BAB II

Tinjauan Pustaka

2.1 Studi Sebelumnya

Terdapat beberapa penelitian yang diambil untuk menjadi referensi oleh peneliti dalam pengerjaan tugas akhir. Beberapa penelitian yang dijadikan referensi dapat dilihat pada tabel 2.1 Studi sebelumnya.

Endang Kurniawan & Imam Riadi [7] melakukan penelitian tentang analisa level keamanan pada sistem akademik dengan standar ISO 27002: 2013 menggunakan SSE-CMM. Hasil nilai rata - rata untuk semua klausa adalah pada 2:51 dari skala 0-5. Dan nilai kesenjangan nilai antara kondisi keamanan yang diharapkan ada pada 2.49. Dari sini bisa disimpulkan bahwa hasil yang diperoleh dari pengukuran tingkat kematangan sistem akademik adalah pada level 3 (well define). Artinya standar proses sudah berjalan sesuai dengan prosedur yang mempunyai standar, dokumentasi, dan pelatihan secara berkala tetapi implementasi yang belum terlalu baik karena hanya diserahkan kepada tim untuk mengikuti proses sehingga dapat terjadi kesalahan maupun penyimpangan prosedur.

Nurul Fadhylah Octariza [8] melakukan penelitian tentang analisisa keamanan informasi menggunakan standar ISO/IEC 27001 dan ISO/IEC27002 pada sistem manajemen perusahaan PT. Jasa Marga dengan metode plan, do, check, dan act. Tahap plan menyatakan bahwa pada tahap ini divisi IT PT. Jasa Marga mempunyai web portal khusus pengguna internal perusahaan yang difungsikan untuk pintu untuk masuk ke sistem divisi masing - masing yang harus mengikuti SMKI untuk dapat membantu melindungi aset - aset penting. Yang mempunyai tanggung jawab dalam mengelola SMKI dan melaksanakan penilaian risiko secara berkala untuk mengontrol adalah ketua divisi IT. Tahap do menyatakan bahwa hasil analisa web portal berada di range nilai 8-11 (*medium*)

dan aset pndukung di range nilai 3-7 (*low*) dengan kesimpulan bahwa hasil analisis risiko pada kedua aset (aset utama dan aset pendukung) berada di tingkat risiko high risk. Pada tahap check, penilaian tingkat kematangan berada pada tingkat 1 karena tidak adanya kebijakan yang mengatur sehingga belum bertindak berdasarkan ISO/IEC27001. Pada tahap act, PT. Jasa Marga perlu membuat kebijakan baru terkait kesadaran keamanan sistem informasi untuk meningkatkan kesadaran pada seluruh pekerja dari tingkat pegawai sampai dengan tingkat pimpinan, juga perlu menyediakan kebijakan - kebijakan yang terkait dengan penggunaan keamanan untuk kegiatan kegiatan operasional misalnya menggunakan kartu akses untuk mengakses ruangan tertentu.

Aulia Nur Fatimah [9] melakukan penelitian tentang analisis pengelolaan keamanan sistem pada STIE Perbanas dengan metode OCTAVE dan FMEA untuk membuat dokumen SOP yang berlandaskan pada kerangka kerja COBIT 5 dan ISO27002:2013. STIE Perbanas mempunyai risiko keamanan sistem informasi yang tinggi yaitu risiko untuk manipulasi data, pencurian data, data tidak valid, dan pencurian data. Penyebab munculnya risiko adalah karena kurangnya kontrol keamanan fisik dikarenakan kontrol keamanan yang dilakukan hanya proses proses yang umum seperti pembetulan jika ada celah yang berpotensi untuk menyebabkan risiko keamanan.

