilah dasar dalam serial ISO 27000.
2. ISO 27001: berisi aspek-aspek pendukung realisasi serta implementasi sistem manajemen keamanan informasi perusahaan
3. ISO 27002: terkait dengan dokumen ISO 27001, namun dalam dokumen ini terdapat panduan praktis pelaksanaan dan implementasi sistem manajemen keamanan informasi perusahaan.
4. ISO 27003: panduan implementasi sistem manajemen keamanan informasi perusahaan.
5. ISO 27004: dokumen yang berisi matriks dan metode pengukuran keberhasilan implementasi sistem manajemen keamanan informasi.
6. ISO 27005: dokumen panduan pelaksanaan manajemen risiko.
7. ISO 27006: dokumen panduan untuk sertifikasi sistem manajemen keamanan informasi perusahaan.
8. ISO 27007: dokumen panduan audit sistem manajemen keamanan informasi perusahaan.
9. ISO 27799: panduan ISO 27001 untuk industri kesehatan.

E. ISO/IEC 27001

ISO/IEC 27001 adalah sebuah metode khusus yang diakui oleh internasional sebagai metode pengamanan informasi [9]. ISO/IEC 27001 berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun sistem manajemen keamanan informasi (SMKI) [1]. Menurut Slamet dan Kawan [11], ISO/IEC 27001 digunakan melindungi *confidentiality*, *integrity* dan *availability* dari informasi. Indeks Keamanan Informasi (Indeks KAMI) merupakan salah satu alat yang digunakan untuk mengevaluasi dan menganalisis tingkat kesiapan atau kematangan SMKI.

F. Indeks KAMI

Indeks KAMI atau bisa juga disebut dengan indeks keamanan informasi adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi. Indeks KAMI adalah sebuah alat atau aplikasi yang digunakan sebagai alat yang digunakan untuk menganalisa dan mengevaluasi tingkat kesiapan baik kelengkapan ataupun kematangan penerapan keamanan informasi. Menurut Yuliani dan Kawan [16] Alat evaluasi ini tidak ditujukan untuk menganalisa kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan

gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2009. Area yang dapat dilakukan evaluasi menggunakan indeks KAMI menurut [16] seperti pada gambar 1. meliputi:

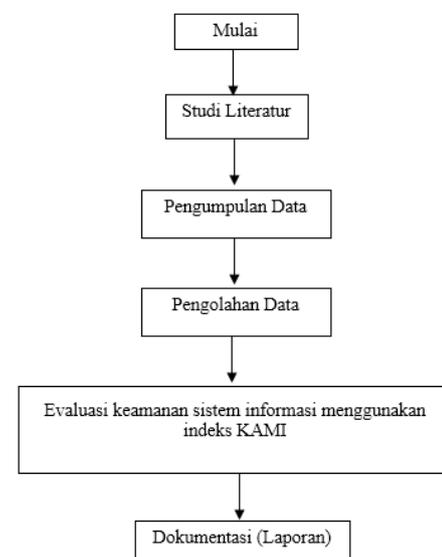
1. Tata Kelola Keamanan Informasi
2. Pengelolaan Risiko Keamanan Informasi
3. Kerangka Kerja Keamanan Informasi
4. Pengelolaan Aset Informasi
5. Aspek Teknologi dan Keamanan Informasi

III. METODE PENELITIAN

Bagian ini akan menjelaskan tahapan-tahapan penelitian yang akan dilakukan (dapat dilihat pada gambar 2). Pada tahapan tersebut akan dijelaskan metodologi atau



Gambar 1. Area Evaluasi Indeks KAMI [3]



Gambar 2. Tahapan Penelitian.

alat dan teknik yang membantu dalam pelaksanaan penelitian. Tahapan tersebut antara lain;

1. Studi Literatur

Tahapan studi literatur adalah tahapan awal pada penelitian ini. Tahapan ini digunakan untuk menentukan tujuan penelitian yang didasarkan pada penelitian-penelitian sebelumnya. Pada tahap ini juga akan dilakukan studi literatur mencari permasalahan-permasalahan yang berhubungan dengan topik penelitian yang akan dilakukan.

2. Perumusan Masalah

Pada tahap ini dilakukan perumusan masalah berdasarkan latar belakang yang dihasilkan dari studi literatur.

3. Pengumpulan Data

Tahap pengumpulan data dilakukan untuk memperoleh pemahaman terhadap permasalahan yang ada di BSI STTQ. Pengumpulan data dilakukan dengan menggunakan metode observasi dan wawancara terhadap pihak-pihak di BSI STTQ baik Ketua BSI, dan dua divisi yang ada di BSI STTQ.

