BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi (TI) setiap hari berkembang pesat, dimana memiliki dampak bagi perkembangan organisasi atau perusahaan, untuk itu suatu organisasi harus beradaptasi untuk mengimplementasikan kemajuan TI [1]. TI harus dijaga sehingga perannya lebih maksimal, penggunaan teknologi informasi di suatu organisasi akan memberikan keunggulan dan keuntungan bagi perusahaan. Koperasi Pekerja Kekar sangat membutuhkan teknologi informasi dalam menjalankan seluruh alur bisnis yang ada. Pada perusahaan penyajian seluruh data membutuhkan teknologi informasi, mulai dari data *inventory* atau gudang, data pembelian barang atau jasa, data aktivitas *finance* seperti kerjasama dengan bank yang berhubungan dengan operasional perusahaan, data aktivitas dari transaksi seperti mutasi antar kas atau bank, laporan gaji, dan laporan keuangan.

Dalam menggerakkan bisnisnya koperasi pekerja kekar menggunakan aplikasi *Accurate*. *Accurate* merupakan software akuntansi yang mempunyai fungsi untuk pembukuan perusahaan yang ada di Indonesia seperti bergerak dibidang, jasa, dagang, distributor, kontraktor dan manufaktur. Aplikasi *accurate* sangat menunjang sumber daya IT yang mempermudah organisasi dalam menjalankan alur bisnisnya. [2].

Menurut survei yang dilakukan oleh *Information Security Breaches Survey (ISBS)* terdapat peningkatan pelanggaran yang terjadi pada keamanan informasi disetiap tahunnya, pada tahun 2014 organisasi yang berskala kecil terjadi pelanggaran keamanan sebesar 60%, pada tahun 2015 meningkat sebesar 14% menjadi 74%. Tahun 2017 perusahaan mendapat rata-rata *e-mail spam* sebesar 45,2% dan *e-mail malware* sebesar 12,8% yang terjadi pada perusahaan skala menengah dan kecil. Perihal tersebut organisasi belum sadar akan pentingnya manajemen keamanan

informasi, ketika ancaman sudah terjadi keamanan informasi akan menjadi permasalahan yang fatal [3].

Dilaksanakannya tata kelola teknologi informasi terdapat faktor keamanan informasi yang menjadi pertimbangan utama untuk diperhatikan. Informasi yang menjadi objek utama dalam tata kelola TI jika mengalami masalah keamanan informasi akan mengakibatkan kinerja tata kelola TI terganggu [4].

Keamanan informasi adalah masalah berkaitan dengan kerahasiaan (*confidentiality*), keutuhan (*integrity*) dan ketersediaan (*availability*), ketiga hal ini sangat penting dalam tata kelola IT untuk menghindari dari akses yang tidak mempunyai hak terhadap sistem. akses itu antara lain perubahan data, penghapusan data dan pencurian data dari sistem tanpa sepengetahuan oleh pihak yang berwenang. Untuk itu diperlukannya audit atau suatu evaluasi terhadap keamanan sistem informasi. Audit atau evaluasi keamanan sistem informasi adalah prosedur yang dilaksanakan untuk mengurangi kemungkinan bahaya kelemahan suatu sistem informasi terhadap akses yang tidak pantas [5].

Berdasarkan hasil wawancara yang dilakukan kepada salah satu karyawan *accounting* aplikasi *accurate* di Koperasi pekerja. Pertama, aplikasi *accurate* yang digunakan perusahaan belum pernah melaksanakan audit keamanan informasi sehingga belum pernah mengetahui bagaimana tingkat pencapaian dalam sistem keamanan yang telah digunakan.

Kedua, adanya ancaman yang menyerang seperti virus, sharing password, kehilangan data, serta koneksi internet dan listrik padam. Ketiga prosedur keamanan sistem informasi yang belum terdokumentasi, walaupun sudah terdapat instalasi antivirus, perawatan sederhana, backup data, dan penggunaan utilitas yang mendukung ancaman keamanan informasi dapat terjadi sewaktu-waktu.

Kedua, ada bahaya yang menyerang, misalnya virus, berbagi kata sandi, kehilangan informasi, dan matinya koneksi internet. Ketiga prosedur keamanan informasi yang

dijalankan hanya sebatas saja tidak terdapat pendokumentasiannya, meskipun sudah memasang anti virus, pemeliharaan sistem informasi, dilakukannya *backup* data, dan pemanfaatan utilitas pendukung namun ancaman keamanan informasi bisa saja terjadi. Untuk mengetahui aplikasi *accurate* tersebut sudah berjalan dengan baik juga sudah memenuhi kebutuhan pengguna, maka diperlukan adanya proses audit layanan teknologi informasi. Dengan manajemen sistem keamanan informasi yang baik, diharapkan dapat meminimalkan risiko yang akan mengganggu kelangsungan bisnis organisasi.

