BAB I
PENDAHULUAN

1.1 Latar Belakang

Meningkatnya perkembangan teknologi informasi selalu beriringan dengan meningkatnya risiko pada pemanfaatan teknologi informasi itu sendiri, sehingga perlu dibangun sistem keamanan untuk melindungi informasi yang ada. Sistem keamanan yang sebelumnya telah dirancang dengan baik, mungkin saat ini sudah tidak seperti beberapa tahun lalu. Sistem informasi beserta informasi di dalamnya adalah aset paling besar dan penting yang patut dilindungi, diawasi dan dikontrol. Oleh karena itu, sangat berguna apabila sistem beserta sistem pengontrolannya setiap beberapa tahun dievaluasi dan diperbaiki ataupun ditingkatkan. Sudah banyak terbukti bahwa prosedur dan sistem pengontrolan sangat jarang dievaluasi terutama pada sistem dengan skala yang kecil.

Laporan *Security Intelligence Report* (SIR: 2017) Volume 22 yang dirilis Microsoft Asia Pasifik, Indonesia masuk dalam daftar lima besar negara di Asia Pasifik yang paling terekspos oleh program berbahaya atau *malware*, urutannya yaitu: Bangladesh, Kamboja, Indonesia, Myanmar dan Vietnam [1]. Laporan ini menyebutkan bahwa sekitar satu dari empat komputer yang menjalankan produk keamanan *real-time* Microsoft di negara-negara tersebut melaporkan adanya serangan malware antara Januari sampai Maret 2017 Laporan investigasi lain disebutkan, sekitar 3,7 *Gigabyte* data dan lebih dari 500 identitas digital dicuri [2].

Audit didefinisikan sebagai proses atau aktivitas yang sistematik, independen dan terdokumentasi untuk menemukan suatu bukti-bukti (audit *evidence*) dan dievaluasi secara obyektif untuk menentukan apakah telah memenuhi kriteria pemeriksaan (audit) yang ditetapkan (ICASA dalam Sarno) [3]. Sedang dalam sebuah jaringan, Audit dilakukan untuk memastikan terjaminnya "*confidentiality*", "*integrity*", dan "*availability*" sebuah sistem komputer. Untuk menjamin supaya tiga hal tersebut dapat tercapai maka diperlukan beberapa proses yang dilakukan secara bersama-sama. Salah satu proses tersebut adalah dengan melakukan audit terhadap sistem komputer dan jaringan komputer di dalamnya [4].

SMK PI Ambarukmo 1 Yogyakarta adalah sekolah menengah kejuruan yang bergerak dibidang pariwisata. Seperti kebanyakan instansi pada umumnya, SMK PI Ambarukmo telah banyak memanfaatkan perkembangan teknologi informasi (TI) untuk mempermudah proses pengolahan informasi siswa dan lain sebagainya. Namun dalam pemanfaatannya, tidak terdapat prosedur yang jelas untuk mengelola aset informasi dan fasilitas pengolahan informasi sehingga sering terjadi kendala atau kesalahan yang menghambat aktivitas-aktivitas di dalamnya seperti: kehilangan data (*file*) akibat penggunaan komputer oleh lebih dari satu orang atau digunakan oleh pegawai lain tanpa izin dan pengawasan dari pihak yang berwenang atas akses ke komputer tersebut, kemudian pada sistem jaringan komputer yang juga belum dikelola dengan baik sehingga sering terjadi insiden jaringan seperti lonjakan pengguna layanan jaringan yang diakibatkan buruknya pengalokasian otentikasi rahasia, penggunaan *bandwidth* yang tidak wajar dan lain-lain. Lemahnya keamanan sistem keamanan jaringan dan tidak terdapat prosedur

yang jelas untuk mengatur, alokasi otentikasi rahasia, batasan akses ke jaringan, daerah aman yang berhubungan dengan informasi dan aset-aset penting membuat penelitian ini perlu untuk dilakukan.

Terdapat berbagai macam framework yang dapat digunakan untuk melakukan audit di antaranya adalah COBIT, ITIL dan ISO [5].

