BAB I

PENDAHULUAN

Pada bab 1 ini berisi penjelasan mengenai latar belakang penelitian, perumusan masalah, tujuan penelitian, batasan penelitian, manfaat penelitian, dan sistematika penulisan.

1.1 Latar Belakang

Penggunaan TI saat ini telah menyebar hampir ke seluruh aspek kehidupan dan profesi, tidak terkecuali instansi pemerintahan sebagai institusi negara yang memiliki banyak divisi dan staf serta pemerintah membutuhkan suatu sistem informasi agar dapat membantu mempercepat dalam memperoleh kebutuhan informasi. Penggunaan TI akan bermanfaat jika penerapannya sesuai dengan tujuan, visi, dan misi organisasi atau instansi yang telah diterjemahkan ke dalam rencana strategis organisasi tersebut, sehingga tujuan organisasi akan tercapai jika rencana dan strategi TI diimplementasikan selaras dengan rencana dan strategi organisasi yang telah ditetapkan.

Pemanfaatan TI sebagai salah satu faktor pendukung untuk melaksanakan rencana strategis suatu instansi atau organisai untuk dikembangkan secara optimal. Pemanfaatan TI di sebuah lembaga pemerintahan juga tidak lepas dari informasi dan data. TI dan informasi merupakan satu kesatuan yang mungkin tidak bisa dilepaskan.

Seiring kemajuan dan perkembangan zaman saat ini informasi merupakan asset berharga bagi sebuah organisasi, karena informasi adalah salah satu sumber daya straegis dalam meningkatkan nilai usaha dan kepercayaan publik. Oleh sebab itu maka perlindungan terhadap informasi atau keamanan informasi merupakan hal yang sepenuhnya harus diperhatikan secara sungguh-sungguh oleh segenap deretan pemilik, manajemen, dan karyawan organisasi yang bersangkutan. Keamanan informasi yang dimaksud menyangkut kebijakan, prosedur, proses, dan aktivitas untuk melindungi informasi dari berbagai jenis ancaman sehingga dapat menyebabkan terjadinya kerugian-kerugian bagi kelangsungan hidup organisasi atau instansi terkait .

Informasi dan teknologi adalah aset yang sangat berharga dalam instansi atau organisasi, namun hal tersebut sering kali kurang dipahami. Instansi yang sukses dapat mengetahui nilai lebih dari penggunaan suatu teknologi informasi dan meningkatkan nilai instansi itu sendiri. Instansi juga

harus memahami dan mengelola resiko terkait, seperti peningkatan pemenuhan akan peraturan atau regulasi dan ketergantungan proses bisnis terhadap teknologi informasi.

Informasi dikumpulkan, disimpan, diorganisasikan, dan disebarluaskan dalam berbagai bentuk baik dokumen berbasis kertas, hingga berkas elektronik atau digital. Apapun bentuk maupun cara penyimpanannya, harus selalu ada upaya melindungi keaman informasi tersebut sebaik mungkin.

Informasi merupakan aset yang sangat bernilai bagi organisasi. Sebagaimana aset organisasi yang lain, maka informasi harus dilindungi. Keamanan informasi bertujuan untuk menjaga aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*). Sistem Manajemen keamanan informasi diperlukan karena ancaman terhadap aspek keamanan informasi semakin lama semakin meningkat.

Keamanan merupakan yang penting dalam sistem informasi terutama dalam melindungi hal yang bersifat rahasia dan ketersediaan aset informasi yang ada baik dalam menyimpan dan mengelola. *Framework* yang dapat memetakan kejadian yang memungkinkan berhubungan dengan keamanan sistem informasi, yang nantinya akan berhubungan dengan informasi di mana dapat melakukan antisipasi terhadap kejadian tersebut.

Keamanan informasi dimaksudkan untuk mencapai tiga sasaran utama, yaitu kerahasiaan, yang bertujuan melindungi data dan informasi perusahaan dari penyingkapan orang –orang yang tidak berhak. Kemudian ketersediaan guna meyakinkan bahwa data dan informasi perusahaan hanya dapat digunakan oleh orang yang berhak menggunakannya. Dan integritas, dimana sistem informasi perlu menyediakan representasi yang akurat dari sistem fisik yang direpresentasikan.

