BAB II
LANDASAN TEORI

2.1 Analisis

Analisis adalah sebuah aktivitas berfikir guna menjelaskan atau menyelesaikan sebuah permasalahan dari satu kesatuan menjadi unit terkecil [6]. Pengertian lain dari analisis yaitu, Analisis merupakan sebuah aktivitas guna menemukan sebuah pola, selain itu, analisis merupakan suatu cara berpikir yang menitikberatkan pada penentuan struktur dan tatanan yang jelas dari bentuk sesuatu yang dideskripsikan. [7]. Untuk mendefinisikan suatu subjek secara tepat dan memahami maknanya secara keseluruhan, analisis memerlukan pemecahan subjek menjadi beberapa bagian dan mengamati bagian-bagian tersebut serta hubungannya satu sama lain [8].

Pendapat lain mengenai analisis yaitu, Analisis merupakan aktivitas yang didalamnya terdapat beberapa kegiatan antara lain mengurai, membedakan, memisah-misahkan sesuatu untuk nantinya diklasifikasikan ulang sesuai kriteria tertentu yang sesuai selanjutnya ditetapkan hubungannya dan diterjemahkan maknanya [9]. Anaisis merupakan sekumpulan aktivitas dan proses [10]. Pada kegiatan ini termasuk di dalamnya banyak indikator antara lain mengidentifikasi, menyelidiki, mengkategori, membedakan dan juga merekonstruksi [11]. Analisis dapat dilakukan dalam berbagai konteks, termasuk ilmu pengetahuan, matematika, bisnis, ekonomi, dan banyak lagi. Alasan utama dilakukannya analisis adalah untuk memperoleh pemahaman lebih jauh terhadap suatu permasalahan atau keadaan sehingga pilihan dapat diambil.

2.2 Keamanan Informasi

Keamanan informasi tidak boleh diabaikan, yang saat ini masih jarang diprioritaskan oleh pemerintahan, perusahaan, atau organisasi sebagai penanggung jawab informasi [12]. Oleh sebab itu, maka diperlukan suatu manajemen berbentuk seperti prosedur kerja untuk memastikan keamanan informasi [13]. Upaya untuk melindungi dan menjaga aset informasi dari berbagai ancaman yang disengaja, terencana, dan tidak disengaja yang berasal dari semakin besarnya risiko kerugian yang ditimbulkan oleh penggunaan teknologi informasi dan komunikasi (TIK), yang dapat membahayakan privasi, integritas, dan ketersediaan layanan, disebut keamanan informasi [12]. Penegertian lain mengenai keamanan informasi yaitu, keamanan informasi memiliki untuk menjaga aset informasi suatu organisasi dari potensi ancaman data dan kerentanan keamanan informasi guna menjamin dan menjaga kelangsungan bisnis organisasi.[13].

Keamanan informasi adalah proses menjaga data penting perusahaan dari akses tidak sah, modifikasi program, perampokan, dan kerusakan perangkat keras pada sistem informasi, prosedur, dan prosedur teknis [14]. Keamanan informasi adalah pertimbangan penting bagi setiap perusahaan dalam situasi ini [15]. Menjaga keamanan informasi adalah isu krusial yang membutuhkan evaluasi serius dari seluruh jajaran organisasi [16]. Dalam hal menjaga informasi dalam organisasi atau bisnis, keamanan informasi memainkan peran penting. Ketersediaan sistem informasi yang berkelanjutan dapat terancam jika keamanan informasi suatu lembaga pemerintah tidak dikelola dengan baik [17]. Sama juga halnya di lembaga pendidikan seperti universitas, ketika keamanan informasi kurang dikelolah dengan baik dapat mengancam kelangsungan penggunaan sistem informasi. Perusahaan

harus menerapkan sistem manajemen keamanan informasi untuk menghentikan hal-hal terkait kebocoran informasi yang merugikan bisnis [18]. Keamanan dapat diperoleh melalui berbagai cara atau strategi, sering kali dilakukan secara bersamaan atau bersamaan satu sama lainnya [19].

2.3 Keamanan Sistem Informasi

Keamanan suatu sistem informasi sangat penting untuk keamanannya [20]. Keamanan umumnya bisa diartikan atau didefinisikan sebagai kualitas atau keadaan aman untuk bebas dari bahaya [20]. Keamanan sistem informasi merupakan segala upaya dalam rangka untuk mencegah dan melindungi sistem informasi dari ganguan bermacam pihak yang tidak diinginkan [21]. Keamanan jaringan atau sistem informasi sangat dipengaruhi oleh adanya bermacam pengaruh atau tindakan yang meresahkan yang bisa mengakibatkan terungkapnya data penting dan rahasia dan selanjutnya berkurangnya kinerja [22]. Ada berbagai jenis ancaman, gangguan, atau serangan terhadap keamanan jaringan atau sistem data, misalnya serangan orang dalam, penyadapan, konfigurasi yang buruk, serangan man-in-the-middle, serangan virus atau serangan penolakan layanan dan lain-lain [22]. Keamanan sistem informasi adalah data yang merupakan salah satu sumber daya penting yang harus dijaga atau dijaga keamanannya [23].

