Vol 1 No. 1, November 2020, pp. 120-124 **Jurnal Pepadun**

AUDIT KEAMANAN SISTEM INFORMASI DI DINAS XYZ PROVINSI LAMPUNG MENGGUNAKAN STANDAR ISO/IEC 27001:2013

[1]Annisa Meyliana, [2]Tristiyanto, dan [3]Rizky Prabowo

[1,2,3] Jurusan Ilmu Komputer Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Lampung
e-mail : [1]annisameylianaa@gmail.com, [2]tristiyanto.1981@fmipa.unila.ac.id,
[3]rizky.prabowo@fmipa.unila.ac.id

Abstract *— Audit of Information security system in the Communication and Information department is needed to determine the extent of information system carried out. This reasearch uses the ISO/ IEC 27001: 2013. Data from this reasearch were obtained based on the result of interview, observation and questionnaire. The respondent conducted a self assessment, then the researcher observe. The results of this study indicate that the average maturity level of the respondent is at level 2 (repeatable) with a value of 2.13 and the average maturity level of the finding is level 2 (repeatable) with a value of 2.40. The difference between the respondent value and the finding value show that in the sub domain information security incident management. This difference occur due to the absence of existing SOP procedure and criteria. Overall, there is no policy in developing the system through a process of security testing.*

Keywords: *Audit Keamanan, ISO 270012013, Maturity level*

1. PENDAHULUAN

Pengelolaan Teknologi Informasi dan Komunikasi yang baik akan mendorong hadir dan terwujudnya *good governance.* Metodologi dan tata kelola yang baik merupakan suatu prasyarat yang menjadi kewajiban dalam pengelolaan sebuah sistem yang baik. Dengan tata kelola yang baik, maka sistem yang *accountable* serta *sustainable* dapat tercapai bagi suatu badan atau lembaga dan dapat memberikan manfaat kepada publik seluas-luasnya [1].

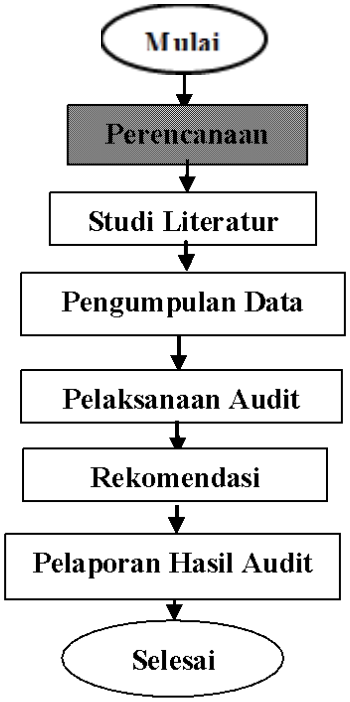
Audit didefinisikan sebagai proses atau aktivitas yang sistematik, independen dan terdokementasi untuk menemukan suatu bukti-bukti (*audit evidence*) dan dievaluasi secara obyektif untuk menentukan apakah telah memenuhi kriteria pemeriksaan (audit) yang ditetapkan. Tujuan dari audit adalah untuk memberikan gambaran kondisi tertentu yang berlangsung di perusahaan dan pelaporan mengenai pemenuhan terhadap sekumpulan standar yang terdefinisi [3].

ISO/IEC 27001 merupakan dokumen standar sistem manajemen keamanan informasi, yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah perusahan untuk mengevaluasi, mengimplementasikan dan memelihara keamanan informasi diperusahan. Kontrol keamanan berdasarkan *ISO/IEC* 27001 terbagi menjadi 14 klausul kontrol keamanan (*security control*), 39 obyektif kontrol (*control objectives*) dan 133 kontrol keamanan.