Keamanan informasi diperoleh dengan mengimplementasi seperangkat alat kontrol yang layak, yang dapat berupa kebijakan-kebijakan, praktekpraktek, prosedur-prosedur, struktur-struktur organisasi dan piranti lunak.

Pada saat ini keamanan informasi menjadi hal penting dalam organisasi yang menggunakan Teknologi Informasi (TI) sebagai aspek dari sebuah system informasi. Semakin besar peningkatan pemanfaatan teknologi informasi dalam berbagai bidang maka risiko ancaman terhadap keamanan informasi juga terus meningkat, melihat dari jumlah tingkat kecanggihan teknologi informasi (TI) dapat menghasilkan indikasi-indikasi ancaman terhadap keamanan informasi terserbut. Berbagai macam kerugian dapat saja terjadi bahkan kerugian finansial dan aset yang merupakan ancaman

besar untuk sebuah organisasi. Fakta ini mendesak pengguna teknologi informasi baik individu dan organisasi atau instansi pemerintah harus siap menghadapi ancaman keamanan informasi. Penyesuaian dalam pengelolaan keamanan informasi perlu dilakukan dari waktu ke waktu seiring berkembangnya teknologi informasi ini. Keamanan Informasi merupakan terjaganya rahasia (*confidentiality*), Keutuhan (*Integrity*), dan Ketersediaan (*Availability*) informasi.

Pada pembukaan Undang-Undang Dasar 1945 merupakan pokok atau kaedah yang fundamental, mempunyai kedudukan yang tepat dan melekat Perusahaan Negara Republik Indonesia. Hal ini karena setiap alinea yang terdapat dalam Pembukaan UUD tercantum tujuan dan prinsip dasar yang hendak dicapai oleh bangsa negara Indonesia. Salah satu tujuan bangsa yang terkandung dalam pembukaan UUD adalah tujuan keamanan nasional, yaitu untuk melindungi segenap bangsa Indonesia, seluruh tumpah darah Indonesia.

Dinas Komunikasi dan Informatika Provinsi Jawa Barat merupakan Dinas yang mempunyai tugas melaksanakan kewenangan daerah di bidang pengolahan TIK. Berdasarkan Peraturan Daerah Nomor 80 Tahun 2016 tentang kependudukan, susunan organisasi, uraian tugas dan fungsi serta tata kelola kerja Kominfo merupakan unsur pelaksana urusan pemerintahan di bidang Komunikasi dan Informatika, bidang Statistik dan bidang Persandian. Tujuan dari Kominfo yaitu meningkatkan pengetahuan, kecerdasan, pemberdayaan dan kesejahteraan masyarakat melalui penyelenggaraan komunikasi dan informatika dalam rangka meningkatkan keterbukaan informasi public.

Tercantum juga dalam pasal 30 UUD 1945 mengenai usaha pertahanan dan keamanan yang dilakukan oleh Negara dijalankan dengan menggunakan sistem pertahanan dan keamanan rakyat secara keseluruhan oleh TNI dan POLRI sebagai kekuatan yang utama, dan rakyat sebagai kekuatan pendukung. Keamanan nasional ini tidak berhenti hanya pada keamanan negara, namun juga keamanan seperti keamanan masyarakat dan keamanan individu atau insani (*human security*). Buzan menyebutkan bahwa keamanan individu mencakup keamanan dalam bidang pangan, kesehatan, lingkungan, pribadi, komunitas dan politik.

Menurut Supradono (2009), keamanan informasi tidak hanya bisa disandarkan pada teknologi keamanan informasi saja, tetapi harus ada pemahaman yang dilakukan oleh organisasi atau perusahaan agar dapat menangani masalah secara tepat dalam memenuhi kebutuhan keamanan informasi. Dengan demikan, dibutuhkan pengelolaan yang komprehensif mengenai keamanan

informasi, keamanan informasi harus memperhatikan tiga aspek, yaitu *Confidentially, Integrity*, dan *Availability* (CIA).