2.4 Standar ISO 27002:2013

Standar ISO/IEC 27002:2013 adalah nama terbaru yang sebelumnya diberi nama ISO/IEC 17799:2005 [24]. ISO/IEC 27002:2013 merupakan panduan standar keamanan informasi organisasi dan penerapan pengaturan keamanan informasi,

pengaturan ini mencakup pemilihan, penerapan, dan pengelolaan pengendalian yang disiapkan untuk digunakan oleh organisasi dengan mempertimbangkan risiko keamanan informasi di lingkungan [24]. ISO/IEC 27002:2013 di dalanya terdapat 14 klausul dalam 35 kategori keamanan utama dan 114 kendali/kontrol keamanan [24]. 14 klausul dari ISO 27002:2013 sebagai berikut:

Tabel 2.1 Klausul ISO 27002:2013

ISO 27002:2013	
Klausul Kontrol Keamanan	
5	Kebijakan keamanan informasi
6	Keamanan informasi organisasi
7	Keamanan sumber daya manusia
8	Pengelolaan aset
9	Kontrol akses
10	Kriptografi
11	Keamanan fisik dan lingkungan
12	Keamanan operasional
13	Keamanan komunikasi
14	Akuisisi, pengembangan dan pengelolaan sistem
15	Hubungan dengan supplier
16	Pengelolaan insiden keamanan informasi
17	Keamanan informasi dari aspek pengelolaan keberlangsungan bisnis
18	Kepatuhan

[Sumber: K. Kailla, R. Y. Fakultas, and R. G. Utomo, "Pengukuran Implementasi Information Assurance Pada Dinas Kependudukan dan Pencatatan Sipil Menggunakan Framework IAFEG," e-Proceeding Eng., vol. 10, no. 2, pp. 2071–2081, 2023.]

2.5 Perbedaan Standar ISO 27002:2013 dan Standar ISO 27002:2022

Perbedaan Standar ISO 27002:2013 dan Standar ISO 27002:2022 adalah pada ISO/IEC 27002:2013 di dalamnya terdapat 14 klausul dalam 35 kategori keamanan utama dan 114 kendali/kontrol keamanan [24], Sedangkan untuk ISO 27002:2022, jumlah kontrol keamanan dikurangi dari 114 menjadi 93 dan kini dikelompokkan dalam 4 domain utama:

1. Orang (8 kontrol)
2. Organisasi (37 kontrol)
3. Teknologi (34 kontrol)
4. Fisik (14 kontrol)

Kontrol baru yang dirilis dengan 27002:2022 meliputi:

Nomor	Klausul kontrol keamanan
5.7	Intelijen ancaman
5.23	Keamanan informasi untuk penggunaan layanan cloud
5.30	Kesiapan TIK untuk kelangsungan bisnis
7.4	Pemantauan keamanan fisik
8.9	Manajemen konfigurasi
8.10	Penghapusan informasi
8.11	Penyembunyian data
8.12	Pencegahan kebocoran data
8.16	Kegiatan pemantauan
8.23	Pemfilteran web
8.28	Pengkodean yang aman

2.6 SSE-CMM

SSE-CMM (*System Security Engineering - Capability Maturity Model*) merupakan metode penghitungan yang digunakan untuk menilai tingkat keamanan, mengembangkan proses seperti proses rekayasa dan proses non-teknis [25]. SSE-CMM terdiri dari dua bagian [25], yaitu:

1. Model untuk rekayasa keamanan proses, proyek dan organisasi.
2. Metode penilaian untuk mengetahui tingkat keamanan proses.

SSE-CMM adalah model yang dipakai guna mensurvei tingkat kedewasaan atau kematangan di bidang keamanan sistem. Model ini mempermudah organisasi untuk mengevaluasi dan meningkatkan tingkat keamanan mereka dengan cara menilai sejauh mana proses-proses keamanan, baik yang bersifat teknis maupun non-teknis,

telah terintegrasi dan dikelola secara efektif. Dengan memakai SSE-CMM, organisasi bisa mengembangkan rencana perbaikan yang terstruktur guna mencapai tingkat kedewasaan keamanan yang lebih tinggi.