Keamanan informasi merupakan salah satu hal penting yang harus diperhatikan oleh perusahaan ataupun organisasi, adanya kebocoran informasi dan kegagalan sistem dapat menyebabkan kerugian baik di sisi finansial maupun produktifitas perusahaan. Keamanan informasi meliputi suatu mekanisme untuk mengontrol akses dan penggunaan *database* pada *level* obyek bagi pengguna, dimana pengguna tersebut memiliki akses terhadap informasi tertentu [2]. Keamanan infromasi adalah salah satu upaya untuk mengamankan aset informasi yang dimiliki [4]. Sedangkan informasi sendiri merupakan suatu aset penting yang harus dilindungi keamanannya. Untuk menjadi aman adalah dengan cara dilindungi dari musuh dan bahaya [5].

2. METODOLOGI PENELITIAN

Audit sistem informasi di DinasXYZ menggunakan standarISO/IEC 27001:2013, Gambar 1 adalah gambar kerangka berfikir dalam penelitian audit sistem informasi.



Gambar 1. Metodologi Penelitian

Langkah-langkah yang dilakukan adalah pada tahap perencanaan ini merencanakan daftar pertanyaan yang akan ditanyakan kepada narasumber. Studi literatur yaitu melakukan *review*, menambah referensi teori-teori yang dibutuhkan dalam penelitian. Tahap pengumpulan data yang digunakan dalam penelitian menggunakan metode observasi, metode wawancara dan kuisioner. Tahap pelaksanaan audit ini menggambarkan tentang pembuatan kuisioner yang diberikan kepada responden, data diperoleh kemudian dikumpulkan untuk diolah secara sistematis dan tahap rekomendasi yaitu saran berupa perbaikan untuk perusahaan. Tahap pelaporan hasil audit yaitu menyusun *draft* laporan audit.

3. HASIL DAN PEMBAHASAN

Data pada penelitian ini didapatkan dari hasil kuisioner, wawancara dan observasi. Pada penelitian ini digunakan sebagai alat pengumpulan data, yang diberikan kepada satu responden dari bidang informatika. Data kuisioner yang telah terkumpul kemudian dianalisa untuk mengidentifikasi hasil kuisioner responden. Hasil audit adalah sebagai berikut:

3.1. Analisis SWOT (*Strength, Weakness, Opportunity, Threat*)

Analisis SWOT adalah analisis untuk mengidentifikasi berbagai faktor secara sistematis dalam merumuskan strategi perusahaan. Analisis SWOT (*strength, weakness, opportunity, threat*) yang menggambarkan pemetaan kondisi kekuatan dan kelemahan serta peluang dan ancaman bagi Dinas XYZ. Berikut hasil dari analisis SWOT yang dapat dilihat pada Tabel 1.

Tabel 1. Analisis SWOT

Strength (Kekuatan)	**Weakness (Kelemahan)**
a. Sistem memiliki *plugin* yang memungkinkan untuk memeriksa kerentanan keamanan *word press* dan akan menyarankan beberapa tindakan perbaikan. b. Semua informasi bias dibagikan di lampung prov dan *server* yang menerima informasi dan menjawab jika ada informasi yang dibutuhkan. c. Memiliki *password* sebagai *encrypt t*sistem. d. Memiliki *file permission*. e. Memiliki *database security*.	a. Biaya operasional relative lebih mahal *b.* Diperlukan adanya satu komputer khusus untuk ditugaskan sebagai *server* c. Data tidak di perbaharui secara berkala
***Opportunity* (Peluang)**	***Threat* (Ancaman)**
a. Sistem ini sangat dibutuhkan oleh masyarakat karena adanya system ini dapat mempermudah layanan informasi b. Adanya kebijakan pemerintahan untuk pengembangan layanan TI agar dapat bisa berkembang lebih baik lagi	*a. Virus* *b. Hacking, cracking* c. Pencurian dan perusakan pada sistem d. *Interruption*

3.2. Hasil Keseluruhan *Maturity Level*

Hasil dari perolehan*current maturity level* pada Dinas XYZ didapatkan *current maturity level* tertinggi pada sub kontrol *Information security aspects of business continuity management* dengan nilai 2.66. Hasil nilai terendah pada sub kontrol *Systems acquisition, development and maintenance* dengan nilai 1.2 dan dengan rata-rata nilai 1.98, dikarenakan di bidang informatika belum memiliki standar dan kriteria dalam kebijakan kontrol keamanan sehingga bidang informatika tidak memiliki dokumen laporan, dan bidang informatika juga belum melalukan perbaikan.

