BAB II
LANDASAN TEORI

2.1. *Cloud Computing*

2.1.1. Definisi *Cloud Computing*

Cloud computing atau komputasi awan adalah salah satu bentuk teknologi informasi yang banyak digunakan pada bidang jaringan komputer atau internet. *Cloud computing* terdiri dari perangkat keras komputer, perangkat jaringan komputer" [12]. Penelitian lainnya menjelaskan bahwa *cloud computing* adalah model untuk memungkinkan akses jaringan di mana-mana, nyaman, sesuai permintaan ke kumpulan sumber daya komputasi yang dapat dikonfigurasi bersama (misalnya, jaringan, *server*, penyimpanan, aplikasi, dan layanan) yang dapat dengan cepat disediakan dan dirilis dengan upaya manajemen minimal atau interaksi penyedia layanan [13]. Komputasi awan adalah paradigma komputasi yang terdistribusi berskala besar dan didorong oleh skala ekonomi, sebuah kumpulan abstraksi, tervirtualisasi, penyimpanan, *platform*, dan diberikan sesuai permintaan kepada pelanggan *eksternal* melalui internet [14]. *Cloud computing* juga memiliki jenis-jenis yang membedakan dari segi layanan maupun jenis kepemilikannya.

2.1.2. Service Model *Cloud Computing*

Menurut Saurabh Singh *cloud* memiliki 4 model layanan [15] :

1. *Infrastructure as a Service (IaaS)* , lapisan layanan ini memberikan elastisitas mengalokasikan sumber daya fisik atau *virtual* membantu menyediakan infrastruktur secara abstrak. Ini juga menyediakan skalabilitas dan ketentuan (seperti *hypervisor*) masalah infrastruktur tanpa perlu menghabiskan sejumlah besar dana dan waktu. IaaS juga berfokus pada bidang keamanan seperti *firewall*, deteksi intrusi, dan pencegahan (IDS / IPS), *monitor* mesin *virtual.*
2. *Platform as a Service (PaaS)* adalah *middleware* dari model layanan dan memberikan layanan dalam bentuk alat pengembangan, kerangka kerja, arsitektur, program, dan *Integrated Development Environments (IDE*). Dengan kata lain, pelanggan dapat mengendalikan aplikasi tetapi tidak memiliki sarana untuk mengelola infrastruktur yang mendasarinya. Ini dapat membantu dalam situasi di mana beberapa pengembang yang berlokasi di lokasi fisik yang berbeda perlu bekerja bersama. Penyedia PaaS yang populer adalah *Google App Engine.*
3. *Software as a Service (SaaS)* adalah kumpulan layanan komputasi jarak jauh. SaaS berada pada model teratas di antara model pengiriman. Hal ini memungkinkan aplikasi untuk digunakan dari jarak jauh oleh vendor pihak ketiga. Hal ini memungkinkan pelanggan untuk menggunakan aplikasi penyedia layanan *cloud*/CSP yang berjalan di infrastruktur *cloud* melalui internet.

SaaS adalah pasar *cloud* yang lazim dan masih terus tumbuh dengan cepat.

4. *Anything as a Service (AaaS),* istilah kolektif yang menggabungkan sejumlah hal sebagai X sebagai layanan. X dapat berupa apa saja atau semuanya sebagai layanan. Layanan ini menjadi dipertukarkan dalam *cloud landscape*. Sistem *cloud* dapat mendukung sumber daya yang besar untuk persyaratan spesifik, pribadi dan granular menggunakan *Monitor as a Services (MaaS), Data as a Service (DaaS), Communication as a Service (CaaS), Security as a Service (SecaaS), Routing as a Service (RaaS).*

   Pada *cloud computing* juga terdapat istilah-istilah yang digunakan dalam menyebut jenis *cloud* dalam model penyebarannya seperti ; *public cloud, private cloud, community cloud, hybrid cloud.*

2.1.3. *Deployment Model Cloud Computing*

Berdasarkan buku CSA *Guide to Cloud Computing*, terdapat 4 kategori yang membedakan sebagai berikut [16]:

1. *Public Cloud,* layanan ini tersedia untuk masyarakat umum, yang dapat mengakses layanan melalui Internet. Infrastruktur dikelola dan dimiliki oleh CSP dengan infrastruktur yang terletak di luar tempat pelanggan. Selain itu, pelanggan tidak dipercaya, yang berarti bahwa mereka belum tentu merupakan bagian dari satu organisasi dan kemungkinan besar bahkan tidak akan mengetahui pelanggan *cloud* lainnya sama sekali.

Contoh umum termasuk layanan *email*, seperti Hotmail, Apple i*Cloud*, atau layanan penyimpanan seperti Dropbox.