Kerangka pengakuan yang mencerminkan tingkat kematangan, atau tingkat pengelompokan kemampuan perusahaan, dapat digunakan untuk mengidentifikasi dan mengevaluasi kemampuan organisasi dalam mencapai tingkat keamanan informasi yang tinggi [25], seperti yang diterangkan dalam tabel 2.2.

Tabel 2.2 *Index* Penilaian Pada Tingkat Kematangan

Level	Range	Keterangan
0	0 – 0.50	Non-Existent
1	0.51 – 1.50	Initial / Ad Hoc
2	1.51 – 2.50	Repeatable But Invinitve
3	2.51 – 3.50	Define Process
4	3.51 – 4.50	Managed and Measurable
5	4.51 – 5.00	Optimized

[Sumber: A. Rosadi and B. A. Wardijono, "Analysis of System Security Levels of Tax Payment and Regional Retribution Based on ISO / IEC27002: 2013 Standard Using SSE-CCM," *Int. Res. J. Adv. Eng. Sci.*, vol. 6, no. 1, pp. 205–211, 2021, [Online]. Available: http://irjaes.com/wp-content/uploads/2021/02/IRJAES-V6N1P175Y21.pdf]

SSE-CMM memiliki lima tingkat kemampuan, seperti yang ditunjukkan pada tabel 2.2, untuk memperlihatkan tingkat kematangan proses, berikut ini semua rinciannya [25]:

a. Tingkat 0 tidak semua prosedur dasar dilaksanakan.
b. Tingkat 1 seluruh praktek dasar dilaksanakan namun secara informal, yang artinya Ini berarti bahwa tidak ada catatan tertulis, tidak ada standar dan dilaksanakan secara terpisah.
c. Tingkat 2 *planned* and *tracked* yang menunjukkan dedikasi untuk merencanakan proses standar.

d. Tingkat 3 *well defined* yang artinya proses standar telah dijalankan sesuai dengan ketentuan yang telah ditetapkan.
e. Tingkat 4 dikendalikan secara kuantitatif, ini berarti peningkatan kualitas dicapai melalui pemantauan setiap proses secara berkala.
f. Tingkat 5 ditingkatkan secara berkelanjutan, menunjukkan bahwa standar sudah optimal dan berfokus pada penyesuaian terhadap perubahan.

Skor antara 0 dan 5 diberikan untuk setiap area proses yang dipilih menggunakan metode SSE-CMM.

2.7 Enkripsi *End-to-end*

Enkripsi *End-to-End* merupakan sebuah teknik enkripsi data yang dilaksanakan pada saat data akan dikirimkan (pengirim) dan kembali didekripsikan ketika pesan sampai di tujuan (penerima) [26]. Enkripsi adalah strategi yang digunakan untuk menyandikan informasi sehingga keamanan data tetap terjaga dan tidak dapat dibaca tanpa mengacaknya terlebih dahulu (kebalikan dari proses enkripsi) [27]. Dari pengertian diatas bisa diperjelas lagi bahwa Enkripsi *end-to-end* adalah suatu teknik keamanan yang dipakai guna melindungi data sewaktu proses pertukaran atau komunikasi dari satu ujung (pemancar) ke ujung lain (penerima). Dalam lingkup enkripsi *end-to-end,* data dienkripsi di sumber dan hanya dapat didekripsi oleh penerima, sehingga hanya pemilik kunci dekripsi yang bisa mengakses konten yang sebenarnya.

