BAB I
PENDAHULUAN

1.1 Latar Belakang

Teknologi Informasi dan Komunikasi (TIK) terus mengalami peningkatan dan perkembangan hingga memiliki peran yang penting untuk sebuah organisasi dalam mencapai visi dan misinya [1]. Semakin pesatnya perkembangan TIK, menyebabkan penggunanya semakin bertambah dan meluas hingga ke penjuru dunia dalam waktu yang relatif cepat. Internet sekarang sudah seakan-akan menjadi kebutuhan utama manusia dalam menunjang aktivitasnya sehari-hari terutama pada proses pertukaran informasi. Pertukaran informasi sekarang dapat dilakukan dengan sangat cepat, tidak terbatas oleh jarak dan dapat diakses tanpa batasan waktu.

Teknologi yang mengalami perubahan secara terus menerus memaksa suatu organisasi untuk bisa menyesuaikan diri dengan perubahan yang ada. Teknologi informasi sekarang sudah dimanfaatkan ke berbagai sektor kehidupan, termasuk juga di dalam sektor penyelenggaraan pemerintahan maupun swasta. Institusi pemerintah atau swasta ketika melakukan penerimaan data, mengolah data dan melakukan distribusi data tentu memerlukan pengamanan untuk menjaga data tersebut agar tetap aman sekaligus untuk keamanan pengguna data tersebut. Di lingkungan pemerintahan saat ini penggunaan TIK sudah semakin tumbuh dan berkembang sejalan dengan kebutuhan instansi untuk memberikan pelayanan publik dengan cepat, andal dan aman. Kepentingan TIK meningkat menjadi usaha untuk meningkatkan nilai pelayanan untuk mewujudkan pengelolaan pemerintah dengan bagus atau bisa disebut dengan *good governance* [2].

Dengan segala kemudahan yang timbul dari perkembangan teknologi dan internet tentu tidak semata-mata menghasilkan hal yang sepenuhnya baik. Tidak menutup kemungkinan bahwa semua hal tersebut juga membawa dampak yang

buruk. Dampak buruk yang dapat terjadi adalah meningkatnya kejahatan siber atau *cyber crime*. Tentu dampak buruk ini menjadi sebuah permasalahan di dalam bidang keamanan informasi.

Keamanan informasi merupakan metode untuk mengamankan data dan informasi dari segala bentuk aktivitas yang dapat mengancam seperti mengakses, merusak dan memanipulasi dari oknum yang tidak berwenang [3]. Menurut penelitian yang dilakukan oleh Arman, dkk. pada tahun 2019 yang menggunakan Indeks KAMI menyatakan keamanan informasi adalah usaha yang dilakukan untuk melindungi aset terkait informasi dari bentuk kerusakan yang dapat dilakukan dan mereduksi kerugian yang mungkin akan terjadi [4]. Informasi sebanding dengan timbulnya risiko. Semakin banyak informasi, makin besar juga risiko yang bisa muncul baik dalam bentuk rusaknya informasi, hilangnya informasi, bocornya informasi dan lainnya. Data ataupun informasi yang dihasilkan oleh instansi adalah aset yang sangat berharga. Hal tersebut merupakan hal yang bernilai karena dalam proses penghasilannya melibatkan banyak sumber daya [4].

Penggunaan teknologi tentu juga perlu dipelihara, diperbaiki serta manajemen keamanan informasi guna melindungi aset instansi dari segala bentuk ancaman. Dengan menjaga aset-aset tersebut tentu diperlukan juga perhatian lebih terhadap faktor-faktor yang mempengaruhi keamanan informasi dari semua perangkat pendukung dan hal-hal yang berpengaruh langsung ataupun tidak langsung pada pengolahan suatu informasi [5].