Dea Anjayani [10] melakukan penelitian tentang analisis penilaian dan mitigasi risiko keamanan sistem informasi pada sistem EMC *(Electronic Medical Record)* RSU Haji Surabaya dengan metode OCTAVE dan FMEA. Terdapat 13 risiko dengan 25 kejadian risiko, risiko mempunyai kejadian risiko lebih dari pada satu karena beda penyebab. Sangat diperlukan pengendalian risiko untuk mengontrol risiko seperti *user access management*, *equipment security*, dan *secure area.*

Apol Pribadi Subriadi dan Nina Fadilah Najwa [11] melakukan penelitian tentang Menganalisis dan mengembangkan metode FMEA untuk pengukuran risiko keamanan sistem informasi. FMEA tradisional tidak konsisten karena menghasilkan *gap analysis input* untuk siklus berikutnya. FMEA yang dikembangkan mempunyai hasil yang lebih konsisten. Dalam penelitian

mendapatkan konsistensi sebesar 0.937 yang termasuk dalam konsistensi mendekati sempurna, sedangkan FMEA tradisional mendapatkan konsistensi 0.848 yang sudah tergolong sangat tinggi. Model FMEA tradisional yang terdiri dari 2 tahap utama, dikembangkan menjadi 4 tahap yaitu *determination of the risk assessment requirements, risk identification, risk analysis, and evaluation.*

Tabel 2.1 Studi Sebelumnya

No	Penulis	Tahun	Domain	Tujuan	Metode	Hasil
1	Endang Kurniawan & Imam Riadi	2018	Keamanan Sistem Informasi	Menganalisis gap & tingkat kematangan sistem informasi akademik UII	SEE-CMM	Kebutuhan TI sudah mempunyai prosedur dan didokumentasikan melalui platihan.
2	Nurul Fadhylah Octariza	2019	Keamanan Sistem Informasi	Menganalisis apakah keamanan web portal PT. Jasa Marga sudah sesuai standar keamanan informasi	Plan, Do, Check. dan Act	Plan: Pegawai mengikuti SMKI untuk membantu melindungi Aset, Do: hasil risiko keseluruhan aset berada pada level high-risk. check: belum ada kebijakan untuk mengatur sehingga belum bertindak berdasarkan ISO/IEC27001. Act: membuat kebijakan baru terkait kesadaran keamanan sistem informasi.
3	Aulia Nur Fatimah	2016	Keamanan Sistem Informasi	Aulia Nur Fatimah	OCTAVE dan FMEA	Pengelolaan keamanan sistem STIE Perbanas sudah dilakukan tetapi hanya proses umum seperti pembetulan jika ada celah yang berpotensi untuk menyebabkan risiko keamanan. Menghasilkan dokumen SOP Keamanan berdasarkan COBIT 5 dan ISO 27002:2013.

4	Dea Anjani	2015	Keamanan Sistem Informasi	Menganalisis penilaian dan mitigasi risiko keamanan sistem informasi pada sistem EMC *(Electronic Medical Record)* RSU Haji Surabaya	OCTAVE dan FMEA	Terdapat 13 risiko dengan 25 kejadian risiko, risiko mempunyai kejadian risiko lebih dari pada satu karena beda penyebab. Sangat diperlukan pengendalian risiko untuk mengontrol risiko seperti *user access management*, *equipment security*, dan *secure area.*
5	Apol Pribadi Subriadi dan Nina Fadilah Najwa	2019	Keamanan Sistem Informasi	Menganalisis dan mengembangkan metode FMEA untuk pengukuran risiko	*Action, Research, Cycle*	Metode FMEA *(Failure Modes and Effects Analysis)* dikembangkan menjadi 4 tahap yaitu *determination of the risk assessment requirements, risk identification, risk analysis, and evaluation.*

2.2 Dasar Teori

2.2.1 PT. Asia Bandar Alam

PT. Asia Bandar Alam merupakan perusahaan retail yang saat ini bertanggung jawab atas merek L'OCCITANE di Indonesia sejak tahun 2002. PT. Asia Bandar Alam memiliki lebih dari 45 gerai di seluruh negeri. L'OCCITANE berawal dari pasar di Provence. Hanya dengan sebuah *alembic*, truk kecil dan pengetahuan mendalam tentang tanaman, Olivier Baussan, di usia 23 tahun, menyuling minyak *esensial rosemary* untuk dijual ke pasar lokal di Provence. Dia memperluas produksinya dari minyak ke sabun hingga krim, mengambil inspirasi dari tanah airnya untuk membawa kecantikan alami ke rumah-rumah di seluruh dunia. L'OCCITANE bekerja secara langsung dengan lebih dari 130 petani Prancis dan 10.000 pemetik dari ladang immortelle di Corsica hingga ladang lavender di Provence untuk memastikan bahwa bahan yang kami gunakan memiliki kualitas terbaik dan bersumber secara berkelanjutan.