3.3. Analisis *GAP*

Berikut ini adalah tabel hasil analisis *GAP* yang didalamnya terdapat sub domain, hasil responden (HR), hasil temuan (HT), dan *expected maturity leve*l yang dapat dilihat pada Tabel 2.

Tabel 2. HasilAnalisis*GAP*

No	Sub Domain	Hasil Responden	HasilTemuan	*Expected Maturity Level*
1	*Information security policies*	3	4	5
2	*Organization of information security*	2	2.28	5
3	*Human resource security*	1.3	2	5
4	*Asset management*	2.2	2.4	5
5	*Access control*	1.41	2.08	5
6	*Physical and environmental security*	2.13	2.8	5
7	*Operations security*	1.91	1.91	5
8	*Communications security*	2.66	2.66	5
9	*Systems acquisition, development and maintenance*	1.41	1.58	5
10	*Supplier relationships*	2.6	2.4	5

11	*Information security incident management*	2.85	2.85	5
12	*Information security aspects of business continuity management*	2.5	2.5	5
13	*Compliance*	1.83	1.83	5
	Rata-Rata	**2.13**	**2.40**	**5**

Hasil dari analisis *gap* dan dari hasil responden, hasil temuan dan ekspetasi level menjelaskan bahwa rata-rata maturity level hasil responden berada pada *level* 2 (*repeatable*) dengan nilai 2.13 yang artinya proses sudah direncanakan, dikelola dan dilakukan secara berulang-ulang, namun belum adanya prosedur dan rata-rata *maturity level* hasil temuan berada pada *level* 2 (*repeatable*) dengan nilai 2.40 yang artinya proses sudah direncanakan, dikelola dan dilakukan secara berulang-ulang, namun belum adanya prosedur.

Dari data diatas dapat dilihat bahwa hasil responden dan hasil temuan memiliki perbedaan. perbedaan tersebut terjadi karena pada bidang informatika belum adanya prosedur, dokumentasi dan laporan yang terkait untuk penyelesaian masalah yang ada. Bidang informatika belum secara teratur dalam mengontrol akses data dan belum terdokumetasi yang sesuai kriteria SOP dan belum adanya evaluasi.

3.4. Rekomendasi

Hasil perhitungan *maturity level* diperoleh tingkat kematangan Dinas XYZ. Dari hasil tingkat kematangan Dinas XYZ Lampung terdapat perbedaan sehingga dari data tersebut diperoleh *gap* diantara keduanya. Berdasarkan hasil temuan dan *gap* yang diperoleh, peneliti membuat sebuah solusi perbaikan yang ada di Dinas XYZ Lampung. Solusi tersebut ditujukan untuk sub domain *Human resource security, Asset management, Access control, Operations security, Systems acquisition, development and maintenance, Organization of information security, Supplier relationship, Compliance.*Berikut ini adalah tabel penjelasan dari rekomendasi.

Tabel 3. Rekomendasi

No	Kontrol	Rekomendasi
1	*Human resource security*	1. Membuat peraturan yang relevan untuk cek yang disetujui oleh manajemen. 2. Membuat prosedur perubahan pekerjaan. 3. Membuat jadwal pelatihan untuk kesadaran keamanan dalam sebuah organisasi.
2	*Asset management*	1. Membuat kebijakan untuk mengatur media removable. 2. Membuat dokumentasi dan investaris secara jelas terkait aset penting. 3. Membuat dokumentasi pengembalian aset.
3	*Access control*	1. Membuat kebijakan untuk proses akses layanan pengguna informasi. 2. Membuat kebijakan pengendalian untuk alokasi informasi. 3. Membuat prosedur *access control* agar semua terlindungi.
4	*Operations security*	1. Membuat prosedur untuk perubahan manajemen. 2. Membuat prosedur yang memastikan bahwa aset yang ditinggalkan telah terlindungi dengan benar, contohnya melakukan *log-off* ketika meninggalkan ruangan. 3. Membuat kebijakan untuk proses pengguna dalam menginstal perangkat lunak. 4. Membuat kebijakan untuk proses informasi dalam kerentanan teknis.

