

BAB I

PENDAHULUAN

1.1 Gambaran Umum Objek Penelitian

PT. XYZ merupakan salah satu *Cloud Service Provider (CSP)* di Indonesia yang didirikan pada tahun 2011 sebagai solusi bisnis terhadap kebutuhan penyimpanan data yang handal, aman dan tepercaya. Dengan menawarkan *operational expense instead of capital expense*, PT. XYZ hadir untuk memenuhi solusi investasi penyimpanan data yang terjangkau dan ekonomis dan sudah tersertifikasi ISO 27001, ISO 9001, dan PCI DSS sebagai upaya memastikan kualitas dan mutu layanan dan manajemen. Perusahaan ini juga merambah pada produk pendukung yang berbasis *Infrastructure as a Service (IaaS)*, *Software as a Service (SaaS)* dan dengan berbagai bidang seperti layanan *e-mail*, *Learning Management System*, *Human Resources Management System* dan *Financial Services*.

Perusahaan saat ini sudah memiliki sistem standar keamanan informasi yang karena sudah melakukan audit keamanan informasi, saat perusahaan tergabung dengan komunitas *cloud* dimana perusahaan disarankan untuk melakukan standarisasi keamanan informasi untuk *Cloud Service Provider (CSP)*. Oleh karena itu, perusahaan perlu melakukan audit untuk mempersiapkan baik dokumen/sistem informasi yang aman untuk *cloud service costumer (CSC)* dengan melakukan audit standar keamanan informasi bagi CSP sebelum melakukan audit oleh pihak terkait pada tahun 2023.

1.2 Latar Belakang

Penggunaan teknologi *cloud computing* merupakan salah satu inovasi paling menarik dan menantang di bidang teknologi informasi, karena penyediaan elastis, fleksibel juga metode penyimpanannya sesuai dengan permintaan dan menyediakan layanan komputasi pada pelanggan [1]. CAGR atau tingkat pertumbuhan per tahun selama 2021 – 2028 dari *market size* serta pendapatan bersama dari permintaan *cloud computing* secara global adalah sebesar 15,80% yang menandakan akan adanya peningkatan penggunaan *cloud computing* [1]. Sedangkan *market size & shared revenue cloud computing* di Indonesia diperkirakan meningkat dengan tingkat pertumbuhan per tahun selama 2021 – 2028 sebesar 28-33% [2].

Gambar 1.1 Market Size Cloud Computing Di Indonesia



Hal tersebut menandakan bahwa adopsi *cloud computing* meningkat tiap tahunnya berdasarkan hasil forecast global dan di Indonesia. Pernyataan ini dikuatkan dengan kehadiran banyaknya *Cloud Service Provider (CSP)* di Indonesia seperti Telkomsigma, Zettagrid Indonesia, CBN Cloud dan masih banyak CSP lainnya.

Ketua *Asosiasi Cloud Computing Indonesia (ACCI)* Alex Budiyanto mengatakan, sebanyak 32 persen responden tidak mengadopsi sistem komputasi awan karena mereka beralasan masih khawatir mengenai akses, kontrol data dan keamanan data [3]. Isu seperti keamanan data, kebocoran informasi, hak akses, privasi dan hal terkait menjadi sorotan dalam keamanan informasi yang menjadi

kekhawatiran pelanggan layanan *cloud/cloud service customer (CSC)*[4].

Kekhawatiran/keraguan dalam penggunaan *cloud* dapat menyebabkan ketidakpercayaan terhadap kedua pihak baik CSC dan CSP yang mengimplementasikan *cloud*[5]. Hal tersebut dapat dihindari dengan meningkatkan kepercayaan CSC oleh CSP dengan mematuhi standar keamanan informasi ISO/IEC 27001: 2013[6]. Untuk memastikan ISO/IEC 27001 dipatuhi oleh CSP, panduan dalam mengimplementasi keamanan informasi disampaikan pada dokumen ISO/IEC 27002:2013. Peningkatan keamanan informasi pada *cloud service provider* dapat dilakukan dengan standar kendali keamanan ISO/IEC 27017:2015 yang merupakan standar keamanan tambahan pada layanan *cloud* yang menjadi referensi tambahan dari ISO/IEC 27001:2013 dan disampaikan dengan format yang sama dengan ISO/IEC 27002:2013.