2.8 Metodologi Penelitian

2.8.1 *State Of Nature*

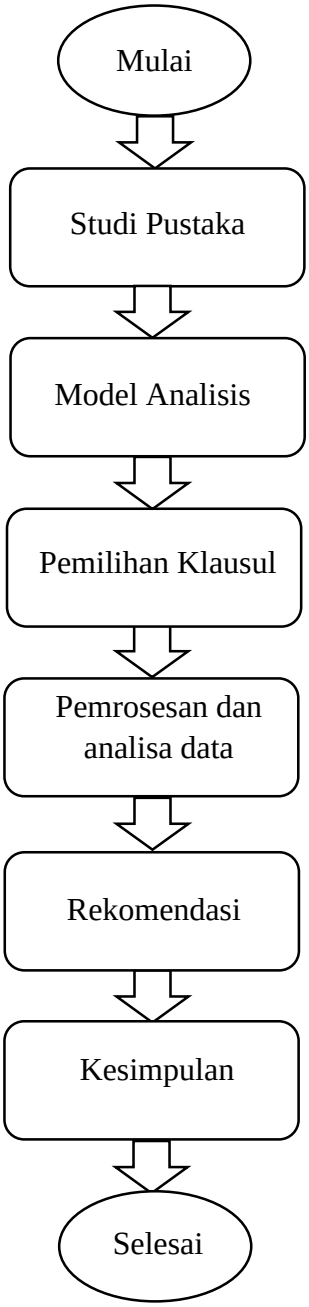
Tabel 2.3 *State Of Nature*

Referensi Penelitian	1
Judul	Analisis Tingkat Keamanan Aplikasi SIMAK Menggunakan Standard ISO/IEC 27002:2013 (Studi Kasus: UPTTIK Universitas Siliwangi)
Nama Penulis	Iyos Rosidin Pajar
Tahun	2021
Hasil	Kontrol keamanan yang diidentifikasi dalam ISO/IEC 27002:2013 dapat digunakan untuk mengevaluasi tingkat kematangan keamanan suatu aplikasi atau sistem informasi. Responden dalam penelitian ini adalah para pekerja dan kepala UPTTIK yang teliti serta individu yang dianggap memahami kondisi khusus dari kerangka data atau aplikasi SIMAK. Hasil dari kuesioner akan digunakan sebagai dasar untuk menilai tingkat kematangan keamanan aplikasi. Selanjutnya, pembobotan dilakukan pada setiap kontrol keamanan yang diperoleh dari masing-masing responden, dan rata-rata dari semua nilai yang diperoleh dari setiap kontrol keamanan dihitung. Dari keempat domain yang digunakan dalam penelitian ini, disimpulkan bahwa aplikasi SIMAK Universitas Siliwangi memiliki nilai kematangan sebesar 1,57, yang menunjukkan bahwa aplikasi tersebut berada pada level repeatable.
Referensi Penelitian	2
Judul	Analisis Tingkat Keamanan Sistem Pembayaran Pajak dan Retribusi Daerah Berdasarkan Standar ISO/IEC27002:2013 Menggunakan SSE-CCM (*Analysis of System Security Levels of Tax Payment and Regional Retribution Based on* ISO / IEC27002: 2013 *Standard Using* SSE-CCM)

Nama Penulis	Aburizal Rosadi dan Bheta Agus Wardijono
Tahun	2021
Hasil	Berdasarkan hasil pengolahan data berikut ini dapat disimpulkan: 1. Implementasi standar ISO 27002:2013 pada sistem *online* pembayaran pajak dan retribusi di DKI Wilayah Jakarta berada di level 4, atau dikontrol secara kuantitatif, berarti setiap proses dipantau untuk meningkatkan kualitas. 2. Sistem komunikasi memakai API ke sistem bank yang dimiliki sudah dinyatakan aman sebab mengimplementasikan kriptografi dan memakai standar ISO 8583, tetapi API untuk pertukaran data ke sistem dan aplikasi bapenda guna pemetaan data dari wajib pajak menuju *database* sistem belum menerapkan kriptografi. 3. Sistem sudah menerapkan pencadangan *database* dan pendaftaran izin pengguna yang bisa mengakses *database* dan aplikasi secara langsung dengan pengguna yang berbeda izin.
Referensi Penelitian	3
Judul	Evaluasi Tata Kelola Keamanan Informasi Berdasarkan Standar ISO/IEC 27001:2013 dengan Menggunakan Model SSE-CMM (*System Security Engineering Capability Maturity Model*) pada Perusahaan Daerah Air Minum Surya Sembada Kota Surabaya
Nama Penulis	Dimas Pramudya Haqqi, Khakim Ghozali, dan Raden Venantius Hari Ginardi
Tahun	2022
Hasil	Dari penelitian ini, kesimpulan dapat diungkapkan sebagai berikut: 1. Berdasarkan Maturity Level, rata-rata dari 4 klausul ISO/IEC 27001:2013 yang digunakan adalah sebesar 3,5. Hasil perhitungan Maturity Level tersebut menunjukkan bahwa kategori yang dicapai adalah "Well Defined," yang berarti bahwa kinerja pada level ini dilaksanakan sesuai dengan persetujuan dan standar yang telah ditetapkan. Proses tersebut sudah didokumentasikan, direncanakan, dan dikelola menggunakan standar yang telah ditetapkan oleh organisasi.

	2. Didapatkan beberapa kesenjangan (gap) yang diperoleh oleh penulis. 3. Penulis menemukan beberapa kekurangan karena kegiatan belum memiliki pedoman dan sistem pelaksanaan yang jelas dalam pelaksanaannya. 4. Beberapa kontrol keamanan direkomendasikan berdasarkan temuan penulis dari penelitian ini.

2.8.2 Kerangka Kerja Penelitian



Gambar 2.1 Kerangka Kerja Penelitian