Menurut Hendradhy (2009), masalah keamanan sistem informasi ada 2 yaitu: "*threat*" (ancaman) dan "*vulnerability*" (kelemahan). Ancaman adalah aksi yang terjadi baik dari dalam sistem maupun dari luar sistem yang dapat mengganggu keseimbangan sistem informasi. Ancaman terhadap sistem informasi dapat dibagi menjadi 2 macam yaitu ancaman aktif dan ancaman pasif (Bodnar dan Hopwood, 2006). Yang termasuk dalam ancaman aktif yaitu kecurangan dan kejahatan terhadap komputer, sedangkan yang termasuk dalam ancaman pasif adalah bencana alam, kesalahan manusia, dan kegagalan sistem/lingkungan (Bodnar dan Hopwood, 2006).

Pentingnya informasi yang dimiliki DISKOMINFO JABAR membuat keamanan informasi itu penting untuk dilakukan. *Value* sebuah informasi menyebabkan seringkali informasi hanya boleh diakses oleh orang-orang tertentu. Kondisi saat ini masih terjadi kurrangnya penanganan keamanan informasi sehingga dapat menimbulkan *Threat* (Ancaman) dan *Vulnerable* (kelemahan) yang mengakibatkan target tidak terpenuhi dan mempengaruhi *Confidentiality* (Kerahasiaan), *Integrity* (keutuhan) dan *Availability* (ketersediaan) yang berdampak pada *Business Impact Analysis* (BIA), (Sarno dan Iffano, 2009).

Pengamanan informasi dan data adalah suatu cara khusus untuk mengamankan informasi maupun data yang berada di dalam perangkat fisik yang bisa menunjang keamanan data atau informasi yang dimiliki sebuah organisasi. Dalam hal ini penjagaan keamanan informasi perlu adanya usaha organisasi dalam memperhatikan faktor keamanan dari seluruh hubungan pendukung, jaringan, dan fasilitas lain yang terkait langsung maupun tidak langsung dengan proses pengolahan informasi atau data. Amannya keseluruhan perangkat tempat informasi berada maka kerahasiaan, integritas, dan ketersediaan informasi akan dapat secara efektif berperan dalam meningkatkan kuwalitas dan citra organisasi. DISKOMINFO JABAR tentu didukung dengan perangkat fisik maupun s*oftwar*e atau aplikasi yang menunjang untuk melakukan segala proses bisnis yang ada dalam organisasi, namun sejumlah ancaman kemanan informasi dari berbagai sumber dapat terjadi. Adapun ancaman tersebut dapat berupa intervensi manusia seperti pencurian, perusakan, aktivitas penyadapan dan sabotase terhadap aset informasi DISKOMINFO JABAR, serta ancaman lain yang yang disebabkan bencana alam atau acaman-ancaman dari asset itu sendiri.

Permasalahan tersebut mendorong penulis untuk merancang system informasi pada DISKOMINFO JABAR untuk menunjang keamana data maupun informasi yang berada pada DISKOMINFO JABAR berdasarkan COBIT5.

Dalam melakukan pengolahan teknologi informasi dibutuhkan sebuah model pengelolaan yang dapat dijadikan sebagai acuan sesuai dengan strategi dan tujuan institusi maka dapat digunakan sebagai alat pengukuran di dalam mengatasi permasalahan-masalahan yang terjadi di institusi seperti COBIT atau ITIL. *Control Objectives for Information And Relate Technology* (COBIT) merupakan sebuah kerangka kerja *Framework IT* yang diterbitkan oleh *Information System Audit and Control Association* (ISACA).

Control objectivre for Information and Related Technology (COBIT) adalah seperangkat sumber daya yang berisi semua informasi yang dibutuhkan organisasi untuk tata kelola TI dan kerangka kontrol. COBIT memberikan praktik yang baik di seluruh domain dan kerangka proses dalam struktur kelola logis untuk membantu mengoptimalkan kemampuan TI dalam investasi dan memastikan bahwa TI berhasil dalam memberikan kebutuhan bisnis.

COBIT 5 adalah salah satu kerangka bisnis untuk meningkatkan tata kelola dan manajemen perusahaan. IT versi *evolusiner* telah menggabungkan pemikiran terbaru dalam tata kelola perusahaan dan teknik manajemen,serta menyediakan prinsip-prinsip, praktek, alat-alat analisis dan model yang diterima secara global dalam membantu meningkatkan kepercayaan dan nilai dari sistem informasi.

