Analisis Sistem Manajemen Keamanan Informasi Pada Dinas Komunikasi Informasi Dan Statistik Kabupaten Lampung Tengah Menggunakan ISO/IEC 27001

1st Rezky Alkais Putra Rudiyanto
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
rezkyalkaisp@students.telkomuniversity.ac.id

2nd Vera Suryani
Fakultas Informatika
Universitas Telkom
Bandung, Indonesia
verasuryani@telkomuniversity.ac.id

Abstrak

Penelitian ini dibuat karena adanya kasus penyerangan pada web portal internal, belum adanya ketersediaan dalam kebijakan keamanan informasi yang telah diterapkan pada web portal internal. Penelitian ini bertujuan untuk dapat bisa merencanakan Sistem Manajemen Keamanan Informasi (SMKI) yang mungkin dapat digunakan sebagai pedoman dari suatu kebijakan keamanan informasi pada divisi Informatika dan Statistik. Penelitian ini membahas tentang mengenai penggunaan ISO 27001 pada Dinas Komunikasi Informasi dan Statistik KabupatenLampung Tengah. penelitian ini menggunakan metode Plan, Do, Check, dan Act dalam pengumpulan data, analisis, dan pengolahan data yang telah ditemukan. Hasil dari penelitian ini adalah tingkatan dari maturity level ISO/IEC 27001 rata –rata untuk tahun 2021 berada di level dua. Diharapkan hasil dari penelitian ini dapat membantu dan memberikan beberapa rekomendasi untuk standar kontrol keamanan yang dapat digunakan sebagai pedoman dan prosedur penerapan keamanan informasi.

Kata kunci : *Sistem Manajemen Keamanan Informasi (SMKI) Pada Diskominfo Lapung Tengah, ISO/IEC 27001, Plan Do Check Act (PDCA) Model.*

Abstract

This research was made because of an attack case on the internal web portal, there is no availability in the information security policy that has been applied to the internal web portal. This study aims to be able to plan an Information Security Management System (SMKI) which may be used as a guideline for an information security policy in the Informatics and Statistics division. This study discusses the use of ISO 27001 at the Information Communications and Statistics Office of Central Lampung Regency. This study uses the Plan, Do, Check, and Act methods in data collection, analysis, and data processing that have been found. The result of this research is that the average maturity level of ISO/IEC 27001 for 2021 is at level two. It is hoped that the results of this research can help and provide some recommendations for security control standards that can be used as guidelines and procedures for implementing information security.

Keywords: *Information Security Management System (SMKI) at Diskominfo Lapung Tengah, ISO/IEC 27001, Plan Do Check Act (PDCA) Model.*

I. PENDAHULUAN

Teknologi informasi adalah sumber daya yang sangat strategis, yang di dalamnya menyediakan informasi yang penting untuk membantu dalam pengambilan keputusan pada sebuah organisa si [22]Salah satu bagian yang sangat mempengaruhi teknologi informasi adalah keamanan informasi [1]. Keamanan informasi yang dikhususkan pada bagian cyber sudah termasuk area dengan perkembangan yang cepat dan perlunya evaluasi inovasi[20].

Keamanan informasi adalah kekuatan yang dapat dikontrol menggunakan sistem manajemen keamanan informasi, yang berfungasi untuk mengatur dan mengoperasikan keamana suatu sistem inforamsi agar dapat digunakan sesuai dengan prosedur[18]. Sistem keamanan informasi mempunya tujuan yaitumenjamin kerahasiaan, keutuhan, dan ketersediaan dari data dan informasi[18].

Standar ISO/IEC 27001 dapat digunakan dalam menerapkan suatu sistem manajemen keamanan informasi [8]. Standar ISO/IEC 27001 adalah standar yang dapat digunakan untuk membantu dari pihak manajemen untuk merencanakan dan menentapkan keamanan informasi yang sesuai dengan aturan yang ada (ISO/IEC 27001). Perusahaan yang telah menggunakan standar ISO/IEC 27001 akan diberikan sertifikat ISMS/SMKI oleh pihak ketiga yang telah mengukur keamanan dan bukti yang ada.

