

PENGUKURAN TINGKAT KEAMANAN SISTEM INFORMASI MENGGUNAKAN INDEKS KAMI VERSI 3.1, DAN MENGUKUR TINGKAT KERENTANAN SERVER MENGGUNAKAN NETWORK SECURITY ASSESSMENT STUDI KASUS KOMINFO KABUPATEN GIANYAR

I Gede Putu Krisna Juliharta¹⁾, I Nyoman Yudi Anggara Wijaya²⁾, Ade Suci Laksana³⁾

Program Studi Sistem Informatika^{1) 2) 3)}

Sekolah Tinggi Manajemen Informatika (STMIK) Primakara, Denpasar, Bali ^{1) 2) 3)}

krisna@primakara.ac.id¹⁾ inyomanyudi@gmail.com²⁾ laksanasuci@gmail.com³⁾

ABSTRACT

Information system security is an indispensable thing for all organizations, agencies or companies to prevent data leakage or damage to information systems. This research was conducted at the Communication and Information Technology Department of Gianyar with Our Index 3.1 which aims to measure the level of maturity and completeness of information based on ISO / IEC 27001. Methods of data collection are by means of literature study, interviews and distributing OUR index questionnaires. The result of the score obtained from the evaluation of electronic system requirements is 24, while the level of completeness of the information gets 213. From these results it can be concluded that the level of information security is still very low. The study was also carried out on a number of network systems from agencies that had public access and under the handling of Diskominfo, weaknesses were categorized as critical by testing using Nessus.

Keywords : Information Security; Index 3.1; ISO / IEC 27001; Nessus.

ABSTRAKSI

Keamanan sistem informasi merupakan hal yang sangat diperlukan bagi seluruh organisasi, instansi ataupun perusahaan guna mencegah adanya kebocoran data maupun kerusakan sistem informasi. Penelitian ini dilakukan di Kominfo Gianyar dengan Indeks Kami 3.1 yang bertujuan untuk mengukur tingkat kematangan dan kelengkapan pada informasi berdasarkan ISO/IEC 27001. Metode pengumpulan data dengan cara studi literatur, interview dan menyebarkan kuesioner indeks KAMI. Hasil skor yang didapatkan dari evaluasi kebutuhan sistem elektronik adalah 24, sedangkan tingkat kelengkapan informasi mendapatkan 213. Dari hasil tersebut dapat disimpulkan bahwa tingkat keamanan informasi masih sangat rendah. Penelitian juga dilakukan pada beberapa jaringan sistem dari dinas-dinas yang memiliki akses publik dan dibawah penanganan Diskominfo, terdapat klemahan-kelemahan yang dikategorikan critical oleh pengujian menggunakan Nessus.

Kata Kunci: Keamanan Informasi, Indeks Kami 3.1, ISO/IEC 27001, Nessus.

PENDAHULUAN

Keamanan Informasi merupakan usaha dalam memperhatikan faktor-faktor seluruh piranti pendukung, jaringan maupun fasilitas yang digunakan. Sudah menjadi kebutuhan atau tuntutan di setiap instansi penyelenggara pelayanan publik. Dengan peran TIK yang semakin penting dalam upaya peningkatan kualitas layanan dari tata kelola pemerintah yang baik. Hal ini Kementerian Kominfo telah menyelenggarakan sosialisasi dan bimbingan teknis (bimtek) berisi tentang definisi, pengertian, kontrol-kontrol, persyaratan dokumentasi keamanan informasi dan contoh-contoh tindakan untuk mengamankan informasi. Mayoritas peserta sosialisasi dan bimtek belum memiliki atau sedang menyusun kerangka kerja yang sesuai dengan standar SNI ISO/IEC 27001. Bimtek juga

mensimulasikan penilaian secara mandiri (self assessment) tingkat kesiapan dan kematangan sistem manajemen keamanan informasi dengan mengisi pertanyaan-pertanyaan yang dirangkum dalam alat bantu penilaian yang disebut Indeks KAMI.