4. Pengolahan Data

Pada tahap pengolahan data, data diolah sesuai dengan templat yang sudah disediakan oleh indeks KAMI. Data yang diinput melalui templat tersebut secara otomatis diolah angkanya.

5. Evaluasi keamanan Sistem Informasi menggunakan indeks KAMI

Tahap ini adalah tahap inti dari penelitian yang akan dilakukan. Pada tahap ini akan dilakukan evaluasi keamanan sistem informasi menggunakan standar ISO 27001 atau INDEKS KAMI. Proses evaluasi dilakukan dengan menggunakan metode wawancara dan observasi kelengkapan data terhadap pihak yang terkait (*Stakeholder*) BSI STTQ. Hasil observasi dan wawancara dimasukkan ke dalam templat Indeks KAMI dan data tersebut diolah secara otomatis oleh templat Indeks KAMI. Hasil pengolahan data kemudian dijadikan sebagai bahan evaluasi kesiapan dari aspek kelengkapan maupun kematangan kerangka kerja keamanan informasi yang diterapkan.

6. Dokumentasi atau Laporan

Tahapan dokumentasi merupakan akhir. Dalam tahap ini dilakukan pelaporan tentang hasil evaluasi dan implementasi kebutuhan keamanan sistem informasi di BSI STTQ.

Gresik. Proses penilaian menggunakan indeks keamanan informasi (KAMI) yang telah memenuhi semua aspek keamanan dan telah didefinisikan oleh standar ISO/IEC 27001:2013. Proses evaluasi dilakukan terhadap pejabat yang bertanggungjawab dan berwenang untuk mengelola Sistem Informasi Akademik. Dalam hal ini adalah Biro Sistem Informasi dan Wakil Ketua bidang Sarana dan Prasarana.

Dalam proses evaluasi, responden akan menjawab pertanyaan yang telah tersedia dalam templat indeks KAMI. Pertanyaan dikelompokkan dalam 2 kategori. Kategori pertama, pertanyaan didasarkan pada tingkat kesiapan penerapan pengamanan yang sesuai dengan kelengkapan kontrol yang diminta oleh standar ISO/IEC 27001:2013. Kategori yang kedua, pertanyaan didasarkan pada tingkat kematangan penerapan pengamanan dengan kategorisasi yang mengacu pada kerangka kerja COBIT.

Berdasarkan hasil interview yang dilakukan terhadap Biro Sistem dan Teknologi Informasi di Sekolah Tinggi pada 2 bagian, yakni bagian pengembangan aplikasi dan pengembangan jaringan, serta penanggung jawab biro sistem dan teknologi informasi yakni pembantu ketua I bidang kurikulum dan akademik. Instrumen yang digunakan adalah templat indeks KAMI.

Dari hasil wawancara dan pengisian templat indeks KAMI kemudian secara otomatis diolah. Hasil pengolahan dari ketiga responden kemudian diakumulasi dan dirata-rata. Berdasarkan hasil perhitungan rata-rata tersebut telah didapatkan tingkat kesiapan penerapan pengamanan sebesar 187 dari total 645, atau sekitar 28,99%. Sedangkan tingkat kematangannya I s/d I +. Berikut rincian hasil evaluasi tingkat keamanan informasinya. Tabel 1 adalah hasil penilaian tingkat kesiapan penerapan pengamanan dan tabel 2 hasil penilaian tingkat kematangan penerapan pengamanan.

Dari tabel 1 tersebut dapat disimpulkan bahwa total nilai yang diperoleh oleh responden adalah sebesar 187 dari Total 645 yang seharusnya. Pada kategori tata kelola mendapat skor 38, kategori pengelolaan resiko sebesar 18, kategori kerangka kerja sebesar 39, kategori pengelolaan aset sebesar 43 dan kategori aspek teknologi dengan skor 49.

TABEL 1
PENILAIAN TINGKAT KESIAPAN PENERAPAN PENGAMANAN

IV. HASIL DAN PEMBAHASAN

Pada tahap ini akan dilakukan penilaian tingkat keamanan informasi pada Sistem informasi Akademik (SIKAD) di Sekolah Tinggi Teknik Qomaruddin

Tabel 2 merupakan ringkasan pertanyaan yang dijawab oleh responden. Dalam pertanyaan tersebut hanya ada jawaban tidak dilakukan, dalam perencanaan, dalam perencanaan/diterapkan sebagian dan diterapkan menyeluruh.