Keamanan adalah bagian yang penting menjadi perhatian dalam proses pelaksanaan tata kelola teknologi informasi guna meningkatkan performa tata kelola tersebut. Jika aspek tersebut mengalami gangguan, maka dapat timbul celah yang berpotensi mengancam keamanan data yang meliputi kerahasiaan, keutuhan dan ketersediaannya [6]. Kerahasiaan atau *confidentiality* merupakan jaminan kerahasiaan terhadap data pada suatu instansi yang tidak boleh diketahui oleh sembarang pihak. Keutuhan atau *integrity* merupakan keutuhan dari data itu sendiri. Data yang dimiliki oleh instansi harus diamankan dengan sedemikian rupa agar isinya tetap utuh dan tidak ada manipulasi atau rekayasa. Ketersediaan atau

availability terkait dengan ketersediaan data saat diakses atau dibutuhkan oleh pihak yang memang memiliki wewenang untuk mengaksesnya [7]. Tanpa adanya penerapan keamanan informasi dapat menyebabkan individu, organisasi, perusahaan swasta maupun instansi pemerintahan menjadi rentan terhadap ancaman-ancaman atau bentuk-bentuk penyerangan terhadap aset yang dimiliki [2].

Pengimplementasian keamanan informasi bisa mendukung usaha peningkatan kualitas layanan dari pemerintah serta menilai seberapa baik tata kelola keamanan informasi yang sudah diterapkan oleh pemerintah. Pada Sistem Pemerintahan Berbasis Elektronik (SPBE) dalam Peraturan Presiden Republik Indonesia No. 95 Tahun 2018 memuat bahwa pemerintah harus berpegang pada pasal 2 ayat 8 tentang keamanan yang rahasia, tersedia, dan data pendukung yang asli [3].

Keamanan informasi dan pelaksanaan sistem elektronik wajib menerapkan standar SNI ISO/IEC 27001 berdasarkan Peraturan Menteri Komunikasi dan Informatika No. 4 Tahun 2016 memuat bahwa pengamanan informasi dilaksanakan untuk kepentingan dan pelayanan publik [4]. Selain itu, untuk sistem elektronik yang berlangsung harus memiliki sertifikat pengamanan informasi setidaknya dalam dua tahun [3].

Pemerintah juga sudah berupaya dengan mengeluarkan peraturan mengenai manajemen risiko adalah alat yang berkepentingan dalam melindungi keamanan informasi dalam instansi, sama halnya dalam Perpres No. 95 Tahun 2018 memuat bahwa keseluruhan Sistem Pemerintahan Berbasis Elektronik (SPBE) perlu meminimalkan ancaman agar pelayanan publik tetap maksimal [8].

Beberapa penelitian yang berkaitan dengan penelitian ini sudah pernah dilakukan sebelumnya. Ada penelitian dengan menggunakan Indeks KAMI sebagai alat bantu untuk melakukan pengevaluasian atau penilaian keamanan informasi di suatu instansi. Seperti yang termuat pada penelitian Afrianto, dkk. pada tahun 2015 yang mencoba untuk menerapkan penggunaan Indeks KAMI untuk mengukur dan mengevaluasi SIAKAD UYP [9].

Penelitian lainnya yang menggunakan Indeks KAMI sebagai alat bantu dalam melakukan pengevaluasian adalah penelitian pada Diskominfo Kota Batu yang dilakukan oleh Oktaviani, dkk. pada tahun 2019 [10]. Dalam penelitian tersebut, peneliti mencoba melakukan pengevaluasian terhadap tingkat kesiapan penerapan keamanan informasi di Diskominfo Kota Batu dengan bantuan Indeks KAMI.

Dari beberapa penelitian yang sudah dilakukan sebelumnya, Sebagian besar melakukan pengevaluasian atau penilaian secara keseluruhan menggunakan semua bagian yang ada di dalam Indeks KAMI dan memberikan rekomendasi solusi di tiap bagian tersebut namun tidak secara spesifik pada bagian tertentu. Beberapa penelitian di atas juga belum ada yang berfokus pada bidang risiko dalam Indeks KAMI.