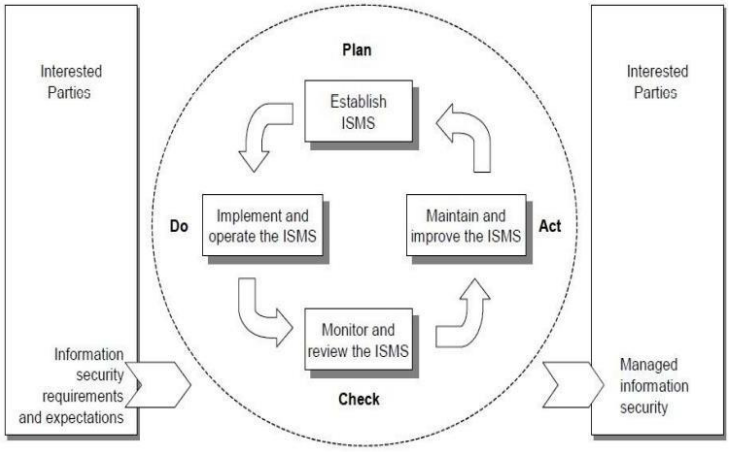
Web portal internal adalah salah satu teknologi informasi yang berguna bagi masyarakat yang dapat memberikan beberapa layanan yang dapat diakses melalui jaringan internet dan membantu pegawai Diskominfo dalam melakukan kegiatan oprasional sehari-hari. Web portal internal digunakan sebagai media untuk Diskominfo menyimpan berkas – berkas seperti pengumuman, surat keputusan (SK), event yang dilaksanakan dan file lainnya. Berdasarkan dari hasil wawancara dengan pihak dari Diskominfo Lampung Tengah, pada tahun 2017 terjadi penyerangan pada web portal internal yangmenyebabkan hilangnya beberapa data dari perusahaan yang bersifat rahasia dan penting. Selain itu, dapat ditemukan kondisi yang terkait dengan keamanan informasi yaitu kurangnya pegawai. Penempatan posisi dari pegawai berdasarkan kemampuan (capability) dan keahlian yang merupakan komponen dari bagian yang diperlukan, sehingga memiliki pengaruh yang sangat positif dan signifikan terhadapproses kinerja [13].

II. KAJIAN TEORI

2.1 ISO 27001

Standar dari ISO 27001 ini ditemukan pada 23 Februari 1947, yang diumumkan sebagai standar industri dan komersial yang sudah berlaku di seluruh dunia, memiliki kantor yang berpusat di Jenewa, Swiss (Murphy and Yates, tahun 2009). Standar internasional ISO/IEC 27001 berguna untuk menentukan, menerapkan, mengoperasikan, meninjau, memelihara, mengawasi, dan meningkatkan kebijakan dan dokumen dari sistem manajemen keamanan informasi (SMKI) berdasarkan kebutuhan dari organisasi[25].

Untuk mengatur semua proses SMKI, maka digunakan standar "Plan-Do- Check-Act" (PDCA) model. Penerapan model PDCA juga akan berguna untuk menentukan, menerapkan, mengawasi, dan meningkatkan keefektifitasan SMKI organisasi [25].



Gambar 2.3. Model PDCA yang diterapkan untuk proses SMKI (SistemManagement Keamanan Informasi

Kontrol keamanan sistem, referensi yang berdasarkan dari ilustrasi, yang dapat dipilih dari katalog kontrol, dan berhubungan dengan Annex A ISO/IEC27001. Dimana penentuan dari SMKI organisasi sangat membutuhkan untuk dapatmelakukan penelitian risiko seusai dengan kebutuhan khusus pada ISO/IEC 27001. Setelah penilaian dilakukan maka sistem dari kontrol harus dapat dipilih dari AnnexA untuk dapat mengurangi seperangkat identifikasi risiko yang telah teridentifikasi [25].