TABEL 2
RINGKASAN PENILAIAN PERTANYAAN MENGGUNAKAN INDEKS KAMI

	Tingkat Kematangan					Jumlah
	Status	Tingkat Kematangan	Jumlah	Status	Tingkat Kematangan	
Tingkat II						
Status	I+	No	I+	I+	I+	
Tingkat III						
Validitas	No	No	No	No	No	
Status	No	No	No	No	No	
Tingkat IV						
Validitas	No	No	No	No	No	
Status	No	No	No	No	No	
Tingkat V						
Validitas	No	No	No	No	No	
Status	No	No	No	No	No	
Status Akhir	I+	I	I+	I+	I+	

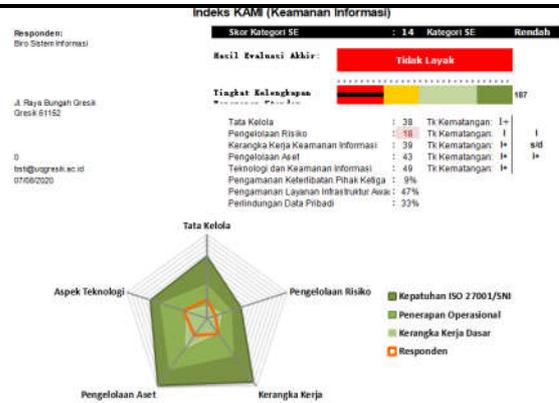
Dari tabel 2 kemudian dirangkum menjadi tabel 3 untuk menentukan tingkat kematangan masing-masing area. Dari tabel 3 tersebut kemudian disimpulkan level kematangannya. Secara keseluruhan hasil penilaian tingkat kematangan berada pada level I s/d I⁺.

TABEL 3
PENILAIAN TINGKAT KEMATANGAN PENERAPAN PENGAMANAN

	II	III	IV	V	
Tidak Dilakukan	2	2	1	2	7
Dalam Perencanaan	50	32	7	2	91
Dalam Penerapan/Diterapkan Sebagian	25	4	4	0	33
Diterapkan Menyeluruh	0	0	0	0	0
Total Pertanyaan					131

Level I s/d I⁺ merupakan level awal dimana pelaksanaan penerapan keamanan masih hanya sebatas perencanaan atau kalau memang sudah diterapkan, hanya diterapkan sebagian. Secara keseluruhan, hasil evaluasi tingkat keamanan informasi yang dilakukan di Biro Sistem Informasi Akademik Sekolah Tinggi Teknik Qomaruddin Gresik dapat dilihat pada gambar 3.

	Tata Kelola	Pengelolaan Risiko	Kerangka Kerja	Pengelolaan Aset	Aspek Teknologi	Total Skor
Kategori Kontrol						
1	8	10	12	24	14	204
2	8	4	10	10	10	252
3	6	2	7	4	2	189
Total Pertanyaan	22	16	29	38	26	645
Agregat Skor	1	1	1	1	1	
1	24	30	36	72	42	
2	72	54	96	132	102	
3	126	72	159	168	120	
Responden	38	18	39	43	49	187



Gambar 3. Hasil Pengukuran Tingkat Keamanan Informasi Sistem Informasi Akademik Sekolah Tinggi Teknik Qomaruddin Menggunakan Indeks Keamanan Informasi (KAMI).

TABEL 4
REKOMENDASI KEBIJAKAN PENERAPAN KEAMANAN SISTEM INFORMASI AKADEMIK SEKOLAH TINGGI TEKNIK QOMARUDDIN

No.	Rekomendasi Kebijakan
1	Perlu adanya lembaga yang bertanggungjawab mengelola pelaksanaan program keamanan informasi
2	Pelaksana pengamanan informasi memiliki sumber daya yang sesuai dengan standar teknologi terbaru
3	Pelaksana pengamanan informasi memiliki dokumen audit atau <i>framework</i> yang telah terstandarisasi
4	Memastikan bahwa pengelola keamanan informasi adalah orang yang memiliki kompetensi dan keahlian sesuai dengan standar keamanan informasi
5	Pengelola perlu untuk berkoordinasi kepada pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan untuk mengidentifikasi persyaratan/kebutuhan pengamanan.
6	Mendefinisikan langkah kelangsungan layanan TIK (<i>bussiness continuity and disaster recovery plans</i>)
7	Melakukan pemeriksaan rutin dan melaporkan hasil pemeriksaan

- 8 Menjadikan permasalahan keamanan informasi menjadi prioritas pengambilan keputusan strategis
- 9 Melakukan penilaian kinerja terhadap pelaksana keamanan informasi
- 10 Merumuskan target dan sasaran pengelolaan keamanan informasi

V. KESIMPULAN

Kesimpulan yang dapat diambil dari penelitian evaluasi tingkat keamanan informasi sebagai upaya peningkatan keamanan sistem informasi akademik (SIKAD) di Sekolah Tinggi Teknik Qomaruddin ini dapat disimpulkan masih belum layak. Baik dari kesiapan penerapan pengamanan dan tingkat kematangan penerapan pengamanan. Oleh sebab itu, dari hasil evaluasi tersebut perlu dilakukan penerapan pengamanan yang lebih baik sehingga tingkat kematangan penerapan pengamanan juga meningkat.