Beberapa instansi yang memiliki dokumentasi sistem manajemen keamanan informasi juga belum mengetahui apakah kerangka kerja yang mereka bangun telah memenuhi standar SNI ISO/IEC 27001. Meskipun mengikuti sosialisasi dan bimtek, mayoritas peserta masih memerlukan pendampingan lanjutan baik untuk penyusunan dokumentasi SMKI maupun metode penerapannya. Mayoritas juga menginginkan agar dokumentasi SMKI dijelaskan secara rinci sehingga diperoleh pemahaman yang lebih komprehensif tentang dokumentasi yang memenuhi standar SNI ISO/IEC 27001.

Dengan adanya peraturan Menteri Komunikasi dan Informatika (Kominfo) nomor 4 tahun 2016 tentang Sistem Manajemen Pengamanan Informasi (SMPI), harus memiliki dan menerapkan SMKI untuk pelayanan publik khususnya yang berkategori “Tinggi” dan “Strategis”. Berdasarkan hasil observasi di Dinas Kominfo Gianyar yang peneliti lakukan saat ini diperoleh hasil bahwa belum pernah melakukan audit apapun pada keamanan informasinya. Sehingga Kominfo Gianyar, mampu untuk membenahi, membangun, dan menerapkan pengamanan pada informasi sesuai dengan standar ISO 27001.[8]

Dalam hal ini, peneliti membantu Kominfo Gianyar dalam melakukan audit secara independen dengan metode keamanan informasi yang digunakan untuk penelitian ini adalah Indeks KAMI yang mengacu pada ISO 27001. Karena Indeks KAMI menjadi panduan penerapan Manajemen Keamanan Informasi yang diterbitkan oleh Kementerian Kominfo sebagai tindak lanjut atas masukan selama kegiatan sosialisasi dan bimbingan teknis yang bertujuan untuk mempermudah kegiatan penilaian mandiri bagi instansi-instansi.

Untuk tahap perlindungan infrastruktur terpenting keamanan informasi yaitu server atau sistem komputer, menggunakan Network Security Assessment. Nessus adalah sebuah aplikasi dari Tenable Security untuk mendeteksi adanya kelemahan atau cacat dari suatu sistem. Nessus melakukan penjabaran kelemahan yang terjadi pada sistem dengan men scanning ip komputer yang digunakan dan mendeskripsikan kelemahan terjadi dan solusi rekomendasi dari Nessus itu sendiri .

Berdasarkan beberapa latar belakang di atas untuk dapat menunjang pengelolaan informasi yang lebih aman serta dapat menunjang semua tugas yang diemban dan mengamankan infrastruktur teknologi informasi dari segala jenis ancaman-ancaman seperti akses terlarang maupun jaringan yang tidak diinginkan. Maka Penulis memutuskan untuk membuat skripsi dengan judul “Pengukuran Tingkat Keamanan Sistem Informasi Menggunakan Indeks KAMI versi 3.1, dan Mengukur Tingkat Kerentanan Server Menggunakan Network Security Assessment Studi Kasus Kominfo Kabupaten Gianyar”.