2. *Private Cloud,* dalam penyebaran *private cloud*, infrastruktur ,*platform*, *software* dapat dikelola dan dimiliki oleh *end costumer* atau CSP. Demikian pula, infrastruktur mungkin terletak di dalam atau di luar *premise*; namun, pelanggan akan memiliki kendali atas lokasi geografis spesifiknya. Poin khusus ini menjadikan *cloud* pribadi sebagai model pilihan untuk meng*hosting* data yang diatur (misalnya, informasi yang dapat diidentifikasi secara pribadi), dan dengan demikian mungkin memiliki batasan tempat penyimpanannya.
3. *Community Cloud,* jenis *cloud* ini sendiri merupakan perluasan konsep dari *cloud* pribadi dengan menggabungkan banyak pelanggan dengan pengguna yang bertujuan sama. Karena itu, *cloud* jenis ini memiliki beberapa karateristik yang mirip dengan *private cloud* salah satu contohnya adalah *cloud* ini adalah ada kolaborasi antar pemangku dengan kepentingan yang sama dan melalui proses otorisasi hanya dengan pihak terpercaya yang diberikan akses ke data.
4. *Hybrid Cloud,* jenis *cloud* berada di antara *private cloud* dan *public cloud*. Salah satu contohnya adalah implementasi M-*Cloud* di Maldova yang memiliki tujuan mengultilisasi sebuah *cloud platform* dan menyediakan *platform* terpusat dan nantinya akan di berikan ke layanan publik. Pendekatan ini akan menggunakan satu pusat data yang dibandingkan dengan 100 data pusat berbeda yang saat ini menyediakan layanan publik.

Merupakan pendekatan *hybird* karena beberapa layanan bersifat publik maupun *private*, contohnya seperti yang menyediakan sumber daya untuk warga negara ada yang terbuka secar publik dan ada juga yang hanya untuk *internal*/privasi sendiri saja.

2.2. Audit Sistem Informasi

2.2.1. Definisi Audit Sistem Informasi

Berikut pengertian audit sistem informasi menurut para ahli:

1. Menurut Nanang Sasongko audit sistem informasi adalah sebuah proses sistematis dalam mengumpulkan dan mengevaluasi bukti-bukti untuk menunjukan bahwa sistem informasi yang digunakan oleh sebuah organisasi telah mencapai tujuannya [17].
2. Audit sistem informasi adalah penekanan pada beberapa aspek penting, yaitu pemeriksaan dilakukan untuk menilai apakah sistem komputerisasi organisasi dapat mendukung pengamanan aset, mendukung pencapaian tujuan organisasi, sudah memanfaatkan sumber daya secara efisien, serta apakah terjamin konsistensi dan keakuratan datanya [18]
3. Audit sistem informasi merupakan tinjauan pengendalian umum dan aplikasi untuk menilai pemenuhan kebijakan dan prosedur pengendalian *internal* serta keefektivitasannya untuk menjaga asset [19].

2.2.2. Tujuan Audit Sistem Informasi

Menurut Safira tujuan audit Sistem Informasi adalah sebagai berikut[20]:

1. Mengamankan aset, aset yang merupakan perangkat keras, perangkat lunak, manusia, data, berkas-berkas, dokumentasi.
2. Menjaga integritas data, tanpa menjaga integritas data, organisasi tidak dapat memperlihatkan gambaran dirinya dengan benar atau kejadian yang ada tidak terungkap seperti apa adanya.
3. Menjaga efektifitas sistem, sistem informasi dikatakan efektif hanya jika sistem tersebut dapat mencapai tujuannya. perlu upaya untuk mengetahui kebutuhan pengguna sistem tersebut (*user),* apakah sistem menghasilkan laporan atau informasi yang bermanfaat bagi *user.*
4. Efisiensi, dikatakan efisien jika audit sistem informasi menggunakan sumberdaya seminimal mungkin untuk menghasilkan *output* yang dibutuhkan.

2.2.3. Tahapan Audit Sistem Informasi

Dalam bukunya Angel R.Otero menjelaskan tahapan dalam audit / *audit phase* sebagai berikut [1]:

1. *Risk Assessment* ,tahapan ini merupakan tahapan fondasi dalam audit karena pada tahapan ini membantu dalam membuat proses *planning* audit individu. *Risk assessment* yang efektif membuat proses audit lebih

fleksibel dan efisien dalam perusahaan bertemu akan adanya perubahan seperti : mengidentifikasi *area risk* baru, mengidentifikasi adanya perubahan pada *area risk* yang sudah ada, mengambil keuntungan dari informasi yang didapat untuk meningkatkan *risk assessment.*