2.2 Domain COBIT 5

COBIT 5 Framewrok dirancang menggunakan 5 domain yang setiap domainnya mencakup penjelasan secara rinci dan termasuk panduan secara luas dan bertujuan menjadi tataKelola dan manajemen TI perusahaan.

Lima domain yang ada pada COBIT 5 adalah sebagai berikut:

- EDM (*Evaluate, Direct and Monitor*)
- APO (*Align, Plan and Organise*)
- BAI (*Build, Acquire and Implement*)
- DSS (*Deliver, Service, and Support*)
- MEA (*Monitor, Evaluate and Assess*)

2.1.1 Perencanaan (*Plan*)

pada tahapan ini dilakukan wawancara secara langsung untuk mendapatkan informasi yang diperlukan, observasi dengan cara mengamati secara langsung kegiatan yang ada di kantor Diskominfo Lampung tengah, mencari referensi lain yang bisa berasa dari internet, dan menentukan klausa mana yang perlu di uji.

2.1.2 Praktik (Do)

Rencana yang sudah disusun akan diimplementasikan dengan bertahap, dari skala kecil hingga besar sesuai dengan rencana yang telah dibuat.

2.1.3 Memeriksa Hasil (*Check*)

Dari hasil yang di dapatkan pada tahapan *Do,* tahap selanjutnya adalah tahapan *Check*, yaitu memilih control keamanan informasi dan juga objektif control yang diterapkan oleh Diskominfo Lampung Tengah.

2.1.4 Tindah Lanjut (Act)

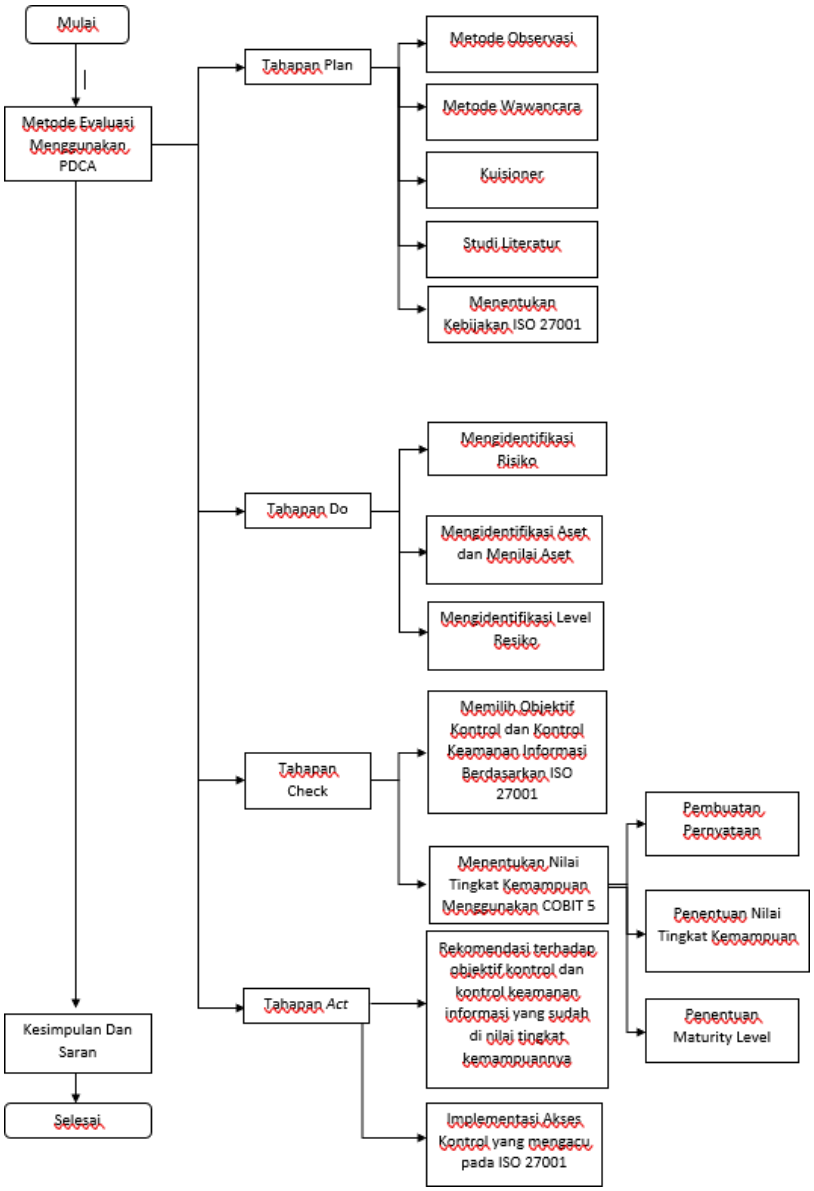
Setelah mendapatkan hasil dari tahapan check, Langkah selanjutnya adalah tahapan act. Tahap ini yaitu akan dilakukan langkah perbaikan dan pengembangandari manajemen keamanan informasi pada Divisi Information