Sehingga fokus pada penelitian ini adalah membantu perusahaan dalam meningkatkan keamanan informasi terhadap penyedia layanan cloud, dengan harapan dapat menyelesaikan isu keamanan informasi yang ditakutkan oleh pelanggan layanan cloud/calon pelanggan. Hal tersebut dapat dicapai dengan penerapan standar keamanan informasi menggunakan ISO/IEC 27017:2015, karena ini merupakan standar tambahan yang di khususkan untuk penyedia layanan cloud dari standar keamanan sebelumnya yaitu 27002.

Analisis audit keamanan informasi ini dilakukan pada studi kasus CSP PT. XYZ menggunakan ISO/IEC 27017:2015. Karena, perusahaan belum mengadopsi standar kendali keamanan tambahan untuk penyedia layanan *cloud* dan sebagai persiapan perusahaan untuk melakukan audit pada tahun 2023. Dalam analisis ini, peneliti juga menggunakan pengukuran *Capability Maturity Model Integration (CMMI)* serta mengetahui kesenjangan (*gap*) perusahaan dengan ISO/IEC 27017:2015.

1.3 Perumusan Masalah

Berdasarkan latar belakang di atas, berikut merupakan rumusan masalah yang akan di evaluasi oleh penulis.

1. Bagaimana menganalisis keamanan informasi *cloud* yang diterapkan oleh PT.XYZ dan menganalisis *gap* berdasarkan ISO/IEC 27017:2015?
2. Berapakah *maturity level* pada kebijakan keamanan informasi *cloud* yang

diterapkan pada penyedia layanan *cloud* PT.XYZ?

3. Bagaimana rekomendasi yang dapat diberikan dari hasil analisis audit yang sudah dilakukan pada penyedia layanan *cloud* PT. XYZ?

1.4 Tujuan

Mengacu terhadap rumusan masalah, tujuan dari penulisan ini yaitu:

1. Menganalisis keamanan informasi dan *gap* yang ada agar sesuai dengan ISO/IEC 27017:2015 pada penyedia layanan *cloud* PT. XYZ
2. Melakukan pengukuran dan menentukan tingkat *maturity level* dari keamanan informasi *cloud* yang dimiliki oleh PT. XYZ
3. Memberikan rekomendasi dari keamanan informasi *cloud* yang dimiliki oleh PT. XYZ berdasarkan ISO/IEC 27017:2015 sehingga nantinya dapat digunakan untuk persiapan audit pada tahun 2023.

1.5 Batasan Masalah

Adapun batasan masalah dalam penelitian ini yaitu sebagai berikut:

1. Pelaksanaan kegiatan audit pada perusahaan PT.XYZ menggunakan acuan dari dokumen ISO/IEC 27017:2015 dan ISO/IEC 27002:2013 sebagai dokumen pendukung.
2. Tahapan audit dilakukan berdasarkan acuan dokumen dari ISO 27001:2013 dan dilakukan hanya sampai tahap ke 4 analisis audit sehingga tidak sampai tahap implementasi.
3. Audit yang dilakukan tidak mengintervensi layanan dan sistem *cloud* perusahaan. Hasil analisis diambil berdasarkan data primer.
4. Ruang lingkup standar yang digunakan hanya pada *cloud service provider (CSP)* tidak sampai *cloud service customer (CSC)*.

1.6 Sistematika Penulisan

Pada penelitian ini terdapat penjelasan sistematika penulisan tugas akhir yang berlaku sebagai berikut:

1. BAB I PENDAHULUAN

Bab ini menjelaskan gambaran umum objek penelitian, latar belakang penelitian, rumusan masalah, tujuan penelitian, dan sistematika penulisan tugas akhir secara umum.

2. BAB II TINJAUAN PUSTAKA

Bab ini membahas terkait landasan teori, penelitian terdahulu yang digunakan dalam mengembangkan hipotesis dari penelitian.

3. BAB III METODE PENELITIAN

Bab ini membahas terkait metode penelitian yang dilakukan dan alur proses penelitian dari pengumpulan sampai analisis data yang dapat menjawab atau menjelaskan masalah penelitian.

4. BAB IV PEMBAHASAN HASIL PENELITIAN DAN REKOMENDASI

Bab ini membahas hasil dari penelitian dan hasil rekomendasi penelitian sesuai dengan alur proses/metode penelitian.

5. BAB V KESIMPULAN DAN SARAN

Bab ini berisikan kesimpulan dan saran dari penelitian yang sudah dilakukan