5	*Systems acquisition, development and maintenance*	1. Membuat kebijakan kontrol keamanan dalam pengembangan perangkat lunak. 2. Membuat kebijakan atau prosedur untuk proses platform. 3. Membuat kebijakan pengembangan sistem harus melalui proses uji keamanan.
6	*Organization of information security*	1. Membuat dokumentasi kontak terhadap pihak yang berkepentingan. 2. Membuat dokumentasi untuk tugas layanan dan informasi.
7	*Supplier relationships*	1. Membuat dokumentasi untuk pemeriksaan pemasok. 2. Membuat kebijakan untuk proses manajemen dalam penyediaan layanan.
8	*Compliance*	1. Membuat kebijakan untuk me-review pengelolaan informasi atau pelaksanaan kontrol keamanan. 2. Membuat dokumentasi untuk kepatuhan teknis.

Hasil penelitian berupa data atau angka disajikan dalam bentuk tabel atau grafik. Jika pada penelitian dilakukan pengembangan aplikasi/perangkat lunak, dapat disajikan beberapa *screenshot* yang penting. Setiap tabel, grafik atau gambar harus dirujuk di dalam tulisan/paragraf.

Bagian pembahasan memberikan ulasan mendalam (*insights*) terhadap data yang diperoleh dalam penelitian. Bagian ini dapat menyajikan tabel atau grafik yang merupakan hasil pengolahan data (bukan hanya data mentah). Author diharuskan untuk menjelaskan temuan yang diperoleh dalam penelitian disertai dengan bukti-bukti yang jelas. Bagian ini dapat berisi ulasan yang membandingkan hasil yang diperoleh dalam penelitian ini dengan hasil yang diperoleh dalam penelitian terdahulu.

4. KESIMPULAN

Dari gap analisis yang didapat, disimpulkan bahwa Sistem Informasi di Dinas XYZ belum memenuhi standar keamanan *ISO* 27001. Saat ini sistem memiliki indeks penilaian sebesar 2.42 dan jika dibulatkan ke dalam penilaian *maturity* berada pada *level* 2 (*repeatable*) sesuai standar *ISO/IEC* 27001:2013. Sub domain *Systems acquisition, development and maintenance* hasil responden bernilai 1.41 dan hasil temuan bernilai 1.58 yang merupakan nilai terkecil dari hasil *maturity level*. Nilai dari hasil responden dan hasil temuan terdapat perbedaan dimana belum adanya kebijakan dalam pengembangan sistem yang melalui proses uji keamanan.

DAFTAR PUSTAKA

[1] Ibrachim, N. e. 2012. *Bakuan Audit Keamanan Informasi Kemenpora.*Indonesia: Kementrian Pemuda dan Olahraga.

[2] Mufadhol. 2009. Kerahasiaan dan Keutuhan Keamanan Data dalam menjaga Integritas dan Keberadaan Informasi Data (Vol.6). *Jurnal Transformatika* , 50-62.

[3] Sarno, R. dan Iffano, I. 2009. *Sistem Manajemen Keamanan Informasi.* Surabaya: ITS Press.

[4] Syafrizal, M. 2007. ISO 17799. *Standar Sistem Manajemen Keamanan Sistem Informasi, Seminar Nasional Teknologi 2007 (STN 2007)*.

[5] Whitman, M. E. dan Mattord, H. J. 2016. *Manajemen of Information Sequrity (5th ed).* Boston: Course Technology.