2. *Audit Plan* ,tahapan ini adalah hal yang mendasar dan dibutuhkan untuk menjelaskan apa yang harus dicapai oleh proses audit seperti, pengeluaran waktu dan biaya, dan menetapkan prioritas sesuai dengan tujuan dan aturan yang ada di perusahaan. Objektif dari audit *plan* adalah mengoptimalkan pemanfaatan sumber audit dengan alokasi biaya dan waktu yang tepat.
3. *Preliminary Review,* pada tahap ini auditor harus mendapatkan pembahasan rangkuman informasi dan mengevaluasi hal tersebut dengan objektif dari audit sendiri. Tujuan dari tahap ini adalah membahas keterikatan IT audit dalam memahami lingkungan IT di perusahaan. Auditor melakukan *interview* secara personal untuk memahami aturan dan praktisi yang ada di perusahaan.
4. *Design Audit Procedures,* pada tahap ini auditor harus menyiapkan program audit bagi *area* yang mau dilakukan audit, memilih kontrol *area* dari framework yang sudah dipilih untuk setiap *area* dalam melakukan proses audit. Program audit adalah *plan* yang bersifat *formal* untuk melakukan *review* dan mengetes setiap *area* yang memiliki dampak yang signifikan terhadap kontrol.

5. *Test Controlss,* tahapan ini memiliki proses seperti memeriksa dokumentasi, serta wawancara, inspeksi, dan observasi yang dilakukasn secara personal.
6. *Substantive Testing,* ketika kontrol yang digunakan dinilai tidak efektif, tahapan ini dibutuhkan untuk membuktikan akurasi dan kelengkapan dari informasi yang didapat dari proses ataupun aplikasi. Test ini didesain untuk menjalankan pembuktian proses verifikasi keakuratan fungsi, efesiensi, dan kontrol dari subjek yang diaudit.
7. *Document result* , tahapan selanjutnya adalah tahap yang menyangkut tentang hasil dokumentasi atas pekerjaan yang telah dilakukan , juga melaporkan hasil dari penemuan audit. Hasil audit harus memiliki deskripsi penemuan audit, kesimpulan, dan rekomendasi.
8. *Communication* , pada tahapan akhir audit lebih baik membicarakan kesimpulan dan penemuan audit kepada *IT Management* untuk mendapatkan persetujuan agar dapat melakukan aksi pembenaran terhadap penemuan audit.

2.3. *Cloud Controls Matrix* (CCM) v3.0.1

Control Domain	CCM V3.0 Control ID	Updated Control Specification	Architectural Relevance					
			Phys	Network	Compute	Storage	App	Data
Application & Interface Security Application Security	AIS-01	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.			X	X	X	X
Application & Interface Security Customer Access Requirements	AIS-02	Prior to granting customers access to data, assets, and information systems, identified security, contractual, and regulatory requirements for customer access shall be addressed.	X	X	X	X	X	X

Gambar 2. 1 Contoh Kerangka CCM

CCM adalah seperangkat kontrol keamanan komprehensif pada *cloud* yang di dalamnya terdapat matriks yang telah disesuaikan dengan arahan dari *Cloud Security Alliance*. CSA telah melakukan kajian ulang terhadap standar yang ada sejak tahun 2008, mengumpulkan hasil-hasil dari metrik (CCM) yang menghubungkan *framework* yang ada melalui daftar detail tentang *cloud assurance control.* CSA menjebatani jarak antara perusahaan pada umumnya dengan standar pemerintahan dengan menawarkan *framework* yang dibuatnya sebagai standar yang kuat [21].

Kontrol pada matrik ini didasarkan dari standar, regulasi dan *framework* kontrol kemanan industri seperti ISO 27001/27002, GAPP, PCI DSS, NIST, NZISM , COBIT dan CSA *guidance* [3].

Pada tabel 1.1 *Table* Kontrol terdapat tabel yang berisi 16 *domain*. Berikut penjelasan singkat dari 8 *domain* terpilih [16] :

1. *Application & Interface Security (AIS)* bagian ini membahas tentang :
    a) Keamanan aplikasi, objek diperlukan untuk mendesain, membangun, dan meluncurkan aplikasi maupun APIs sesuai dengan standar industri.
    b) Kesatuan data yang perlu jaga melalui rekonsiliasi dan pengecekan dua kali untuk menghindari terjadinya *erorr*, *corruption*, dan ancaman keamanan lainnya.
    c) Keamanan data, yang menghubungkan dengan aturan keamanan untuk menghindari isu seperti *disclosure* dan kehancuran data.
2. *Audit Assurance & Compliance* (AAC), bagian ini membahas tentang :
    a) Perencanaan audit, tempat Anda mengembangkan cara untuk meninjau efektivitas rencana dan tindakan keamanan Anda. Suatu rencana perlu dibuat dan disepakati sebelum tinjauan lebih lanjut dapat dilakukan.
    b) Audit independen, proses di mana ulasan dan penilaian selesai. CCM v.3.0.1 merekomendasikan audit untuk dilakukan setidaknya setahun sekali. Persyaratan akses pelanggan, bagian dari rutinitas aplikasi yang perlu ditempatkan sebelum pelanggan dapat memperoleh akses ke data, aset, dan elemen lain dari aplikasi itu sendiri.
    c) Pemetaan regulasi sistem informasi, yang melibatkan proses penyelarasan dan pembuatan kerangka kerja kontrol yang sejalan dengan standar hukum dan industri lainnya untuk diikuti.
3. *Change Controls & Configuration Management* (CCC), bagian ini membahas :