Seperti halnya dengan instansi pemerintahan lainnya, Diskominfo Provinsi XYZ menerapkan keamanan informasi sesuai dengan peraturan pemerintah dan juga menganggap data adalah hal yang bernilai yang wajib dilindungi keamanannya meliputi unsur CIA yaitu *Confidentiality*, *Integrity* dan *Availability*. Diskominfo Provinsi XYZ sebagai instansi yang memanfaatkan teknologi informasi, keamanan informasi sangat penting terutama dalam penggunaan TIK sebagai pendukung berjalannya proses bisnis yang dilakukan. Hal itu dilakukan bertujuan untuk meningkatkan kualitas layanan kepada setiap pemangku kepentingan.

Diskominfo Provinsi XYZ merupakan instansi pemerintahan yang memanfaatkan teknologi informasi dalam melaksanakan proses bisnisnya. Proses bisnis tersebut merupakan aset utama bagi Diskominfo Provinsi XYZ termasuk juga dengan sub-proses dan kegiatan-kegiatan di dalamnya. Berlangsungnya proses bisnis instansi dengan baik merupakan modal untuk Diskominfo Provinsi XYZ untuk memberikan layanan yang baik untuk masyarakat. Dari hal tersebut sudah seharusnya Diskominfo Provinsi XYZ menerapkan pengamanan informasi yang baik karena proses-proses bisnis yang berlangsung tentu berhubungan dengan banyak pihak baik internal maupun eksternal. Dalam situasi tersebut,

sangat memerlukan manajemen keamanan informasi terutama di bagian risiko untuk mengamankan aset utama instansi.

Diskominfo Provinsi XYZ sudah secara rutin melakukan pengevaluasian baik secara mandiri maupun melibatkan pihak ketiga contohnya Badan Siber dan Sandi Negara (BSSN). Pengevaluasian rutin dilakukan setahun sekali. Akan tetapi dari hasil pengevaluasian di tahun terakhir yaitu tahun 2019, penerapan keamanan informasi di Diskominfo Provinsi XYZ masih belum maksimal. Masih ada beberapa bagian yang nilainya masih rendah walaupun secara keseluruhan hasil penilaiannya sudah cukup baik. Tapi cukup bukan berarti harus berhenti melakukan perbaikan. Perbaikan harus tetap dilakukan hingga mencapai optimal.

Namun ada bagian yang masih memiliki nilai rendah yaitu pada bagian risiko. Bagian ini memiliki nilai rendah yang jaraknya agak signifikan jika dibandingkan dengan nilai pada bidang-bidang lainnya. Tentu saja hal tersebut merupakan suatu celah kelemahan yang harus segera diatasi oleh pihak Diskominfo Provinsi XYZ. Jika dibiarkan akan berakibat buruk bagi instansi di kemudian hari.

Hal tersebut juga sejalan dengan hasil wawancara terhadap narasumber dari Bidang Persandian dan Keamanan Informasi (PDKI) yang menyatakan pihak instansi memang belum menerapkan manajemen risiko keamanan informasi. Di samping itu, saat ini masih sering terjadi beberapa insiden terkait dengan keamanan informasi. Insiden tersebut dapat berupa insiden internal dan insiden eksternal yang dapat mengancam aset utama dari instansi. Insiden internal yang sering terjadi adalah kelalaian dari personel instansi itu sendiri seperti kelalaian dalam pengelolaan dokumentasi dan lainnya. Sedangkan insiden eksternal yang sering terjadi adalah serangan *ransomware* yang mendapatkan *trigger* dari internal instansi yang dapat menyebabkan kerusakan pada dokumentasi instansi, belum terpasangnya antivirus di beberapa perangkat komputer, program antivirus yang belum *update* dan masih banyak lagi.