DAFTAR PUSTAKA

- [1] Direktorat Keamanan Informasi. 2017. Panduan Penerapan Sistem Manajemen Keamanan Informasi Berbasis Indeks Keamanan Informasi. Jakarta: Kementerian Komunikasi dan Informatika RI.
- [2] Fitriansyah, A dan Kawan. 2012. Tata Kelola Keamanan Informasi Berbasis ISO/IEC 27001:2005. Jurnal Teknologi Informasi ESIT Vol. VII No. 02 Oktober 2012.
- [3] Indeks Keamanan Informasi (KAMI) <http://bssn.go.id/>.
- [4] Kadir, A. (2009). Pengenalan Sistem Informasi. *American Enterprise Institute for Public Policy Research*.
- [5] Marco. R. (2016) Indeks Penilaian Tingkat Kematangan (*Maturity*) *It Governance* pada Manajemen Keamanan Layanan Teknologi Informasi, Jurnal DASI vol. 17 no. 2. Pp 76-82, ISSN: 1411-3201.
- [6] Matondang, N dan Kawan. 2019. Analisis Tingkat Kesiapan Pengamanan Sistem Informasi (Studi Kasus Upn Veteran Jakarta). Jurnal Teknologi Informasi dan Pendidikan. Vol. 12, No. 1, Maret 2019.
- [7] N. Abidin, S. Assani', Pengambilan Keputusan Strategi Manajemen Sistem Informasi Dan Teknologi Informasi (SI/TI) Berdasarkan Prioritas Menggunakan AHP (*Analytical Hierarchy Process*), NJCA - Volume 3, Nomor 2, Desember 2018: 146 – 151, 2018.
- [8] Raharjo, B. 2002. Keamanan Sistem Informasi Berbasis Internet. Bandung: PT Insan Indonesia.
- [9] Riswaya A. R. dan Kawan. 2020. Evaluasi Tatakelola Kemanan Teknologi Informasi Menggunakan Indeks KAMI Untuk Persiapan Standar SNI/IEC 27001 (Studi Kasus: STMIK Mardira Indonesia). Jurnal CComputech & Bisnis Vol. 14, No. 1 Juni 2020.
- [10] Safitri, M. E. dan Kawan. 2020. Analisis Penilaian Risiko Pada Keamanan Sistem Informasi: Studi Literatur. Jurnal Informatika dan Sistem Informasi (JIFoSI) Vol. 1, No.2. Juni 2020.
- [11] Slamet, M. R. dan Kawan. 2019. Penilaian Pengamanan Teknologi Pada Sistem Pembelajaran Elektronik Menggunakan Indeks Keamanan Informasi Di Politeknik Negeri Batam. Journal of Business Administration Vol 3 No. 1. Maret 2019. hlm, 162-171.
- [12] Tim Direktorat Keamanan Informasi. 2011. Tatakelola Keamanan Informasi Bagi Penyelenggara Pelayanan Publik. Direktorat Keamanan Informasi. Direktorat Jendral Aplikasi Informatika Kementerian Konumikasi dan Informatika Republik Indonesia.
- [13] Wahyudi H. dan Kawan. 2020. Audit Kemanan Sistem Informasi Manajemen Akademik dan Mahasiswa Menggunakan SNI/IEC 27001:2013 (Studi Kasus: STMIK Mardira Indonesia). Jurnal CComputech & Bisnis Vol. 14, No. 1 Juni 2020.
- [14] Whitman, M.E. dan Mattord, H., 2011, *Principles Of Information Security, Fourth Edition, Course Technology, US*.
- [15] Yuliani, S.Y dan Kawan. 2018. *Review Study of Hoax Email Characteristic. International Journal of Engineering and Technology (UAE)*. hlm, 778-782.
- [16] Yuliani, S.Y dan Kawan. 2020. Asesmen Keamanan Informasi Menggunakan Indeks Kami. NARATIF (Jurnal Ilmiah Nasional Riset Aplikasi dan Teknik Informatika). Vol. 02 No. 01 Juni 2020.