a) Pengembangan atau akuisisi baru, tempat Anda menambahkan kebijakan dan prosedur untuk menangani elemen baru yang ditambahkan ke bisnis.
b) Pengembangan *outsourcing*, yang dimaksudkan untuk membantu mitra bisnis Anda mengikuti standar keamanan dan praktik terbaik yang sama.
c) Pengujian kualitas, *domain* kontrol yang juga dirancang untuk membantu bisnis Anda menguji berbagai solusi, termasuk manajemen layanan ITIL, menggunakan metode pengujian standar dan *baseline.*
d) Perubahan produksi, yang berkaitan dengan hal-hal seperti implementasi bisnis-kritis dan bermigrasi ke infrastruktur atau solusi baru.

4. *Datacenter Security* (DCS), melibatkan proses-proses yang berkaitan dengan :
   a) Identifikasi peralatan, yang melibatkan penggunaan teknologi yang sadar lokasi dan langkah-langkah lain untuk memvalidasi integritas pusat data itu sendiri, semuanya sekaligus mencegah peralatan yang tidak sah untuk dicolokkan.
   b) Peralatan di luar lokasi, yang juga menangani pembuatan kebijakan dan prosedur yang terkait dengan penggunaan peralatan di luar lokasi bisnis.
   c) Otorisasi, di mana akses fisik ke *server* dan peralatan pendukung lainnya dikontrol dan dicatat secara cermat untuk keamanan maksimum.
5. *Human Resources* (HRS), memiliki proses yang berhubungan dengan :
   a) Pemutusan hubungan kerja karyawan, yang menetapkan cara menangani pemutusan hubungan kerja dan tugas-tugas yang terkait dengannya, termasuk dokumentasi dan komunikasi.

b) *Training* dan *awareness*, yang menentukan cara terbaik untuk menjaga tingkat kesadaran keamanan yang tinggi melalui program pelatihan untuk semua peran.

c) Meskipun menggunakan perangkat seluler, kebijakan keamanan harus tetap menjadi prioritas ketika informasi terkait bisnis dan sumber daya *server* diakses.

6. *Identity & Access Management* (IAM), memiliki proses yang berhubungan dengan :

a) Pemisahan tugas, yang selanjutnya membatasi pengguna dan peran untuk mengakses sistem secara keseluruhan.

b) Pembatasan akses kode sumber, tempat Anda mencegah akses dari kode sumber aplikasi dan solusi yang dikembangkan secara *internal*.

c) Akses pihak ketiga, fungsi kritis yang membatasi akses oleh kontraktor pihak ketiga sambil mempertahankan log aktivitas terperinci untuk peninjauan di masa mendatang.

7. *Interoperability & Portability* (IPY) , memiliki proses yang berhubungan dengan:

a) Berurusan dengan penggunaan APIs dan komunikasi antar layanan.

b) Permintaan data dan bagaimana data ini harus di urus sesuai dengan format standar.

c) Kebijakan dan hukum, berisi prosedur dan kebijakan tentang layanan dengan layanan aplikasi begitu juga dengan sistem yang digunakan oleh konsumen.

8. *Threat and Vulnerability Management* (TVM), pada tahapan ini memiliki proses yang berhubungan dengan :

a) Perangkat lunak anti-virus dan anti-*malware*, yang mencakup pengaturan kebijakan dan prosedur yang mencegah eksekusi *malware* dan ancaman keamanan serupa lainnya.

b) Kerentanan dan manajemen *patch*, yang menggabungkan model berbasis risiko untuk mengidentifikasi potensi risiko keamanan dan memprioritaskan pengembangan *patch* dan solusi untuk mereka.

c) Kode seluler, *domain* kontrol yang dirancang untuk mengatasi kebutuhan yang berkembang akan langkah-langkah keamanan ujung-ke-ujung yang lebih baik dan komunikasi antara perangkat yang terhubung.

2.3.1. *Cloud Assessment Initiative Questionnaire* (CAIQ)

CAIQv3.0.1 CONSENSUS ASSESSMENTS INITIATIVE QUESTIONNAIRE v3.0.1

Control Domain	Control ID	Question ID	Control Specification
Application & Interface Security *Application Security*	AIS-01	AIS-01.1	Applications and programming interfaces (APIs) shall be designed, developed, deployed, and tested in accordance with leading industry standards (e.g., OWASP for web applications) and adhere to applicable legal, statutory, or regulatory compliance obligations.
		AIS-01.2	
		AIS-01.3	
		AIS-01.4	
		AIS-01.5	