2.2.2 Definisi Data

Data merupakan bahan bahan yang masih mentah, diuraikan sebagai atribut yang beruntun menunjukan jumlah dan tindakan [12]. Metode pengumpulan data yang paling umum digunakan antara lain:

- Pengamatan langsung sendiri
- Wawancara
- Kuisioner

Pengamatan langsung sendiri (observasi) merupakan suatu bentuk metode ilmiah untuk mengumpulkan data yang paling sering digunakan dalam menggali informasi, meski begitu observasi menjadi metode yang kurang diminati dan kurang mendapat perhatian pada berbagai literatur metodologis. Para ilmuan menilai bahwa observasi hanya dianggap

sebagai aktivitas pendukung karena tidak lebih dari kegiatan mengumpulkan data visual[13]. Observasi mempunyai kelebihan yaitu metode observasi tidak mencolok, dan tidak perlu berinteraksi langsung kepada partisipan. Observasi juga mempunyai kelebihan lain yaitu minimalnya pengaruh dan potensi yang ditimbulkan oleh pengamat itu sendiri. [14]

Wawancara merupakan salah satu proses mengumpulkan data yang sering digunakan pada penelitian secara kualitatif. Wawancara harus mempunyai tujuan dan biasanya dimulai dengan pertanyaan pertanyaan yang bersifat informal. Semua percakapan mempunyai kendali atau peralihan oleh satu partisipan lainnya, wawancara ditujukan supaya mendapatkan informasi hanya dari satu sisi saja[15].

Kuisioner merupakan proses pengumpulan data dengan metode survei sehingga dapat mengumpulkan opini dari para responden. Kuisioner dapat dikirimkan langsung oleh peneliti jika hanya membutuhkan responden yang tidak banyak/tidak terlalu luas jangkauannya. Kuisioner juga bisa dikirimkan melalui pos maupun e-mail untuk menghemat pengeluaran biaya. Pertanyaan-pertanyaan pada kuisioner juga harus dirancang secara terbuka maupun tertutup. Pertanyaan tertutup dapat memudahkan analisa karena akan mengurangi variablitias tanggapan responden [16].

2.2.3 Definisi Informasi

Informasi merupakan kumpulan data - data yang sudah diterjemahkan menjadi sebuah bentuk yang lebih berguna untuk penerima. Data adalah sumber informasi, Data menggambarkan kejadian dan kesatuan yang nyata. Kejadian (*event*) merupakan kejadian yang terjadi hanya pada saat saat tertentu. Informasi meruapan data yang diolah sehingga mempunyai nilai yang nyata ataupun dapat dirasakan bagi penerima dan dapat berguna untuk membuat keputusan saat ini maupun

keputusan untuk masa mendatang [12]. Informasi memiliki fungsi untuk menambah pengetahuan ataupun meminimalisir keraguan dalam memakai sebuah informasi. Informasi berguna untuk memberikan visualisasi pada suatu masalah sehingga pengambilan keputusan bisa dilakukan dengan lebih cepat. Informasi dapat juga digunakan untuk memberi sebuah aturan, standar, maupun indikator bagi pengambil keputusan.

2.2.4. Keamanan Informasi

Keamanan informasi merupakan bagaimana pencegahan penipuan ataupun setidaknya mendeteksi penipuan pada sebuah sistem yang basisnya informasi. Keamanan tidak bisa muncul secara tiba tiba. Keamanan harus direncanakan dengan baik dan benar supaya bisa maksimal. Pengelolaan pada keamanan bisa dilihat pada sisi pengelolaan risiko (*risk management*) menggunakan "Risk Management Model" untuk mengelola ancaman-ancaman. Untuk mengurangi risiko, dilakukanlah *countermeasures* contohnya adalah usaha untuk mengurangi *threat*, usaha untuk mengurangi *vulnerablility*, dan usaha untuk bisa mendeteksi kejadian - kejadian yang tidak bersahabat (*hostile event*) [17]

2.2.5 Aspek Keamanan

Keamanan komputer mencakup 4 aspek keamanan yang merupakan privasi (*privacy*), integritas (*integrity*), autentifikasi (*authentication*), dan ketersediaan (*availability*) [18]

1. Privasi: aspek privasi merupakan usaha untuk menjaga keamanan informasi dari orang-orang yang tidak mempunyai hak akses. privasi biasanya mengarah ke data yang bersifat privat contohnya adalah email, password, nama orang tua, dan lain - lain.