Penggunaan COBIT 5 dalam mengukur tingkat tata kelola TI di instansi pemerintah dimaksudkan sebagai pedoman untuk peningkatan kinerja selanjutnya. *Framework* COBIT memiliki rentang lingkup yang luas dan memiliki fungsi pada tingkat yang lebih manajerial (*What*) bukan kepada teknis penggunaan (*How*). COBIT memiliki kompromi antara dimensi horisontal dan vertikal yang lebih baik dari standar-standar lainnya. COBIT mempunyai spektrum proses TI yang lebih luas dan lebih mendetail. Model perancangan COBIT lebih bersifat praktis, lebih lengkap, dan cocok untuk monitoring proses TI untuk membantu tercapainya pelaksanaan tata kelola TI yang baik.

1.2 Perumusan Masalah

Penelitian ini ditujukan untuk memecakan beberapa perumusan masalah sebagai berikut :

1. Bagaimana kondisi sistem keamanan informasi pada DISKOMINFO JABAR pada saat ini ?
2. Bagaimana rancangan sistem keamanan informasi pada DISKOMINFO JABAR berdasarkan COBIT5 ?

1.3 Tujuan Penelitiam

Tujuan dari penilitian ini adalah sebagai berikut :

1. Memahami system keamanan informasi pada DISKOMINFO JABAR saat ini sebagai acuan untuk menindaklanjuti usulan perancangan system keamanan informasi .
2. Memberikan usulan atau rekomendasi system keamanan informasi pada DISKOMINFO JABAR berdasarkan COBIT5.

1.4 Ruang Lingkup

Terdapat batasan-batasan yang menjadi lingkup penelitian dalam melakukan penelitian mengenai perancangan manajemen keamanan informasi, seperti:

1. Penelitian ini hanya membahas manajemen keamanan informasi DISKOMINFO JABAR
2. Penelitian ini hanya berada pada ruang lingkup analisis domain proses (EDM03 & APO120)
3. Penelitian ini hanya berada pada ruang lingkup aplikasi Service Desk
4. Penelitian menggunakan COBIT5 sebagai metode analisis risiko
5. Penelitian menggunakan ISO 27001 untuk pemilihan kontrol keamanan informasi

1.5 Manfaat Penelitian

Manfaat pada penelitian ini adalah sebagai berikut:

1. Hasil dari penelitian ini diharapkan dapat menjadi referensi dan masukan bagi perkembangan ilmu manajemen keamanan informasi dengan menggunakan standar COBIT5 di lingkungan pemerintahan.
2. Menghasilkan nilai yang bermanfaaat dan meningkatkan manajemen keamanan informasi terhadap kinerja yang ada pada DISKOMINFO JABAR dalam mencapai tujuannya.
3. Meningkatkan kesadaran akan pentingnya manajemen keamanan informasi yang baik bagi DISKOMINFO JABAR.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Pada bab ini berisi uraian mengenai latar belakang penelitian, perumusan masalah, tujuan penelitian, batasan penelitian, manfaat penelitian, dan sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini berisi penelitian terkait yang telah ada sebelumnya, dari penelitian terkait tersebut diambil hanya teori yang akan digunakan dalam penelitian ini. Pada bagian kedua berisi teori dari literatur yang relevan dengan permasalahan yang diteliti.

BAB III METODOLOGI PENELITIAN

Pada bab ini dijelaskan langkah-langkah penelitian secara rinci yaitu model konseptual dan sistematika pemecahan masalah.

BAB IV PENGUMPULAN, PENGOLAHAN, DAN ANALISIS DATA

Pada bab ini dijelaskan mengenai tahapan pengumpulan data yang kemudian diolah dan dianalisis menjadi informasi yang berguna pada penelitian ini pada bab berikutnya.

BAB V PERANCANGAN DAN HASIL ANALISIS

Pada bab ini dilakukan perancangan solusi berdasarkan analisis yang dilakukan pada bab sebelumnya.

BAB VI PENUTUP

Bab ini berisi kesimpulan dan saran. Kesimpulan merupakan gambaran umum dan solusi yang diberikan atas permasalahan yang diangkat pada penelitian ini. Sedangkan saran merupakan saran yang dapat digunakan untuk penelitian terkait yang akan dilakukan selanjutnya.