BAB I
PENDAHULUAN

Pada bab ini akan dibahas tentang latar belakang yang melandasi penelitian Tesis ini, pembatasan masalah dan rumusan dari permasalahan dalam penelitian Tesis ini, serta tujuan dan manfaat dari penelitian Tesis ini dilihat dari tinjauan praktis dan teoritis.

I.1 Latar Belakang Masalah

Informasi dinilai sebagai aset penting dalam kehidupan berorganisasi. Informasi dapat menjadi bahan masukan untuk mengambil keputusan bagi organisasi. Sebagai konsekuensinya, jika informasi tersebut jatuh atau diakses oleh pihak yang tidak berhak maka dapat menimbulkan kerugian bagi organisasi.

Informasi yang dikelola dalam organisasi bergerak sangat dinamis sejak dibuat, dipindahkan, disimpan, hingga dipergunakan. Sementara itu, informasi juga dapat disimpan di berbagai media, dapat dimodifikasi dengan relatif mudah, serta dapat dipindahkan dari satu media ke media yang lain dalam waktu yang relatif cepat.

Kemudahan pengolahan informasi tersebut membawa dampak positif bagi organisasi, namun muncul pula berbagai kerawanan yang mengancam eksistensi informasi sebagai aset organisasi. Kerawanan yang banyak terjadi berupa pencurian, penyadapan, perusakan, modifikasi informasi, bencana alam, penyalahgunaan, sabotase, kesalahan prosedur dari pengguna informasi dan masih banyak lagi. Kerawanan-kerawanan tersebut dapat mengakibatkan kerusakan bahkan kehilangan informasi.

Hilangnya informasi dapat menimbulkan dampak yang fatal bagi organisasi. Misalnya, modifikasi oleh pihak yang tidak berhak atas suatu data dalam daftar agenda kegiatan dapat mengakibatkan kekacauan kinerja organisasi. Contoh yang lebih berakibat fatal misalnya pencurian informasi dan data yang berkaitan dengan keuangan dan hal-hal yang bersifat strategis milik organisasi.

Organisasi pemerintah pun tak luput dari ancaman keamanan informasi dikaitkan dengan perkembangan peradaban baru yakni *e-civilization. E-civilization* adalah suatu sistem dimana masyarakat saling terhubung memanfaatkan internet. Peradaban ini memudahkan masyarakat untuk saling berhubungan kapan saja dan dimana saja melalui

dunia maya. Fenomena peradaban baru ini juga melanda instansi pemerintah di Indonesia. Terkait hal tersebut, pemerintah Indonesia telah menerbitkan Instruksi Presiden tentang *e-government.*

Berdasarkan Instruksi Presiden Nomor 3 Tahun 2003 Tentang Kebijakan dan Strategi Nasional Pengembangan *e-Government*, pemerintah harus mampu memanfaatkan kemajuan teknologi informasi untuk meningkatkan kemampuan mengolah, mengelola, menyalurkan, dan mendistribusikan informasi dan pelayanan publik. Melalui tata kelola teknologi informasi dan komunikasi diharapkan dapat mendukung terwujudnya *good governance* pada pemerintahan di Indonesia.

Seperti penerapan teknologi informasi yang lainnya, penerapan *e-government* selain memiliki manfaat dapat pula menimbulkan ancaman terhadap informasi oleh pihak yang tidak berkepentingan. Munculnya gangguan terhadap informasi pada *e-government* dapat berujung pada ancaman stabilitas nasional. Padahal fakta yang ada di Indonesia mencerminkan pelaksanaan *e-government* masih belum berjalan aman. Situs *www.zone-h.org* menyebutkan bahwa dari bulan September 2011 hingga April 2012 tercatat sejumlah serangan pada domain "*go.id*". Serangan-serangan tersebut terjadi sebanyak 1.250 kali atau sebanyak tujuh *website* instansi pemerintah yang diserang dalam satu hari (Jumiati, 2012).

Pada era pemerintahan Joko Widodo dan Jusuf Kalla, e-government diharapkan dapat meningkatkan pengawasan terhadap akuntabilitas kegiatan dan anggaran dari instansi pemerintah. Era pemerintahan yang dipimpin Joko Widodo saat ini lebih menekankan untuk memanfaatkan teknologi informasi untuk menunjang kinerja Kabinet Kerjanya. Untuk meningkatkan keamanan informasi di pemerintahan, Joko Widodo menginstruksikan untuk melakukan upaya pengamanan terhadap informasi yang ada di pemerintahan.