Peneliti akan menggunakan Indeks KAMI sebagai standar penilaian. Indeks KAMI adalah sebuah metode evaluasi berbasis SNI-ISO/IEC 27001:2013 berskala nasional yang digunakan untuk menganalisa tingkat kesiapan pengamanan informasi pada instansi pemerintah ataupun non pemerintah. Metode evaluasi pada indeks KAMI memiliki tujuan memberikan gambaran dari kondisi kesiapan kelengkapan dan kematangan keamanan informasi pada suatu organisasi[6]. Selanjutnya akan memberikan rekomendasi sesuai hasil evaluasi Indeks KAMI terhadap SNI ISO/IEC 27001 dan melakukan *Risk Assessment* atau penilaian risiko terhadap Koperasi Pekerja Kekar.

Berdasarkan uraian yang telah dijelaskan maka penulis akan melakukan penelitian pada aplikasi *accurate* di Koperasi Pekerja Kekar dengan judul “Peran Pengendalian Internal dan Evaluasi Keamanan Informasi Di Koperasi Pekerja Kekar Menggunakan Metode Indeks Kami Berdasarkan SNI ISO 27001:2013”.

1.2 Rumusan Masalah

Rumusan masalah yang menjadi fokus dalam penelitian ini, yaitu:

1. Bagaimana nilai kematangan, kelengkapan, kesiapan pengelolaan keamanan informasi serta *risk assessment* pada Koperasi Pekerja Kekar?
2. Bagaimana rekomendasi yang diusulkan dari pengendalian internal dan evaluasi keamanan informasi menggunakan Indeks KAMI berdasarkan standar ISO/IEC 27001:2013 di Koperasi Pekerja Kekar?

1.3 Batasan Masalah

Batasan masalah dalam penelitian ini antara lain:

1. Pengendalian internal hanya mencangkup keamanan informasi dan penilaian risiko di Koperasi Pekerja Kekar.
2. Penilaian yang dilakukan menggunakan standar penilaian Indeks Keamanan Informasi (KAMI) versi 4.1 dari Kementerian Kominfo yang dibuat oleh Badan Siber dan Sandi Negara (BSSN) .
3. Lingkup penilaian hanya pada pengelolaan keamanan informasi menggunakan indeks KAMI meliputi tata kelola, pengelolaan risiko, kerangka kerja, pengelolaan aset, dan aspek teknologi pada Koperasi Pekerja Kekar.
4. Lingkup penilaian risiko meliputi identifikasi aset, identifikasi ancaman, identifikasi risiko di Koperasi Pekerja Kekar.

1.4 Tujuan Penelitian

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Mengetahui gambaran kondisi kesiapan kelengkapan kerangka kerja keamanan teknologi informasi pada Koperasi Pekerja Kekar dengan kriteria SNI ISO/IEC 27001:2013.
2. Memberikan tingkat kematangan keamanan informasi menggunakan indeks KAMI sesuai dengan kontrol SNI ISO 27001:2013 di koperasi pekerja kekar.
3. Memberikan mitigasi risiko berupa kontrol SNI ISO 27001:2013 terhadap aset di Koperasi Pekerja Kekar.
4. Memberikan rekomendasi berdasarkan analisis menurut standar Indeks Keamanan Informasi (KAMI) berdasarkan dengan SNI ISO 27001:2013 untuk memperbaiki dan meningkatkan keamanan informasi pada Koperasi Pekerja Kekar.

1.5 Sistematika Penulisan

Adapun sistematika penulisan penyusunan tugas akhir ini kedalam lima bab yang diuraikan sebagai berikut:

BAB I Pendahuluan

Bab I akan membahas tentang latar belakang, rumusan masalah, batasan masalah, tujuan penelitian, metodologi dan sistematika penulisan tugas akhir.

BAB II Tinjauan Pustaka

Bab II akan menjelaskan bagian kajian kepustakaan sebagai acuan untuk teori-teori yang berkaitan dengan penelitian.

BAB III Metodologi Penelitian

Bab III ini akan membahas metodologi analisis yang akan digunakan dalam penelitian evaluasi dan pengendalian internal yang mencakup skema penelitian, metode pengumpulan data, metode analisis data, tahapan penelitian dan jadwal penelitian.

BAB IV Hasil dan Pembahasan

Bab IV ini membahas mengenai hasil dari penelitian yang dilakukan dan memberikan analisis atau pembahasan mengenai hasil pada setiap metode yang digunakan.

BAB V Penutup

Bab V ini berisi tentang kesimpulan serta saran terkait evaluasi keamanan informasi dan pengendalian internal yang diberikan oleh penulis dari hasil penelitian yang sudah dilaksanakan.