2. Integritas: aspek integritas merupakan aspek yang menekankan bahwa informasi tidak boleh diubah secara sembarangan, harus dengan seijin

pemilik informasi. contohnya adalah sebuah email dapat di *intercept*saat sedang dikirimkan ke penerima. Isi email tersebut dapat diubah kemudian dapat diteruskan ke alamat tujuan sehingga integritas dari email tersebut sudah tidak bisa dijaga.

3. Autentifikasi: aspek ini digunakan untuk menyatakan sebuah informasi adalah asli. yang dimaksud asli disini adalah orang yang memberikan informasi dan orang yang mengakses adalah orang yang dimaksud dengan isi informasi yang sebenar benarnya.
4. ketersediaan: aspek ini berhubungan dengan ketersediaan sebuah informasi saat dibutuhkan. contoh hambatan adalah serangan DoS yang dimana permintaan server dikirim permintaan palsu yang sangat banyak sehingga terjadi lemot, *hang*, maupun *system crash*.

2.2.5 Kejahatan Komputer

Kejahatan komputer merupakan tidakan yang ilegal dalam penggunaan komputer untuk kejahatan seperti pencurian perangkat lunak maupun keras, manipulasi data, mengakses sistem komputer dengan ilegal, dan lain - lain. Kejahatan komputer bisa diklasifikasikan menjadi 4 yaitu[19].

1. Keamanan fisik (*physical security*): keamanan fisik contohnya adalah akses orang ke perusahaan, media, dan peralatan yang dipakai. Para penjahat komputer (*crackers*) sering mencari berkas berkas di tempat tempat yang tidak terduga contohnya adalah tempat sampah, misalnya tulisan tulisan yang berisi password maupun manual yang langsung dibuang tanpa dihancurkan terlebih dahulu.
2. Keamanan orang (personel): keamanan orang seperti identifikasi data diri, dan profil seseorang yang mempunyai akses masuk keruangan tertentu. kelemahan pada keamanan sistem informasi

seringkali bergantung pada manusia (pengelola dan pemakai). *social engineering* seringkali digunakan oleh kriminal yang seakan-akan dirinya yang berhak mengakses informasi.

3. Keamanan data, media, dan teknik komunikasi: keamanan kelas ini merupakan kelemahan dalam software yang dipakai pada suatu komputer, seorang kriminal bisa saja memasang *virus* ataupun *trojan horse* supaya informasi informasi penting dapat dikumpulkan walaupun sebenarnya kriminal tersebut tidak berhak untuk mendapatkan akses.
4. Keamanan dalam operasi: keamanan dalam operasi ini meliputi kebijakan kebijakan yang mengatur sebuah sistem keamanan dan juga meliputi *post attack recovery*. *post attack recovery* merupakan rangkaian kebijakan ataupun prosedur yang digunakan jika terjadi serangan, seringkali perusahaan belum memiliki kebijakan ini.

2.2.6 Kerangka Kerja ISO 27002:2013

Penelitian ini menggunakan kerangka kerja ISO 27002:2013 sebagai pedoman dalam melakukan analisa risiko keamanan sistem informasi dimana ISO 27002:2013 sudah disusun dalam standarisasi kontrol yang sesuai dengan kebutuhan perusahaan. Terdapat 14 klausa kontrol yang sudah distandarisasi mulai dari nomor 5 sampai dengan 18, dimulai dari:

5. *Information security policies* menilai bagaimana organisasi mengungkapkan niatnya terkait dengan keamanan sistem informasi.
6. *Organization of information security* menilai bagaimana organisasi mengelola keamanan informasi pada perusahaan dan bagaimana kepempimpinan organisasi memberikan dukungan dan arahan secara keseluruhan.

7. *Human resources security* menilai bagaimana organisasi menetapkan syarat karyawan terpenuhi untuk mengerti akan peran dan tanggung jawab pekerjaan dan akses tersebut dihapuskan setelah tidak lagi bekerja diperusahaan.