METODOLOGI PENELITIAN



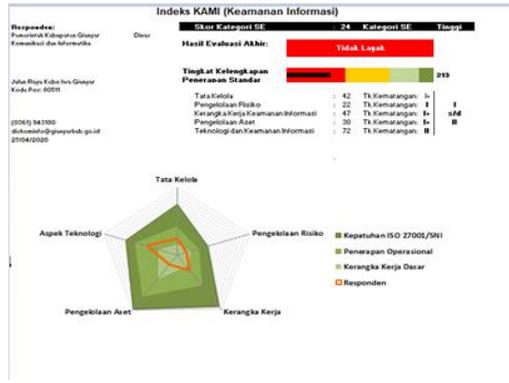
Gambar 1. *Research Methodology*

Proses pengukuran tingkat keamanan sistem informasi di KOMINFO Gianyar dengan menggunakan Indeks KAMI versi 3.1 dan pengukuran tingkat kerentanan server pada dinas di Gianyar yang memiliki ip publik yaitu pada dinas BPKAD, Bappeda dan dinas Kominfo sendiri menggunakan Network Security Assessment, dimulai dengan proses menemukan masalah, melakukan studi pustaka atau literatur, pengumpulan data dan wawancara. Pengumpulan wawancara yang bersifat bebas terbuka, dan pengisian kuesioner dari Kementerian Kominfo menggunakan Indeks Kami 3.1 dan pada dinas yang berada dibawah tanggung jawab Kominfo Gianyar yang memiliki Ip yang bersifat publik akan dilakukan scanning oleh Nessus. Setelah dilakukan pengukuran dan scanning ip dilanjutkan dengan memberikan rekomendasi untuk perbaikan dan di akhiri dengan memberikan kesimpulan dari penelitian yang dilakukan sesuai dengan Gambar.

HASIL DAN PEMBAHASAN

Mekanisme Pengumpulan Data

Pengumpulan data dalam penelitian dilakukan melalui proses wawancara dengan pihak pengelola sistem di dinas komunikasi informasi dan statistic kota Gianyar sehingga hasilnya subyektif. Selain proses wawancara proses pengumpulan data juga memberikan panduan mengenai pengisian Indeks Kami 3.1. Hasil dari Indeks Kami 3.1 untuk sistem manajemen pengamanan informasi di kota Gianyar dapat dilihat dari Gambar 2.



Gambar 2. Indeks KAMI 3.1

Dan pada Network Security Assesment data yang diperoleh sampel dari beberapa dinas yang ada di kota Gianyar, data server yang di dapatkan adalah server dari dinas Bappeda, BPKAD, Kominfo.

Data Pengukuran Indeks Kami 3.1

Dalam proses pengukuran indeks kami 3.1 ada total 5 langkah dengan memiliki pertanyaan pada masing-masing kategori. Langkah pertama dalam pengukuran dengan Indeks Kami 3.1 adalah mengisi identitas responden dengan mengisi identitas instansi, alamat, nomor telp, dan identitas pengisi lembar evaluasi dan sebagainya.

Selanjutnya adalah menjawab pertanyaan kategori sistem elektronik yang digunakan di Kabupaten Gianyar, bagian ini bertujuan mengevaluasi tingkat kepentingan penggunaan Sistem Elektronik di Kabupaten Gianyar, tujuan dari langkah ini adalah pengelompokkan sistem elektronik ke kategori rendah, tinggi, atau strategis dengan sejumlah pertanyaan terkait nilai inventasi, total anggaran operasional, jumlah pengguna. Total pertanyaan sepuluh buah, dan hasilnya dapat dilihat di Tabel.

Tabel 1. Kategori Sistem Elektronik

Bagian I: Kategori Sistem Elektronik			
Bagian ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan			
[Kategori Sistem Elektronik] Rendah; Tinggi; Strategis			
Jumlah Pertanyaan			10
Jawaban Bagian I			
A	B	C	
2	6	2	
Skor Bagian I			24

Dengan nilai 24 dapat disebut bahwa sistem elektronik yang digunakan di pemerintah kota Denpasar termasuk kategori tinggi.

Tabel 2. Tata Kelola Keamanan Informasi

Bagian 2: Tata Kelola Keamanan Informasi			
Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
Jumlah Pertanyaan			22
Jawaban Bagian 2			
Status Pengamanan	Kategori Kontrol		
	1	2	3
Tidak Dilakukan	-	-	6
Dalam Perencanaan	4	2	-
Dalam Penerapan / Penerapan Sebagian	4	5	
Diterapkan Secara Menyeluruh	-	1	-
Total Nilai Bagian 2			42

Tabel 2. mengukur seberapa jauh pemerintah kabupaten Gianyar melaksanakan tata kelola keamanan informasi dari sistem elektronik yang dimilikinya. Pertanyaan pada bagian ini fokus pertanyaan terkait adanya fungsi dari organisasi terhadap tata kelola keamanan informasi. Nilai evaluasi pada kategori ini adalah 42.