Gambar 2. 2 Contoh CAIQ

Cloud Security Alliance (CSA) merancang kuesioner penilaian mandiri yang komprehensif untuk memungkinkan penyedia layanan untuk mengevaluasi diri mereka sendiri. Kuesioner penilaian diri ini disebut sebagai *Consensus Assessments Initiative Questionnaire* (CAIQ), yang terdiri dari enam belas *domain* keamanan dan masing-masing berisi sejumlah kontrol keamanan yang bervariasi [5]. *Cloud Assessment Initiative Questionnaire* (CAIQ) adalah kuesioner yang disiapkan untuk *Cloud Service Provider* (CSP) untuk mendokumentasikan langkah-langkah keamanan yang diterapkan. Kuisioner ini didasarkan pada taksonomi kontrol keamanan CSA *Cloud Control Matrix* (CCM) dan ditujukan untuk membantu *Cloud Service Customer* (CSC) memahami cakupan keamanan dari penawaran *cloud* tertentu dalam kaitannya dengan standar keamanan yang populer, kerangka kontrol, dan peraturan [22]. CAIQ berisi pertanyaan yang merupakan daftar periksa perilaku dan sesuai dengan *Cloud Controls Matrix* (CCM) CSA yang menjelaskan kontrol keamanan yang harus diterapkan oleh layanan *cloud* [23]. CAIQ menawarkan cara yang diterima industri untuk mendokumentasikan kontrol keamanan apa yang ada di layanan *cloud*, memberikan transparansi kontrol keamanan dan sampai batas tertentu jaminan [24].

2.4. *Maturity Level*

Maturity level atau *capability level* pada suatu organisasi menyediakan cara untuk mengkarakterisasi kemampuan dan kinerjanya [25]. *Maturity level* adalah dataran evolusioner yang terdefinisi dengan baik untuk mencapai proses akuisisi

perangkat lunak yang matang. Lima tingkat kematangan yang khas adalah *initial, repeatable, defined, quantitative, and optimizing* [26]. Setiap *level* dibangun di atas *level* sebelumnya dengan menambahkan fungsionalitas atau ketelitian baru yang menghasilkan peningkatan kemampuan [27] . 5 tingkat kontinuitas *maturity level*, di mana tingkat paling atas (ke-5) adalah keadaan ideal dengan kombinasi optimisasi proses dan peningkatan berkelanjutan proses akan dikelola secara sistematis [28].

2.5. *Cloud Security*

Cloud Computing menyajikan banyak tantangan untuk organisasi ataupun perusahaan yang akan menggunakannya. Bila organisasi berpindah ke layanan komputasi awan publik tentu infrastruktur sistem komputasi dikendalikan oleh pihak ketiga yaitu *Cloud Service Provider* (CSP) dan tantangan ini harus ditangani melalui inisiatif manajemen. Inisiatif manajemen ini akan memerlukan gambaran jelas peran kepemilikan dan tanggung jawab dari CSP dan organisasi yang berperan sebagai pelanggan. Dalam Presentasi yang dilakukan oleh *Security Issues in Cloud Computing*, Saurabh K Prashar menyatakan bahwa masalah *security* merupakan masalah utama yang timbul dengan adanya teknologi *cloud computing* [29]. Saat ini, perang di dunia maya tidak diragukan lagi merupakan tantangan paling kompleks dalam lingkungan *multi-tenant* dan *distributed cloud*. Ketika data di kirim ke layanan *cloud*, kebutuhan akan keamanan harus dijadikan kepentingan utama [15].

Berdasarkan hasil survei dan penelitian yang dilakukan oleh *Cloud* Security Alliance (CSA) terkait *security issue* yang dinaungi oleh *Cloud Service*

Provider (CSP) memaparkan jenis-jenis isu yang dinamakan *Egregious Eleven* dan disusun secara ranking sesuai dengan hasil survei. Berikut pemaparan dari *Egregious Eleven* [30]:

1. *Data Breaches,* pelanggaran data adalah insiden informasi yang bersifat sensitif, terlindungi, dan rahasia tersebar, dilihat, dicuri, atau digunakan oleh orang yang tidak memiliki ijin. Pelanggaran data ini bisa terjadi dikarenakan bisa jadi menjadi sasaran objektif utama dalam penyerangan atau hasil dari kesalahan manusia dan lemahnya aplikasi yang tidak mengikuti *security best practice. Data breach* memiliki konsekuensi negatif seperti hilangnya hak intelektual oleh kompetitor yang menghalangi pengeluaran produk baru, konsekuensi dengan pihak regulasi yang akan menyebabkan rugi pada perusahaan, dan bisa merusak *image* perusahaan yang memengaruhi nilai di pasar. Untuk mengatasi hal ini bisa dengan menyesuaikan regulasi atau prosedur di perusahaan dengan *domain* yang ada di CCM contohnya: (AIS-01/AIS-04, CCC-05, DSI-01/DSI-05, EKM-01/EKM-04, GRM-02, IAM-01/IAM-04).
2. *Misconfiguration and Inadequate Change Control,* miskonfigurasi terjadi ketika aset komputasi di susun tidak benar, yang menyebabkan komputasi menjadi lemah akan aktivitas berbahaya. Biasanya miskonfigurasi sumber komputasi meyebabkan *data breaches* dan membisakan penghapusan atau modifikasi dari sumber dan gangguan layanan. *Cloud-based resource* sebenarnya sangat kompleks dan dinamis yang membuat hal ini menantang untuk konfigurasi. Perusahaan harus merangkul otomatisasi