Technology (IT) dengan cara memberikan beberapa rekomendasi terhadap objektif kontrol dan kontrol dari keamanan informasi yang telah dinilai dari tingkat kemampuannya di tahapan sebelumnya. Rekomendasi yang akan diberikan adalah standar yang mengacu pada ISO/IEC 27001.

III. METODE

3.1 Metode Konseptual

Metode konseptual ini adalah gambaran berupa rancangan yang terstruktur atau kerangka yang dapat berikir dengan menggunakan gambar, metode yang dapat memecahkan masalah secara terstruktur, yang berdasarkan dari model konseptual yang telah dibuat.



Gambar 3.4 Kerangla Penelitian

3.2 Tools Yang Dipakai

Pada pengerjaan penelitian ini saya menggunakan beberapa tools yang saya anggap dapat berguna untuk penelitian ini, saya menggunakan 2 Tools, seperti dibawah ini:

3.2.1 Google Form

Untuk membuat kuisioner seperti diatas, membutuhkan sebuah tools yang sudah tersedia di google, dan bukan hanya goolge form saja, tapi ada banyak tools lainnya, saya menggunakan Google Form karena cepat dan mudah dipahami, selain itu juga sudah banyak sekali orang yang

menggunakannya untuk membuat kuisioner.

Fitur didalamnya juga beragam yang dapat meembuat lembar kuisioner terlihat menarik dari pemilihan warna background, font, border, dll.

diperlukan, dan setelah data dimasukan oleh partisipan maka data akan keluarberufa kurfa atau gambar yang dapat memudahkan untuk pembaca memahaminya.

3.2.2 OWASP ZAP

Untuk tools ini saya gunakan untuk mendapatkan nilai dari vulnerability pada web Diskominfo Lampung Tengah, saya menggunakan aplikasi ini karena menurut saya pada aplikasi ini dapat melihat kelebihan dan juga kekurangan padasebuah situs web.

Pada tools ini dapat mengidentifikasi bagian mana yang rentan akan serangan dari luar ataupun dalam, serangan dari luar yang saya maksud adalah serangan yangterjadi akibat orang ketiga yang sengaja meng-Hack kedalam sistem utama untuk mendapatkan keuntungan, sedangkan serangan dari

Bukan hanya itu saja, tetapi bisa disesuaikan dengan kebutuhan, semisal kita membutuhkan kuisioner dengan jawaban yang Panjang maka terdapat space kosong untuk menulis jawaban sepanjang mungkin, ada juga pilihan ganda jika

dalam yang saya maksud seperti kemungkinan terjadinya kegagalan sistem, proxy yang kurang memadai atauserangan virus lainnya.

Dengan menggunakan tools ini, jika menemukan masalah yang kemungkinan terjadi maka sistem dari tools ini akan memberikan saran untuk melakukan perbaikan pada Web yang dituju, jika merasa kurang berfungsi, maka dapat disarankan untuk melakukan report kepada developer yang membuat aplikasi berbasis web tersebut.