Tabel 3. Pengelolaan Risiko Keamanan Informasi

Bagian 3: Pengelolaan Risiko Keamanan Informasi			
Bagian ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
Jumlah Pertanyaan			16
Jawaban Bagian 3			
Status Pengamanan	Kategori Kontrol		
	1	2	3
Tidak Dilakukan	2	-	2
Dalam Perencanaan	6	2	-
Dalam Penerapan / Penerapan Sebagian	2	2	0
Diterapkan Secara Menyeluruh	-	-	-
Total Nilai Bagian 3			22

Tabel 3. memberikan gambaran pengelolaan resiko di pemerintah kabupaten Gianyar belum memiliki program kerja dan penetapan penanggung jawab manajemen risiko juga belum ada, total nilai evaluasi pada tahap ini adalah 22 dengan tingkat kematangan I.

Tabel 4. Kerangka Kerja

Bagian 4: Kerangka Kerja Pengelolaan Keamanan Informasi			
Bagian ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
Jumlah Pertanyaan	29		
Jawaban Bagian 4			
Status Pengamanan	Kategori Kontrol		
	1	2	3
Tidak Dilakukan	-	-	7
Dalam Perencanaan	7	5	-
Dalam Penerapan / Penerapan Sebagian	5	5	-
Diterapkan Secara Menyeluruh	-	-	-
Total Nilai Bagian 4	47		

Pengelolaan Keamanan Tabel 4. Memberikan gambaran mengenai kerangka kerja pengelolaan keamanan informasi di sistem manajemen keamanan informasi kabupaten Gianyar. Memperoleh nilai 47.

Tabel 5. Pengelolaan Aset Informasi

Bagian 5: Pengelolaan Aset Informasi			
Bagian ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
Jumlah Pertanyaan	38		
Jawaban Bagian 5			
Status Pengamanan	Kategori Kontrol		
	1	2	3
Tidak Dilakukan	11	3	-
Dalam Perencanaan	1	3	3
Dalam Penerapan / Penerapan Sebagian	4	3	1
Diterapkan Secara Menyeluruh	1	0	-
Total Nilai Bagian 5	30		

Tabel 5. Pengelolaan aset terlihat pada gambar memiliki paling banyak bagian pertanyaan yang tidak dilakukan. Sehingga pendataan dan pengelolaan terkait aset dalam manajemen keamanan informasi di kabupaten Gianyar yang mereka miliki belum terukur dengan baik. Dan nilai yang didapatkan pada bagian aset adalah 30.

Tabel 6. Teknologi dan Keamanan Informasi

Bagian 6: Teknologi dan Keamanan Informasi			
Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi.			
[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh			
Jumlah Pertanyaan	26		
Jawaban Bagian 6			
Status Pengamanan	Kategori Kontrol		
	1	2	3
Tidak Dilakukan	12	-	-
Dalam Perencanaan	-	4	1
Dalam Penerapan / Penerapan Sebagian	-	4	1
Diterapkan Secara Menyeluruh	2	2	-
Total Nilai Bagian 6	72		

Tabel 6. Menunjukkan nilai yang diperoleh pada keamanan informasi pada teknologi paling tinggi yaitu 72. Hampir semua pertanyaan yang diajukan memiliki status dalam penerapan/penerapan sebagian.

Hasil Pengukuran Indeks KAMI 3.1

Berdasarkan hasil pada data pengukuran Index Kami 3.1 diperoleh hasil mengenai gambaran bagaimana peran serta penggunaan teknologi informasi di Pemerintah Kabupaten Gianyar, serta nilai tingkat kematangan dari pengelolaan keamanan sistem informasi di Kabupaten Gianyar. Untuk bagian I pada Tabel I. Dapat dilihat bahwa Teknologi informasi dan komputer memiliki peran penting. Ditunjukkan berdasarkan Nilai sebesar 24 yang memiliki arti memiliki kategori Tinggi.