dan menggunakan teknologi memindai secara terus menerus untuk sumber daya yang salah konfigurasi dan memperbaiki masalah secara *real time.* Untuk mengatasi hal ini bisa dengan menyesuaikan regulasi atau prosedur di perusahaan dengan *domain* yang ada di CCM contohnya: (AIS-01/AIS-04, CCC-02/ CCC-03/CCC-05, DSI-01/DSI-04, EKM-03/EKM-04, GRM-01/GRM-02, HRS-09, IAM-02/IAM-05, IVS-02/IVS-07).

3. *Lack of Cloud Securtiy Architecture and Strategy*, salah satu tantangan terbesar selama transisi ini adalah penerapan keamanan yang sesuai arsitektur untuk menahan serangan *cyber*. Sayangnya, proses ini masih menjadi misteri bagi banyak organisasi. Selain itu, fungsionalitas dan kecepatan migrasi sering kali diutamakan daripada keamanan. Faktor-faktor ini menyebabkan kurangnya keamanan arsitektur dan strategi di *cloud* yang meninggalkan organisasi rentan terhadap serangan *cyber*. Untuk mengatasi hal ini bisa dengan menyesuaikan regulasi atau prosedur di perusahaan dengan *domain* yang ada di CCM contohnya: (AIS-04, GRM-01/GRM-08, IAM-02, IVS-06/IVS-13, STA-03/STA-05).
4. *Insufficient Identity, Credential, Access, and Key Management*, identitas, kredensial, sistem manajemen akses termasuk alat dan kebijakan yang memungkinkan organisasi untuk mengelola, memantau dan mengamankan akses ke sumber daya berharga. Sistem manajemen identitas harus berskala untuk menangani manajemen siklus hidup bagi jutaan pengguna sebagai serta CSP. Sistem manajemen identitas harus

mendukung pencabutan akses segera untuk sumber daya dengan perubahan personel, seperti pemutusan hubungan kerja atau transisi peran. Identitas seperti itu proses siklus hidup manajemen harus terintegrasi dan otomatis dalam lingkungan *cloud* dan dicapai tepat waktu. Untuk mengatasi hal ini bisa dengan menyesuaikan regulasi atau prosedur di perusahaan dengan *domain* yang ada di CCM contohnya: (EKM-01/EKM-04, HRS-01/HRS-10, IAM-01/IAM-13).

5. *Account Hijacking,* pembajakan akun adalah ancaman yang diperoleh penyerang jahat akses ke dan penyalahgunaan akun yang sangat diistimewakan. Di lingkungan *cloud*, akun dengan yang resiko tertinggi adalah akun layanan *cloud* atau akun pelanggan. Untuk mengatasi hal ini bisa dengan menyesuaikan regulasi atau prosedur di perusahaan dengan *domain* yang ada di CCM contohnya: (BCR-01, IAM-02/IAM-11, IVS-01/IVS-08, SEF-01).
6. *Insider Threat,* orang dalam dapat berupa karyawan atau mantan karyawan, kontraktor, atau mitra bisnis tepercaya lainnya. Tidak seperti pelaku ancaman *eksternal*, orang dalam tidak harus menembus *firewall*, jaringan pribadi *virtual* (VPN), dan pertahanan keamanan perimeter lainnya. Orang dalam beroperasi dalam lingkaran kepercayaan keamanan perusahaan tempat mereka memiliki akses langsung ke jaringan, sistem komputer, dan data sensitif perusahaan. Untuk mencegah hal ini bisa dengan menyesuaikan regulasi atau prosedur di perusahaan dengan

domain yang ada di CCM contohnya: (BCR-01, IAM-02/IAM-11, IVS-01/IVS-08, SEF-01).