Dalam Siaran Pers Nomor 100/PIH/KOMINFO/12/2013 Tentang Laporan Akhir Tahun 2013 Kementerian Komunikasi dan Informatika, Indonesia telah menjadi negara target serangan maya terbesar di dunia, yakni mencapai 1.277.578 serangan dalam per bulan atau sekitar 42.000 serangan per hari. Baru kemudian disusul Amerika Serikat (dengan 332.000 serangan atau 11.000 serangan per hari) dan berikutnya RRC (dengan 151.000 serangan atau 5.000 serangan per hari).

Data Breach Investigation Report – Verizon (Verizon, 2010), menyebutkan bahwa sumber daya manusia adalah faktor yang paling menonjol sebagai celah yang patut diwaspadai dalam kerawanan keamanan informasi. Temuan menunjukkan bahwa selama tahun 2008-2010 hampir satu dari tiga kerawanan informasi berasal dari serangan faktor manusia dari dalam organisasi sendiri. Sementara itu InfoSecurity Europe, 2010, Information Security Breaches Survey 2010 (ISBS-2010) menyebutkan bahwa tipe-tipe celah kerawanan keamanan informasi selain sumber daya manusia adalah sebagai berikut:

a. Kegagalan sistem dan data : 70% dari responden
b. Infeksi virus : 52% dari responden
c. Pencurian : 49% dari responden
d. Kesalahan manusia : 80% dari responden
e. Serangan pihak yang tidak sah : 63% dari responden

Dengan adanya kerawanan keamanan informasi yang dapat mengancam sistem *e-government* dan stabilitas nasional, maka aspek yang penting untuk diperhatikan adalah upaya keamanan informasi. Keamanan informasi merupakan istilah untuk menggambarkan langkah-langkah melindungi informasi dari ancaman dan kerawanan yang senantiasa berkembang seiring kemajuan teknologi. Langkah-langkah tersebut secara tidak langsung menjamin keberlangsungan organisasi serta menekan terjadinya risiko keamanan yang mungkin terjadi. Maka dari itu sistem tata kelola keamanan informasi menjadi sangat penting untuk diimplementasikan pada organisasi agar informasi dapat selalu terlindungi.

International of Standard Organization (ISO) adalah organisasi yang membahas tentang standard yang anggotanya merupakan badan nasional yang relevan dari berbagai negara (ISO, 2005). ISO telah menerbitkan suatu standar untuk mengelola keamanan informasi bagi organisasi yakni ISO/IEC 27001: 2005. Di Indonesia, standar tersebut diadopsi menjadi SNI ISO/IEC 27001:2009 melalui metode terjemahan oleh Panitia Teknis PK 03-02 Sistem Manajemen Mutu yang dibentuk oleh Badan Standardisasi Nasional (BSN).

SNI ISO/IEC 27001: 2009 merupakan dokumen standar Sistem Manajemen Keamanan Informasi yang memberikan gambaran secara umum mengenai apa saja yang seharusnya dilakukan dalam usaha mengimplementasikan konsep-konsep keamanan

informasi organisasi. Di dalamnya terdapat aturan dan pengelolaan keamanan informasi. Elemen keamanan informasi yang dibahas bukan hanya yang berkaitan dengan bidang teknologi saja, tetapi juga masalah sumber daya manusia, kebijakan, fasilitas, serta sarana prasarana yang dimiliki oleh organisasi.

Terkait instruksi Presiden tentang penerapan e-government dan pengamanan informasi milik pemerintahan, serta pentingnya pengawasan kinerja dan akuntabilitas keuangan instansi pemerintah, maka perlu dilakukan upaya optimalisasi terhadap tugas dan fungsi unit kerja pengawasan pada instansi pemerintah, dalam hal ini Inspektorat maupun Inspektorat Jenderal pada suatu Kementrian atau Lembaga Non-Kementerian.

Inspektorat merupakan unit kerta pengawasan di Lembaga Sandi Negara (Lemsaneg). Inspektorat dipimpin oleh Inspektur yang berada di bawah Kepala Lemsaneg dan bertanggung jawab langsung kepada Kepala Lemsaneg. Inspektorat mempunyai tugas melakukan pengawasan terhadap pelaksanaan tugas di lingkungan Lemsaneg dan menangani data-data strategis tentang pelaksanaan kegiatan di lingkungan Lemsaneg yang bersifat rahasia.

Berdasarkan Laporan Akuntabilitas Kinerja Instansi Pemerintah (LAKIP) Inspektorat pada tahun 2013 dan 2014, kinerja Unit Kerja Inspektorat dilihat dari hasil audit terhadap kegiatan dan anggaran yang ada di Lemsaneg. Informasi mengenai kegiatan yang ada di Lemsaneg merupakan informasi sensitif terkait anggaran, operasional dan penelitian persandian nasional. Dalam melaksanakan tugasnya, Inspektorat membutuhkan peralatan berbasis IT seperti komputer dan penyimpanan data terpusat. Oleh karena itu, perlu dilakukan pengukuran terhadap kesiapan pengamanan informasi yang ada di Inspektorat Lemsaneg.