Berdasarkan uraian-uraian insiden yang masih sering terjadi di atas, apabila instansi kurang memiliki kesadaran terhadap risiko yang ada maka kelalaian tersebut dapat berdampak serius bagi instansi. Contoh dari dampak yang

dapat muncul seperti terganggunya kinerja pelayanan pemerintah, menurunnya reputasi pemerintah, hilangnya kepercayaan masyarakat terhadap layanan pemerintah dan sebagainya. Maka, dibutuhkan pengelolaan terhadap risiko secara efektif guna mencegah atau mengurangi terjadinya dampak insiden yang lebih merugikan lagi [11]. Diskominfo Provinsi XYZ perlu melakukan pengelolaan terhadap risiko keamanan informasi agar dapat mengidentifikasi ancaman yang ada, memetakan kerentanan ancaman tersebut dan mengidentifikasi aset TIK yang dimiliki instansi dengan baik.

Ada berbagai alat bantu atau kerangka kerja yang dapat digunakan untuk melakukan pengelolaan risiko salah satunya adalah ISO/IEC 27005. Bagi penyelenggara publik, sangat dianjurkan dalam pengamanan informasi menggunakan seri ISO 27000 sesuai dengan Panduan Penerapan Tata Kelola Keamanan Informasi [12]. Sama dengan ISO/IEC 27005 untuk manajemen risiko keamanan informasi yang menjadi standar pada instansi pemerintah. Walaupun sudah ditetapkan tapi Diskominfo Provinsi XYZ masih belum melalukan pengelolaan terhadap risiko. Akibatnya masih sering terjadinya insiden-insiden yang mengancam keutuhan aset utama instansi.

Oleh sebab itu, evaluasi terhadap penerapan keamanan informasi sangat diperlukan untuk terciptanya strategi yang matang ke depannya. Pengevaluasian mencangkup proses pengumpulan bukti-bukti yang mendukung penerapan keamanan informasi pada instansi tersebut. Bukti tersebut tentu akan merepresentasikan bahwa keamanan yang sudah diterapkan dapat melindungi aset yang dimiliki oleh instansi. Dengan adanya alat bantu evaluasi kelengkapan dan kematangan ini, sangat membantu instansi untuk memahami bagaimana mengetahui keadaan dan posisinya saat ini serta menentukan posisi atau target yang ingin dicapai ke depannya [13].

Dari hasil pengevaluasian penerapan keamanan informasi Diskominfo Provinsi XYZ pada tahun terakhir, pihak instansi harus segera menyusun tindakan untuk meningkatkan nilai dari bagian risiko pada Indeks KAMI agar nilai penerapan keamanan informasi dapat ditingkatkan secara optimal di seluruh bagian. Selain untuk mengamankan aset-aset instansi, Tindakan tersebut juga

bertujuan untuk membantu tercapainya visi dan misi instansi dengan efektif dengan menggunakan sumber daya seefisien mungkin.

1.2 Rumusan Masalah

Masalah utama pada Diskominfo Provinsi XYZ saat ini adalah rendahnya nilai bidang risiko berdasarkan penilaian menggunakan Indeks KAMI yang dilakukan pada tahun terakhir yaitu 2019. Rendahnya penilaian tersebut menggambarkan bahwa belum maksimalnya penerapan pengelolaan risiko keamanan informasi di Diskominfo Provinsi XYZ terutama untuk melindungi aset utama instansi. Aset perangkat utama instansi perlu segera dilakukan perlindungan melihat masih sering terjadinya ancaman yang menyerang aset tersebut. Terlebih lagi pihak instansi belum menerapkan manajemen risiko keamanan informasi.

Pengelolaan risiko sangat penting dilakukan di lingkungan pemerintahan untuk menunjang penerapan keamanan informasi serta mendukung anjuran pemerintahan pusat untuk menyelenggarakan *e-government*. Rendahnya penilaian pada bagian risiko dapat mengakibatkan Diskominfo Provinsi XYZ tidak siap untuk mengatasi risiko-risiko yang akan muncul secara tidak terduga. Jika tidak segera diatasi, dapat mengancam kelangsungan proses bisnis instansi bahkan aset yang dimilikinya. Hal tersebut tentu juga akan merembet ke penurunan reputasi Diskominfo Provinsi XYZ baik di lingkungan pemerintahan pusat, pemerintahan provinsi, pemerintahan daerah maupun di lingkungan masyarakat.