7. *Insecure Interfaces and APIs,* desain APIs yang buruk dapat mengarahkan ke penyalahgunaan atau lebih buruknya kebocoran data. Rusak atau API yang diretas telah menyebabkan banyak kebocoran data. Organisasi harus memahami kebutuhan keamanan dalam proses desain dan menyajikan tampilan ini di internet. Untuk mengatasi hal ini bisa dengan menyesuaikan regulasi atau prosedur di perusahaan dengan *domain* yang ada di CCM contohnya: (AIS-0/AIS-04, IAM-01/IAM-13).
8. *Weak Control Plane,* memindahkan pusat data ke *cloud* terdapat beberapa tantangan dalam membuat penyimpanan data dan program pelindung yang memadai. Sebuah *control plane* yang lemah berati seorang yang bertanggung jawab terhadap arsitektur sistem tidak bertanggung jawab penuh dalam infrastruktur, *logic,* keamanan, dan verifikasi data. Keterbatasan ini dapat menghasilkan kerusakan data, ketidaktersediaan data bahkan kebocoran data. Untuk mencegah hal ini bisa dengan menyesuaikan regulasi atau prosedur di perusahaan dengan *domain* yang ada di CCM contohnya: (BCR-01, DSI-04, GRM-01/GRM-11).
9. *Metastructure and Applistructure Failures,* metastruktur dapat disimpulkan sebagai garis batasan untuk CSP/konsumen yang sering disebut sebagai *waterline.* Contoh kelemahan dari model ini, implementasi APIs yang buruk oleh CSP mengundang kesempatan dan serangan bagi penyerang untuk menganggu *cloud* konsumen dengan

mengganggu kerahasiaan, kesatuan, dan ketersediaan layanan. Untuk mencegah hal ini bisa dengan menyesuaikan regulasi atau prosedur di perusahaan dengan *domain* yang ada di CCM contohnya: (AIS-01/AIS-04, AAC-01, BCR-02, IAM-01/IAM-13, CCC-01, IPY-01, IVS-09).

10. *Limited Cloud Usage Visibility*, hal ini terjadi ketika organisasi tidak memiliki ketersediaan untuk menganalisa dan memvisualkan apakah layanan *cloud* yang digunakan organisasi aman atau berbahaya. Untuk mencegah hal ini bisa dengan menyesuaikan regulasi atau prosedur di perusahaan dengan *domain* yang ada di CCM contohnya: (EKM-03, DSI-01/DSI-06, GRM-02, HRS-03/HRS-10).
11. *Abuse and Nefarious Use of Cloud Services,* pelaku kejahatan bisa memengaruhi sumber dari *cloud computing* yang menargetkan pengguna, organisasi, atau penyedia *cloud* lainnya. Penyerang juga bisa menaruh sumber virus pada layanan *cloud* menggunakan *domain* dari CSP. Untuk mencegah hal ini bisa dengan menyesuaikan regulasi atau prosedur di perusahaan dengan *domain* yang ada di CCM contohnya: (AIS-02, BCR-09, CCC-02).

2.6. Teknik Pengumpulan Data

2.6.1. Wawancara

Wawancara adalah salah satu metode dasar dari pengumpulan data yang digunakan dalam ilmu sosial. Wawancara sebuah *form* spesifik dari komunikasi di mana pengetahuan di produksi melalui interaksi antara

orang yang di wawancarai dan pewawancara itu sendiri mereka bisa saling bertukar pandangan yang berfokus pada topik tertentu. Teknik ini mendukung paradigma positif antar kedua sisi dalam proses pengumpulan data meskipun harapan dan asumsi peneliti dapat tergabung selama proses penyusunan [31]. Wawancara memiliki kelebihan dalam mengambil data seperti pelaku wawancara bisa langsung mengklarifikasi dan memahami secara langsung terkait data yang diambil bersamaan dengan teknik observasi, hal ini di tuliskan dalam buku yang ditulis oleh Cathrina Marshall [32].

2.6.2. Observasi

Observasi adalah inti dari penelitian kualitatif. Hal ini menangkap berbagai jenis aktivitas, baik itu ikut dalam aktivitas pengaturan maupun mengetahui orang dan mempelajari rutinitas lingkungan yang dijadikan objek observasi. Observasi memerlukan pencatatan sistematis dan perekaman sebuah acara, perlakuan, interaksi dan objek dalam pengaturan sosial. Observasi dapat dipenuhi tidak hanya dengan indra penglihatan tapi juga dapat dilakukan dengan indra lain. Seorang peneliti dengan keterbatasan penglihatan dapat menarik kemampuan audit lainnya dengan indra perasa, penciuman yang dapat menghasilkan pandangan dan deskripsi baru terkait pengaturan tertentu [32].

2.7. Penelitian Terdahulu

Tabel 2. 1 Tabel Deskripsi Penelitian Terdahulu

1	**Nama**	Jirayu Kanpariyasoontorn Twittie Senivongse
	Tahun	2017
	Jurnal	*International conference on Advance Communication Technology* (ICACT2017)
	Judul	*Cloud Service Trustworthiness Assessment Based on Cloud Controls Matrix*
	Metode	CCM & NIST SP800-53
	Hasil	Metode penilaian ini dapat membantu konsumen pengguna jasa dalam menentukan dan membandingkan kepercayaan untuk hal terkait layanan CSP sebagai salah satu faktor yang perlu diperhatikan dalam proses pemilihan layanan.
2	**Nama**	Erdal Cayirci Alexandr Garaga Anderson Santana de Oliveira Yves Roudier
	Tahun	2016
	Jurnal	*Journal of Cloud Computing: Advances, Systems and Applications*
	Judul	*A Risk Asessment Model for Selecting Cloud Service Providers*
	Metode	Prototyped CARAM
	Hasil	CARAM adalah model penilaian risiko kualitatif dan relatif untuk membantu CSC (*Cloud Service Customer*) memilih CSP yang paling sesuai dengan profil risiko mereka. Ini didasarkan pada kerangka kerja yang ada seperti ENISA, CAIQ dan CNIL dan melengkapinya untuk menyediakan alat praktis bagi CSC.