Kesiapan pengamanan informasi di Inspektorat Lemsaneg dapat dianalisa dengan mengacu pada SNI ISO/IEC 27001: 2009. Lalu analisis terhadap kesiapan pengamanan informasi tersebut dilakukan menggunakan *gap analysis*, karena analisis tersebut dapat mengetahui kesenjangan antara kondisi Inspektorat saat ini dengan kondisi ideal pada SNI ISO/IEC 27001: 2009. Selanjutnya hasil *gap analysis* dapat digunakan sebagai acuan dalam membuat rekomendasi penerapan pengamanan informasi yang ideal.

I.2 Pembatasan Masalah

Mengingat luasnya ruang lingkup informasi dan pengamanan informasi, penelitian Tesis ini dibatasi hanya meliputi topik sebagai berikut:

a. Lokus penelitian terbatas pada Inspektorat Lemsaneg, dimana Inspektorat merupakan unit kerja yang berperan dalam pengawasan terhadap kinerja dan akuntabilitas anggaran pada instansi pemerintah.
b. Standar yang digunakan sebagai acuan kesiapan pengamanan informasi menggunakan SNI ISO/IEC 27001: 2009. Standar ini memberikan persyaratan-persyaratan yang harus dipenuhi untuk memulai mengatur keamanan informasi. Standar SNI ISO/IEC juga dapat digunakan untuk bagian dari organisasi.

   Persyaratan dalam standar tersebut selanjutnya disebut dengan klausul yang terdiri dari 11 bagian yaitu:

   1) Kebijakan keamanan informasi yang diterapkan di Inspektorat Lemsaneg.
   2) Struktur Organisasi keamanan informasi yang ada pada Inspektorat.
   3) Manajemen aset yang dimiliki Inspektorat Lemsaneg.
   4) Pengelolaan insiden keamanan informasi di Inspektorat Lemsaneg terkait kesiapan pengamanan informasi.
   5) Sumber daya manusia Inspektorat Lemsaneg menyangkut keamanan informasinya.
   6) Keamanan fisik dan lingkungan di Inspektorat Lemsaneg terhadap kesiapan pengamanan informasi.
   7) Akses kontrol di lingkungan Inspektorat Lemsaneg.
   8) Komunikasi dan manajemen operasi di lingkungan Inspektorat Lemsaneg.
   9) Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi di lingkungan Inspektorat Lemsaneg.
   10) Manajemen kelangsungan bisnis (business continuity management) di lingkungan Inspektorat Lemsaneg.
   11) Kesesuaian di Inspektorat Lemsaneg.
c. Analisis yang digunakan untuk mengetahui kesiapan pengamanan informasi pada Inspektorat Lemsaneg menggunakan *gap analysis*.

I.3 Rumusan Permasalahan

Berdasarkan latar belakang dan pembatasan masalah yang telah dijelaskan sebelumnya, maka permasalahan yang akan dibahas dalam penelitian ini adalah:

a. Bagaimana tingkat kesiapan pengamanan informasi di Inspektorat Lemsaneg?
b. Bagaimana tingkat kesiapan pelaksana dan keamanan lingkungan Inspektorat Lemsaneg?
c. Bagaimana tingkat kesesuaian proses kerja di Inspektorat Lemsaneg terhadap pengamanan informasi?

I.4 Tujuan Dan Manfaat Penelitian

a. Tujuan

   Tujuan yang ingin dicapai dari penelitian ini adalah:

   1) Mengetahui hasil *gap analysis* tentang kesiapan pengamanan informasi pada Inspektorat Lemsaneg berdasarkan SNI ISO/IEC 27001: 2009.
   2) Mengetahui rekomendasi penerapan SMKI pada unit kerja Inspektorat Lemsaneg berdasarkan *gap analysis*.

b. Manfaat

   Manfaat dari penelitian ini ada dua dimensi. Pertama adalah dimensi akademis, yakni penelitian ini dapat memperkaya pengetahuan tentang penerapan sistem manajemen keamanan informasi sehingga teori yang telah ada dapat terus dikembangkan.

   Selain itu penelitian ini memiliki manfaat berdimensi praktis, yakni dapat membantu menumbuhkan kesadaran akan pentingnya keamanan informasi hingga nantinya dapat membantu organisasi untuk menetapkan dan menerapkan peraturan tentang tata kelola keamanan informasi.