Oleh karena itu, Diskominfo Provinsi XYZ perlu melakukan suatu tindakan untuk meningkatkan penerapan keamanan informasi melalui peningkatan di bidang risiko guna melindungi aset utama instansi. Dengan penerapan keamanan informasi yang optimal maka Diskominfo Provinsi XYZ akan lebih merasa aman dalam melaksanakan proses bisnisnya maupun dalam menyelenggarakan *e-government* sesuai dengan anjuran pemerintahan pusat.

1.3 Pertanyaan Penelitian

Pada bagian ini akan memaparkan pertanyaan-pertanyaan yang akan dicari jawabannya melalui penelitian ini. Berikut ini adalah beberapa pertanyaan yang diajukan pada penelitian ini.

1. Bagaimana tingkat kesiapan pengamanan informasi di Diskominfo Provinsi XYZ berdasarkan Indeks KAMI?
2. Bagaimana cara meningkatkan kesiapan pengamanan informasi di bidang risiko berdasarkan ISO 27005 : 2011 khususnya untuk melindungi aset utama Diskominfo Provinsi XYZ?

1.4 Batasan Masalah

Penelitian ini berisikan batasan-batasan masalah yang sudah ditentukan dengan sedemikian rupa oleh peneliti. Berikut merupakan batasan-batasan masalah pada pelaksanaan penelitian ini.

1. Pengevaluasian pada kesiapan penerapan keamanan informasi menggunakan Indeks Keamanan Informasi (KAMI) versi 4.0 sebagai alat bantu
2. Pemberian rekomendasi pada manajemen keamanan informasi berdasarkan ISO 27005 : 2011 yang berfokus pada aset utama instansi

1.5 Tujuan Penelitian

Peneliti ini mempunyai tujuan-tujuan yang ingin diraih. Di bawah ini adalah penjabaran dari tujuan tersebut.

1. Untuk mengetahui tingkat kesiapan pengamanan informasi melalui pengevaluasian pada manajemen keamanan informasi di Diskominfo Provinsi XYZ
2. Untuk membuat strategi perbaikan pada manajemen keamanan informasi Diskominfo Provinsi XYZ khususnya dalam melindungi aset utama instansi

1.6 Manfaat Penelitian

Penelitian ini tentu bermanfaat. Ada dua kategori manfaat pada penelitian ini. Pertama manfaat keilmuan merupakan hal yang berkaitan dengan bidang akademis atau teori. Kedua manfaat praktis berarti berkaitan dengan praktik yang sesungguhnya di lapangan. Berikut ini merupakan penjabaran dari manfaat-manfaat tersebut.