IV. HASIL DAN PEMBAHASAN

4.1 Nilai Kesenjangan Kematangan Saat Ini

Berdasarkan dari rangkuman nilai kematangan diatas, maka, bisa diketahuinilai dari kesenjangan pada masing – masing domain, yaitu:

Table 4.28 Maturity Level

Domain	Maturity Level		
	Current Maturity	Expected Maturity	Gap/Selisih
APO 07	1,5	2	0,5
APO 13	1,7	2	0,3
DSS 02	1,7	2	0,3
MEA 03	2	2	0
APO 13	1,8	2	0,2
BAI 09	1,7	2	0,3
APO 13	1,75	2	0.25
APO 08	2	2	0
APO 10	1,8	2	0,2

Total Rata - Rata	0,2

Berdasarkan dari hasil analisis kesenjangan yang ditunjukan pada tabel di atas, terdapat jarak hampir di setiap domain yang di uji menggunakan cobit 5, antara kondisi yang di harapkan untuk saat ini dengan kondisi saat ini. Kesenjangan terbesar terdapat pada domain APO 07, walaupun *gap* terbilang lumayan kecil tetapi tetap membutuhkan penyesuaian pada masing – masing domain untuk mencapai nilai yang diinginkan, karena nilai 0,2 adalah rata – rata yang di dapat perdomain, terutama pada domain APO 07.

Fungsi dari Framework pada sebuah web sangat membantu web developer,framework juga memliki fungsi lain yaitu:

- Membuat kode program menjadi lebih terstruktur.
- Meningkatkan keamanan pada web.
- Mempercepat pembuatan dari website.
- Pemeliharaan dan perawatan website lebih mudah.

Framework yang digunakan oleh web portal internal ini adalah OpenResty,yaitu Framework Javascript berbasis komponen yang digunakan utnuk mengubah server nginx menjadi server aplikasi web yang kuat, dimana pengembang web dapat menggunakan Bahasa pemrograman Lua untuk skrip berbagai modul nginx C dan modul Lua yang ada dan membangun apliaksi web berkinerja sangat tinggi yang dapat menanganin koneksi 10k – 1000k + dalam satu kotak.

3.3 Pentingnya Keamanan Informasi Dan Web

Dalam rangka pentingnya dari keamanan pada suatu web, penulis melakukan wawancara kepada pihak yang bersangkutan

3.2 Framework Yang Digunakan Pada Web Portal

Framework adalah sebuah kerangka kerja yang dapat digunakan untuk membatu developer mengembangkan website. Framework diciptakan untuk membantu web developer untuk menulis baris kode, dengan menggunakan framework dapat mempermudah dalam penulisan kode, cepat, dan terstruktur rapih.
yaitu pada divisi komunikasi, informatika dan statistic yang bekerja untuk Diskominfo.

Untuk jangka waktu maintenance pada web portal internal ini yaitu setiap 1 bulan sekali untuk menghindari adanya error dan data yang menumpuk, mereka melakukan pengecekan untuk setiap data dan event yang ingin disebarkan melalui web portal internal.

Jika ada gangguan teknis pada web portal internal atau adanya bencana alammaka data yang ada sudah dapat dipastikan keamanannya karena telah dilakukan backup data secara otomatis dan berkala kepada pihak Pusat Data Nasional.

IV. KESIMPULAN

Berdasarkan dari hasil dan pembahasan yang dibahas dan telah ditemukan pada bab yang ada sebelumnya dapat disimpulkan bahwa laporan yang ada berdasarkan dari hasil analisis dapat digunakan dan menjadi ajuan untuk mencapai standar sistem manajemen keamanan informasi (SMKI) dengan menggunakan ISO/IEC 27001 yang dapat dijadikan sebagai rekomendasi dan peningkatan dari keamanan sistem informasi yang ada di Diskominfo Lampung Tengah.