1. COBIT adalah singkatan dari *Control Objective Over Information and Related Technology*. Cobit yang dikeluarkan oleh ISACA (*Information System Control Standard*) yang merupakan organisasi non-profit untuk IT *Governance*. Fungsi utama Cobit adalah membantu perusahaan dalam memetakan proses TI mereka ke standar praktik terbaik dari ISACA. Cobit biasanya dipilih oleh perusahaan yang melakukan audit sistem informasi, baik yang berkaitan dengan audit keuangan atau audit TI secara umum.
2. ITIL (*Information Technology Infrastructure Library*). ITIL yang dikeluarkan oleh OGC (*Office of Government Commerce*) , adalah seperangkat *framework* untuk mengelola IT Service Level. Meskipun dalam banyak hal ITIL sangat mirip dengan COBIT, namun perbedaan mendasarnya adalah Cobit menetapkan standar dengan melihat berdasarkan proses dan risiko, dan di sisi lain, ITIL menetapkan standar dari layanan TI dasar.
3. ISO-27001 jauh berbeda antara COBIT dan ITIL, karena ISO-27001 adalah sebuah "*security standard*", sehingga memiliki domain yang lebih kecil namun lebih mendalam dibandingkan dengan COBIT dan ITIL.

Proses audit pada SMK PI Ambarrukmo akan digunakan standar ISO/IEC 27001:2013. ISO/IEC 27001 adalah standar sistem manajemen keamanan informasi yang fokus pada pengalamatan dan audit membuat metodologi menjadi kerangka kerja kontrol dan manajemen daripada kerangka proses. Meskipun berbagi struktur ini dengan COBIT, ISO 27001 memiliki target yang lebih spesifik "keamanan" dan dengan demikian melayani manajemen tingkat yang lebih rendah. Metodologi COBIT menargetkan kebutuhan tingkat teratas dari suatu perusahaan, yang berusaha meningkatkan orientasi bisnis secara keseluruhan melalui kontrol dan metrik TI [15]. Dibandingkan dengan COBIT, ISO 27001 lebih cocok untuk diimplementasikan pada SMK PI Ambarukmo dengan kasus yang sudah dijelaskan pada paragraf 4 di atas meskipun COBIT, ISO dan ITIL saling melengkapi. Standar ini berisi spesifikasi dan persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI). Beberapa hal yang menjadi bahan pertimbangan lain dalam penggunaan standar ini adalah standar ini fleksibel karena dikembangkan tergantung dari kebutuhan dan tujuan organisasi.

Berdasarkan latar belakang tersebut, penulis membuat penelitian yang berjudul "Audit Manajemen Tata Kelola Teknologi Informasi Pada SMK PI Ambarrukmo Untuk Meningkatkan Keamanan Jaringan Komputer".

1.2 Rumusan Masalah

Keamanan sebuah sistem jaringan komputer sangat dipengaruhi oleh tingkat kematangan manajemen tata kelola TI yang diterapkan karena sistem jaringan yang diterapkan berkaitan dengan bagaimana manajemen kontrol, manajemen aset,

kendali akses, keamanan fisik dan lingkungan yang mana ini merupakan bagian dari tata kelola TI suatu organisasi atau instansi. Maka dari itu penulis membuat rumusan masalah yaitu apakah tingkat kematangan tata kelola teknologi informasi dan jaringan pada SMK PI Ambarrukmo sudah sesuai dengan standar ISO/IEC 27001:2013.

1.3 Batasan Masalah

a. Audit dan pengambilan data dilakukan di SMK PI Ambarrukmo.
b. Audit ini mengacu pada standar SNI ISO/IEC 27001: 2013.
c. Ruang lingkup audit berfokus pada 5 klausul ISO/IEC 27001: 2013 yaitu: Kebijakan Keamanan Informasi, Manajemen Aset, Kendali Akses, Keamanan Fisik dan Lingkungan dan Keamanan Komunikasi.
d. Penentuan rung lingkup dilakukan dengan menyesuaikan kondisi objek dengan klausul-klausul pada standar ISO/IEC 27001:2013.
e. Metode penilaian menggunakan pendekatan *maturity* model.
f. Penulis memberikan dokumentasi hasil audit yang disertakan dengan dokumen rekomendasi hasil audit kepada objek penelitian.