Untuk bagian 2, 3, 4, 5, dan 6 digunakan untuk mengukur tingkat maturity level dari sistem manajemen keamanan informasi Kota Denpasar. Hasil pengukuran dapat dilihat pada Tabel 7.

Tabel 7. Pengukuran Indeks Kami 3.1

INDEX KAMI 4.0	SKOR	MATURITY LEVEL
Bagian 2 : Tata kelola keamanan Informasi	42	I+
Bagian 3 : Pengelolaan Resiko Keamanan Informasi	22	I
Bagian 4 : Kerangka Kerja Pengelolaan Keamanan Informasi	47	I+
Bagian 5 : Pengelolaan Aset Informasi	30	I+
Bagian 6 : Teknologi dan Keamanan Informasi	72	II
Total Skor	213	I – II

Total kematangan untuk bagian 2 sampai bagian 6 adalah 213 dalam maturity level masuk dalam kategori I-II. Artinya sistem manajemen keamanan informasi kabupaten Gianyar berada pada kondisi awal. Arti kondisi awal adalah sudah adanya pemahaman mengenai pengelolaan keamanan sistem informasi namun penerapan langkah pengamanan masih kurang dalam memperhatikan resikonya.

Sehingga pengukuran pada Indeks Kami 3.1 diatas dapat diambil kesimpulan bahwa sistem manajemen keamanan informasi di pemerintahan kabupaten Gianyar berada pada tahap **Tidak Layak**. Seperti pada Gambar 3.

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

Gambar 3. Hasil Pengukuran Indeks Kami 3.1

Data Pengukuran Network Security Assessment

Data yang diperoleh dalam pengukuran tingkat keamanan server ini adalah mengambil sampel ip pada server yang ada di pemerintahan kabupaten Gianyar. Ip yang bersifat publik, artinya diakses banyak atau dengan sembarang orang. Pengukuran ip server menggunakan Nessus. Akan dilakukan scanning oleh Nessus dan diberikan tingkat kerentanan server pada level critical, hard, medium, low, info sekaligus penjabaran hal-hal yang terjadi pada server. Nessus juga memberikan solusi untuk perbaikan kerentanan yang terjadi

Berikut rentang skor pada masing-masing level kerentanan yang ada pada server dinas kota Gianyar, pada Gambar 4.

Gambar 4. Rentang skor kerentanan

Ip server dari dinas Bappeda, BPKAD, dan KOMINFO. Pada Gambar 5, 6, 7 adalah hasil pengukuran kerentanan menggunakan Nessus.



Gambar 5. Hasil pengukuran server dinas Bappeda

Bappeda dalam hal ini memiliki 5 hal kerentanan pada level medium atau sedang, dan 24 hal kerentanan pada level info atau tidak ada.



Gambar 6. Hasil Pengukuran server dinas Kominfo

Hasil pengukuran kerentanan server pada dinas Kominfo Gianyar memiliki 7 hal kerentanan pada level medium dan 38 pada level info atau tidak ada.



Gambar 7. Hasil Pengukuran server dinas BPKAD

St	Severity	Base Score Range
NoI	None	0.0
Lov	Low	0.1-3.9
Me	Medium	4.0-6.9
Hig	High	7.0-8.9
CriI	Critical	9.0-10.0

Pada server dinas BPKAD dalam pengukuran kerentanannya memiliki 1 hal kerentanan pada level critical, 3 hal pada level high, 9 hal pada level medium, dan 53 hal info atau tidak ada.