Dari hasil analisis penelitian, ISO/IEC 27001 dapat berfokus pada bagaimana carany a menentukan standarisasi kebijakan untuk perusahaan dan manajemen risiko yang mungkin saja blom menerapkan kebijakan IT khususnya dibagian keamanan informasi.

Hasil dalam penelitian yang dilakuka n ini dapat diketahui bagaimana menetapkan tujuan, kebijakan, dan arahan kontrol dari keamanan informasi yang bisa dilanjutkan dengan analisis nilai aset dan risiko yang setelahnya dapat digunakan untuk menentukan penggunaan klausul pada ISO/IEC 27001 dan menghasilkan suatu rekomendasi pada penetapan kebijakan keamanan informasi pada web portal internal yaitu dapat melakukan pengidentifikasian kondisi yang membahayakan dan keamanan dari sumber daya manusia terkait dengan awareness pada keamanan informasi.

Ketua divisi Information Technology bertanggung jawab untuk semua pengelolaan pada proses SMKI dan penilaian resiko yang akan dilakukan secara berkala, dan untuk kontrol akses yang telah difokuskan pada teknis pemberdayaan, pemeliharaan aset dan tingkatan pada keamanan yang telah dimiliki khususnya pada kondisi fisik.

Teruntuk hasil analisis terkait kondisi aset dari web portal internal itu merupakan salah satu aset utama yang dimiliki oleh Diskominfo Lampung Tengah. Seiring berjalannya waktu dan pembelajaran yang di dapat pada masalah sebelumnya, divisi Information Technology telah melakukan serangkaian perbaikanyang membuat web portal internal mereka menjadi lebih baik dan meminimalisir untuk terjadinya hal yang tidak diinginkan.

Dari hasil menganalisis nilai maturity level pada kantor Diskominfo Lampung tengah telah didapatkan nilai gap 0,2. Untuk hasil dari penilaian pada maturity level ini sesuai dengan hasil dari evaluasi SPBE pada tahun 2021 yang seimbang di angka 2 yang artinya hanya cukup baik, akan tetapi sesuai dengan pengakuan dari pihak terkain, pada tahun 2022 saat ini aka nada peningkatan mencapai 3,2 untuk hasil dari evaluasi pada SPBE, kenaikan ini disebabkan oleh adanya beberapa faktor yang salah satunya adalah dikarenakan adanya program

REFERENCES

[1]. *Foundations of ITIL 2011 Edition*. Zaltbommel: Van HarenPublishing. KaryaBernard, Pierre tahun (2011)

[2]. Manajemen Sumber Daya Manusia. Karya Abdurrahmat, Fathoni. Tahun (2006)

[3]. Prosedur Penelitian Suatu Pendekatan Praktik. Karya Arikunto, Suharsimi.Tahun {2010)

[4]. Audit Sistem Keamanan Informasi Menggunakan ISO 27001 pada SMKN 1 Pugung, Lampung, Karya Pangky Februari, dan Fitria dari University of IIB Darmajaya, tahun 2019.

[5]. Analisis dan Penerapan Sistem Manajemen Keamanan informasi SIMHP BPKP menggunakan standar ISO 27001, Karya dari Muhammad Bakri, dan Nia Irmayana, tahun 2017.

[6]. Analyzing The Relevance of Inhibiting Factors in Implementing ISO 27001 Using theDEMATEL karya Muh. Sidratul Muntaha A.M.A, Wildan Farani, Wahyudin Buca K., Muhamad Insan Rizky, Achmad Nizar Hidayanto, Nur Fitriah Ayuning Budi, Ave Adriana Pinem, Satrio Baskoro Yudhoatmojo. Tahun (2020)

[7]. *Audit Keamanan Sistem Informasi pada Kantor Pemerintah Kota Yogyakarta Menggunakan COBIT 5*. Seminar NasionalTeknologi Informasi dan Komunikasi. Yogyakarta. Karya Ciptaningrum et al. tahun (2015)