A. Manfaat Keilmuan

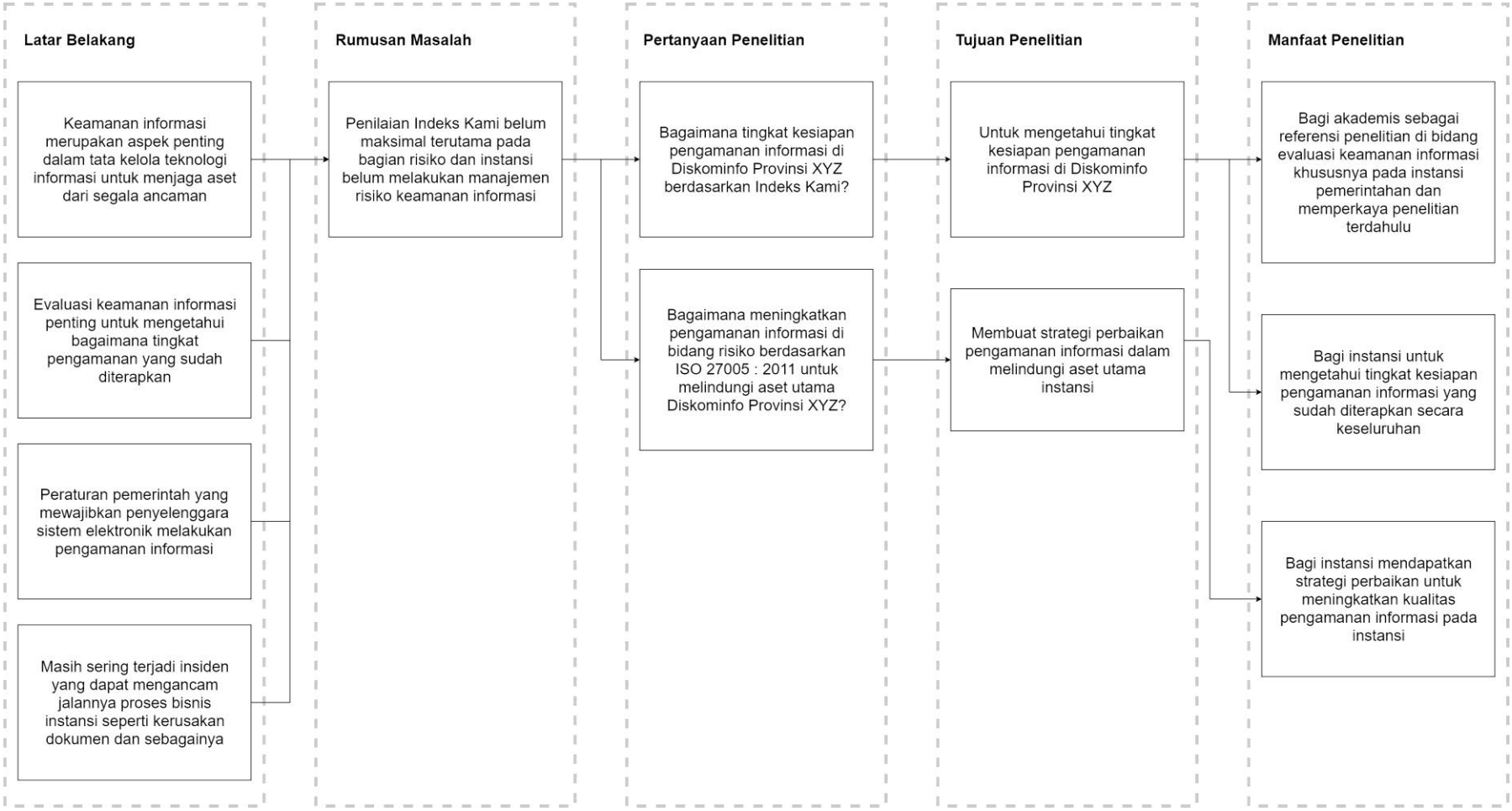
1. Di bidang akademis atau ilmiah, menjadi referensi penelitian terutama di bidang pemerintahan terkait penilaian manajemen keamanan informasi dan juga untuk memperkaya penelitian terkait yang sudah ada sebelumnya.

B. Manfaat Praktis

1. Bagi instansi, bermanfaat untuk mengetahui tingkat kesiapan pengamanan informasi yang sudah diterapkan secara keseluruhan
2. Bagi instansi, mendapatkan strategi perbaikan yang disarankan oleh peneliti untuk meningkatkan kualitas manajemen keamanan informasi pada instansi

1.7 Bagan Keterkaitan

Hubungan dari latar belakang, rumusan masalah, pertanyaan penelitian, tujuan penelitian serta manfaat penelitian akan dijelaskan pada bagian ini. Bagan keterkaitan ini akan membantu pembaca dalam memahami keterkaitan antara bagian satu dengan lainnya pada penelitian ini. Keterkaitan tersebut akan digambarkan dengan jelas melalui Gambar 1.1 di bawah ini.



Gambar 1. 1 Bagan Keterkaitan