1.4 Maksud dan Tujuan Penelitian

Sistem komputer sangat kompleks sehingga tidak ada satu pun sistem yang ada benar-benar aman, secanggih apa pun program yang dibangun akan selalu terdapat *bugs* atau kesalahan di dalamnya. Sistem jaringan komputer membuat semua hal menjadi lebih mudah karena kita dapat terhubung dengan semua *host* yang terdaftar secara *public* di seluruh dunia, akan tetapi juga dapat menjadikan

sistem lebih rentan disusupi. Setiap celah yang ada dapat di manfaatkan oleh orang yang tidak bertanggung jawab untuk masuk ke dalam sistem dan mencuri data-data penting, untuk itu jaringan komputer perlu selalu diawasi dan di evaluasi, dengan begitu setiap kelemahan sistem keamanan yang ada dapat di tutupi.

Tujuan dilakukannya penelitian ini adalah membuat perancangan audit tata kelola TI dan jaringan komputer kemudian melakukan evaluasi untuk memperoleh tingkat kematangan tata kelola TI dan jaringan di tempat tersebut, mampu menerapkan tata kelola TI secara efektif efisien dan konsisten, serta untuk memenuhi sebagian persyaratan kelulusan dalam jenjang sarjana (S1) di Universitas Amikom Yogyakarta.

1.5 Manfaat Penelitian

a. Memberikan informasi terkini sistem keamanan jaringan SMK PI Ambarukmo.
b. Memberikan skor tingkat kematangan tata kelola TI di tempat tersebut.
c. Menghasilkan dokumen audit sebagai acuan SMK PI Ambarrukmo dalam pengambilan langkah-langkah pengembangan tata kelola TI dan keamanan jaringan komputer.
d. Meningkatkan kesadaran pentingnya menjaga kerahasiaan data dan informasi yang dimiliki.
e. Dapat menjadi referensi pada penelitian yang berkaitan dengan audit keamanan jaringan komputer di masa mendatang.

1.6 Metode Penelitian

Penelitian ini menggunakan metode sebagai berikut:

1.6.1 Metode Pengumpulan Data

Berikut adalah beberapa metode yang digunakan dalam pengambilan data:

1.6.1.1 Studi Literatur

Penulis mengumpulkan data dari berbagai sumber tidak langsung seperti buku-buku, jurnal dan karya ilmiah lain seperti skripsi.

1.6.1.2 Observasi

Peneliti melakukan peninjauan objek penelitian secara langsung untuk mengumpulkan informasi yang perlukan.

1.6.1.3 Wawancara

Peneliti melakukan seksi tanya jawab dengan staf / administrator jaringan sekolah untuk mendapatkan informasi yang dibutuhkan, selain tanya jawab penulis juga akan memberikan kuesioner.

1.6.2 Metode Audit

PLAN – DO – CHECK – ACT (PDCA) adalah metode audit yang akan diterapkan pada penelitian ini. Proses ini meliputi perencanaan audit, pelaksanaan audit, evaluasi hasil audit dan pembuatan rekomendasi dari setiap kelemahan yang ditemukan.

1.7 Sistematika Penulisan

Penulisan penelitian ini disusun secara sistematis dan dibagi dalam beberapa bagian bab. Urutan penulisan dalam penelitian ini dimaulai dari BAB I sampai BAB V.

BAB I. PENDAHULUAN

Bab ini menerangkan tentang latar belakang, rumusan masalah, batasan masalah, maksud dan tujuan penelitian, manfaat penelitian, metode penelitian dan sistematika penulisan.

BAB II. LANDASAN TEORI

Bagian ini berisi tentang tinjauan pustaka dan landasan teori yang berkaitan dengan topik yang akan dibahas dalam penelitian ini.

BAB III. METODE PENELITIAN

Bagian ini berisi tentang uraian rinci tentang metode penelitian yang memberikan penjelasan mengenai detail langkah-langkah yang dilakukan untuk mencapai tujuan dan simpulan akhir penelitian.

BAB IV. HASIL DAN PEMBAHASAN

Bagian ini memuat hasil dari penelitian dan pembahasan penelitian yang telah dilakukan.

BAB V. PENUTUP

Bab ini berisi tentang kesimpulan dan saran-saran untuk penelitian selanjutnya.