3	**Nama**	Fariba Ghaffari Hossein Gharaee Mohammad Reza Forouzandehdoust
	Tahun	2016
	Jurnal	2016 *8th International Symposium on Telecommunications* (IST'2016)
	Judul	*Security Considerations and Requirements for Cloud Computing*
	Metode	*Separation of responsibility model* (CSA & ITU)
	Hasil	Model referensi keamanan yang diusulkan (CSA & ITU) mempertimbangkan baik persyaratan keamanan dan kontrol di setiap model layanan dan, untuk semua lapisan *cloud*. Model ini bisa menjadi *practical roadmap* baik untuk penyedia jasa layanan *cloud* maupun konsumen pengguna layanan *cloud*.
4	**Nama**	Vera Wella
	Tahun	2019
	Jurnal	ULTIMA InfoSys, Vol.X, No.1
	Judul	Evaluasi Kualitas Manajemen Mutu pada PT Intikom Berlian Mustika dengan Menggunakan ISO 9001:2015
	Metode	ISO 9001:2015
	Hasil	Tingkat kematangan kualitas manajemen mutu PT.Intikom berada pada *level* 4th yang berarti *managed* dan *measureable*. Intikom bisa mencapai target yang diinginkan dan dapat mengaplikasikan ISO 9001:2015 untuk peningkatan mutu agar bisa naik ke *level* 5

Pada penelitian ini memiliki kesamaan pada 1-3 penelitian terdahulu yang dituliskan pada tabel 2.1 yakni metode yang digunakan ada menggunakan CCM (*Cloud Controls Matrix*) dari CSA, tapi penelitian yang paling mendekati

kemiripannya dengan penelitian ini adalah penelitian yang dilakukan oleh Jirayu Kanpariyasoontorn & Twittie Senivongse dengan dilakukanya proses pengukuran dengan menggunakan matriks dari CSA & *mapping* pertanyaan ke CAIQ (*Consensuss Initiative Questionare*) [23]. Pengukuran matriks yang dilakukan oleh Jirayu diimplementasikan dengan membandingkan dengan *framework* lain sedangkan pada penelitian ini, dilakukan pengukuran langsung kepada CSP disertai dengan adanya penentuan *maturity level* perusahaan. Dapat digaris bawahi bahwa pada penelitian yang dilaksanakan kali ini, peneliti memfokuskan pada implentasi penggunaan *framework* langsung ke perusahaan penyedia layanan *cloud*.

Pada penelitian ke-2 berjudul *Cloud Service Trustworthiness Assessment Based on Cloud Controls Matrix*, hal yang dilaksanakan pada penelitian tersebut adalah membuat *framework* yang diadopsi menggunakan dasar dari CCM & ENISA (*European Network and Information Security Agency*). Pada penelitian ditemukan adanya kelemahan pada penggunaan CAIQ yang hanya berbasis jawaban *yes/no* sehingga ia membuat pembaharuan kerangka untuk pertanyaan [22]. Dengan demikian penelitian yang dilaksanakan kali ini, peneliti mengambil kelemahan yang ada pada CAIQ dan dijadikan bahan penyesuaian bagaimana nantinya mengadakan penelitian menggunakan CAIQ dari CCM ini.

Penelitian ke-3 oleh Fariba Ghaffari, penelitian yang dilakukannya menggunakan *separation of responsibility model* yang menghasilkan perbandingan *responsibility* untuk setiap *domain* pada masing-masing *framework.* Pada penelitian kali ini, peneliti menggunakan penelitian *separation of responsibility model* untuk

menjadi sumber untuk melakukan analisa dan menentukan pilihan *domain* berdasarkan *responsibility model* yang dibuatnya.

Pada penelitian ke-4 terkait manajemen mutu menggunakan ISO 9001:2015, rangkaian evaluasi yang dilakukan menggunakan *framework* ISO 9001:2015 serta diimplementasikan pengukuran ke perusahaan [33]. Pada penelitian tersebut memiliki proses yang hampir sama dengan proses yang diimplementasikan pada penelitian ini hanya saja menggunakan metode atau *framework* yang berbeda. Oleh sebab itu, penelitian tersebut dapat dijadikan sumber referensi untuk pembuatan metode yang digunakan pada penelitian ini.