Rekomendasi Keamanan Sistem Informasi untuk Pemerintah Kota Gianyar

Dikota Gianyar hasil pengukuran kerentanan server, menunjukkan pada skala I-II sedangkan kesiapan untuk mengikuti sertifikasi ISO 27001 tingkat kematangan sistem manajemen keamanan informasi harus berada pada level IV terkelola dan terukur. Untuk dapat mencapainya hal tersebut maka ada hal-hal yang dapat direkomendasikan untuk mencapai tingkat kematangan sebagai berikut:

- Bagian I : Perlu adanya peningkatan anggaran dalam rangka kegiatan operasional dan monitoring terhadap sistem keamanan informasi
- Bagian II : Jawaban diterapkan secara menyeluruh hanya 1 dari 22 total pertanyaan. Perlunya langkah kongkrit dalam atau tindakan yang bersifat berkelanjutan dalam tata kelola keamanan sistem informasi terkait penanggung jawab dan pengelolaan sistem keamanan informasi
- Bagian III : Pada pengelolaan resiko keamanan informasi tidak ada jawaban yang diterapkan secara menyeluruh, perlu dilakukan langkah kongkrit untuk memiliki program kerja pengelolaan resiko keamanan, penanggung jawab, dan pelaporan status pengelolaan resiko.
- Bagian IV : Kerangka kerja pengelolaan keamanan informasi perlu dilakukan monitoring dan evaluasi terhadap pengelolaannya. Membuat mekanisme, jadwal, sasaran dalam pengelolaan kerangka kerja terkait keamanan informasi.
- Bagian V : Bagian pengelolaan aset informasi 22 hal yang tidak dilakukan. Perlu dilakukannya pengelolaan aset sistem manajemen keamanan informasi. Dokumentasi aset juga perlu di dokumentasi dan evaluasi.

SIMPULAN

Tingkat keamanan sistem informasi Kominfo Gianyar masuk kedalam kategori tidak layak, terutama di kategori pengelolaan risiko dengan nilai 22. Skor maksimal 645 dan Kominfo Gianyar berada di skor 213 pada level I-II. Dengan tingkat penggunaan Sistem Elektronik berada dilevel tinggi. Dengan skor ini, Kominfo Gianyar tergolong tidak cukup untuk mengikuti sertifikasi ISO 27001. Sedangkan tingkat kematangan sistem manajemen keamanan informasi harus berada pada level IV.

DAFTAR PUSTAKA

- [1] Edo Rizky Pratama, S. A. (2018). Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001 (Studi Kasus KOMINFO Provinsi Jawa Timur) . *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 2, 11.
- [2] Firzah A Basyarahil, H. M. (2017). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 pada Direktorat Pengembangan Teknologi dan Sistem Informasi (DPTSI) ITS Surabaya. *JURNAL TEKNIK ITS*, 6, 1.
- [3] Juliharta, I. G. (2012). Bussines Impact Analysis Sistem Dan Jaringan Komputer Menggunakan Metode Network Security Assesment. *Jurnal Ekplora Informatika*, 2, 1.
- [4] KAMIlah, I. (2019). Analisis Keamanan Vulnerability pada Server Absensi Kehadiran Laboratorium di Program Studi Teknik Informatika. *Seminar Nasional Sains dan Teknologi 2019 Fakultas Teknik Universitas Muhammadiyah Jakarta* .
- [5] Muh. Faturachman Husin, H. F. (2017). Implementasi Indeks KAMI di Universitas Sam Ratulangi . *E- Journal Teknik Informatika* , 12, 1.
- [6] Pasetyo, D. D. (2019). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks KAMI Berdasarkan ISO/IEC 27001:2013 pada Politeknik Ilmu Pelayaran Semarang. *Journal of Information Sistem Vol. 4, No 1, Mei*.
- [7] T, T. (2018). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) berdasarkan ISO 27001:2013 pada Pusat Informasi dan Pangkalan Data Perguruan Tinggi X . *Jurnal CoreIT*, 4, 2.

[8] Informasi, T. D. (2011). Buku Panduan Tata Kelola Keamanan Informasi Bagi Penyelenggara Publik.

[9] Annex A Controls. ISMS.online, 22 June 2020, www.isms.online/iso-27001/annex-a-controls/.