8. *Asset management* menilai bagaimana manajemen asset organisasi, termasuk cara untuk identifikasi, melacak, klasifikasi, dan penetapan hak kepemilikan aset perusahaan.

9. *Access Control* menilai penggunaan keamanan administrative, fisikal, maupun teknikal pada organisasi untuk mengenola proses konuminkasi sistem dan pengguna.

10. Cryptography menilai kebijakan organisasi tentang penggunaan kriptografi (enkripsi).

11. *Physical and environmental security* menilai langkah organisasi untuk melakukan perlindungan pada sistem maupun infrastruktur bangunan terhadap potensi adanya ancaman yang dapat terjadi.

12. *Operations security* menilai kebijakan, prosedur, dan kontrol organisasi dalam perlindungan sistem.

13. *Communications security* menilai kebijakan, prosedur, dan kontrol organisasi dalam manajemen jaringan.

14. *System acquisition, development, and maintenance* menilai apakah organisasi mempunyai persyaratan keamanan yang ditetapkan sebagai bagian dari pengembangan maupun implementasi sistem informasi.

15. *Supplier relationships* menilai bagaimana organisasi berinteraksi dengan pihak ketiga untuk mengamankan sumber daya informasi dan teknologi yang diakses, diproses, dan dikelola oleh pihak ketiga.

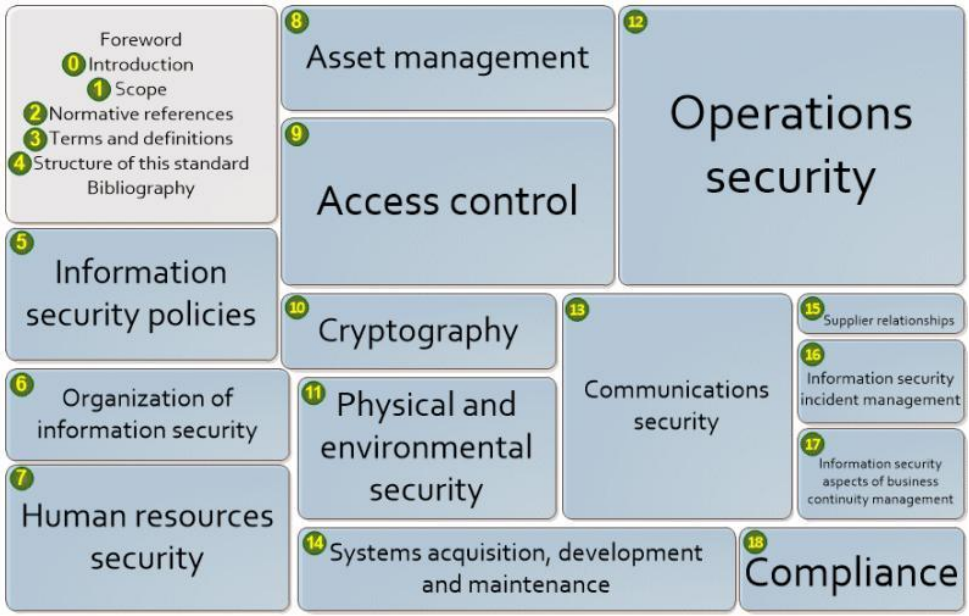
16. *Information security incident management* menilai program keamanan informasi organisasi dalam memanajemen peristiwa keamanan. Program yang baik akan memastikan karyawan dilatih

untuk mendeteksi, melaporkan, dan menanggapi kejadian yang tidak diinginkan.

17. *Information security aspects of business continuity* menilai manajemen kelangsungan bisnis organisasi. Sebuah organisasi yang matang harus memiliki kepastian kelangsungan organisasi maupun dalam keadaan luar biasa termasuk pemeliharaan Langkah – Langkah untuk memastikan keamanan sumber daya informasinya.

18. *Compliance* menilai proses organisasi untuk tetap mengikuti persyaratan hukum dan kontrak dalam melindungi aset informasi yang bersifat sensitif.

Kontrol ISO 27002:2013 dapat dilihat pada gambar 2.1 dibawah ini [20]:



Gambar 2.1 Kontrol ISO 27002:2013