[8]. *ISO/IEC 27000, 27001 and 27002 for Information SecurityManagement*. Journal of Information Security. Karya Disterer, Georg. Tahun (2013)

[9]. *Determining Evaluated Domain Process Through Problem Identification Using COBIT 5 Framework.* Karya Fitroh & Rustamaji tahun .(2017)

[10]. "Apa Itu Framework". Available Online: https://www.dicoding.com/blog/apa-itu-framework/

[11]. Penetapan Metode Cobit 5.0 Domain DSS02 Dan DSS03 Untuk Mengukur Tingkat Kapabilitas Tata Kelola Sistem Di PT. INDOFOOD CBP SUKSES MAKMUR TBK oleh: Cahyono Budy Santoso dan Aep Apandi Saleh tahun 2017. [12]. Pemetaan Domain Cobit 5 Dalam Tata Kelola TI Penerapan Office 365 di ITB STIKOM Bali oleh: Dian Pramana, Ni Made Rai Masita Dewi, dan Odie Kharisma Putra pada tahun 2021

[13]. *Pengaruh Analisis Jabatan terhadap Pencapaian Kinerja Organisasi di Universitas Muhammadiyah Surakarta*. Karya Giyarto. Tahun (2015).

[14]. *Process Reference Guide Exposure Draft*. Rolling Meadows, USA. KaryaISACA. Tahun (2012).

[15]. *Skripsi Analisis Faktor-Faktor yang Mempengaruhi Kepercayaan dalam Bertransaksi Online Shopping pada MahasiswaUIN Syarif Hidayatullah Jakarta*. Karya Lestari, Putri. Tahun (2018).

[16]. *Sistem Manajemen Keamanan Informasi*. Karya Sarno & Iffano. Tahun(2009).

[17]. *Metodologi Penelitian Kualitatif*. Karya Satori, D. dan Komariah, A. Tahun(2013).

[18]. *A Best Practice Approach for Integration of ITIL and ISO/IEC 27001 Services for Information Security Management*. Indian journal of science and technology, Vol. 5, No. 2. Karya Sheikhpour & Modiri. Tahun (2012).

[19]. *Information Security Management System Standards: A Comparative Study of the Big Five*. International Journal of Electrical &Computer Sciences IJECS- IJENS, Vol:11, No:05. Karya Susanto et al. Tahun (2011).

[20]. *The Impact of Security Awarness on Information Technology Professionals' Behavior*. Computers & Security. Karya Torten et al. Tahun (2018).

[21]. Pengukuran Maturity Level Tata Kelola Teknologi Informasi Menggunakan Framework Cobit 4.1 Pada PT. DINAMIKA MITRA SUKSES MAKMUR oleh: Erick Dazki, S.Kom.,M.Kom, Zaenab Islami, Wahyu Tisno Atmojo, S.Kom.,M.Kom. pada tahun 2020

[22]. *The Evolution of Enterprise Organization Designs*. Karya Galbraith,J.R. tahun (2012)

[23]. Analysing IT Governance Maturity Level using COBIT 2019 Framework: A Case Study of Small Size Higher Education Institute (XYZ-edu), karya Ahmad Ishlahuddin, Putu Wuri Handayani, Kasfu Hammi, Fatimah Azzahro. Tahun (2020)

[24]. Evaluation of Employee Attendance System Using COBIT 5 Framework. KaryaNaikson Fandier Saragih, Candora Sagala, Imelda Sri Dumayanti, Indra Kelana Jaya, Edward Rajagukguk, Asaziduhu Gea. Tahun (2020)

[25]. Perencanaan dan Implementasi Informasi Security Management System Menggunakan Framewok ISO/IEC 27001, Karya Anggi Anugraha Putra, Oky Dwi

Nurhayati, Ike Pertiwi Windasari, tahun (2016).

[26]. Maturity Model of Information Security for Software Developers. KaryaM. P. Silvae R. M. Barros. Tahun (2017)