

BAB I

PENDAHULUAN

1.1 Latar Belakang

Radio Republik Indonesia adalah suatu studio siaran yang menyelenggarakan penyiaran informasi maupun hiburan berupa musik, sandiwara dan sebagainya yang dikemas dalam suatu acara. Semua acara tersebut dipenuhi semata-mata untuk memenuhi kebutuhan masyarakat akan informasi sehingga peristiwa yang sedang terjadi di nusantara ini dapat diketahui dengan cepat. Maka dari itu dalam melaksanakan siaran ini, RRI mempunyai tujuan sebagai titik acuan. Tujuan tersebut adalah sebagai berikut: Menyebarluaskan informasi pemerintah serta memberikan hiburan kepada masyarakat dan memberikan pendidikan.

Sesuai dengan Peraturan Pemerintah Republik Indonesia No.12 Tahun 2005 tentang Lembaga Penyiaran Publik tanggal 18 Maret 2005, RRI Surabaya menempati stasiun type B yang beralamatkan di Jl. Pemuda No. 82-90 Surabaya. RRI Surabaya memiliki banyak aset meliputi aset informasi, aset piranti lunak, aset fisik, dan layanan. Salah satu aset tersebut dikelola oleh bagian Pengembangan Multimedia Baru (PMB) yang merupakan bagian pengelolaan informasi data yang digunakan untuk menunjang siaran seperti: menyimpan berita yang akan disiarkan, menyimpan lagu, serta tugas yang mendukung siaran dalam lingkup Radio RRI Surabaya. Bagian PMB juga mengumpulkan sementara berita dari seluruh stasiun kelas tiga Jawa Timur yang selanjutnya dikirim ke stasiun kelas satu pada rentang waktu tertentu.

Bagian PMB yang dimiliki oleh RRI Surabaya terintegrasi dengan seluruh RRI kelas tiga seluruh Jawa Timur dan RRI kelas satu di Jakarta. Selain itu RRI Surabaya terintegrasi secara online dan memiliki jaringan komputer yang terbagi menjadi empat server, yaitu server berita, lagu, backup, dan server streaming. Dengan demikian, sebagai stasiun penyiaran kelas dua yang memiliki seluruh informasi penyiaran publik RRI Surabaya harus memiliki jaringan streaming data, back up, dan recovery yang berjalan dengan baik.

Selama ini bagian PMB mengalami permasalahan dari sisi *Confidentiality* adalah kesalahan penyimpanan berita yang tidak sesuai dengan perencanaan. Dampak dari permasalahan ini adalah terganggunya pihak penyiar membaca berita, sehingga siaran langsung menjadi tidak akurat. Dari sisi *Integrity* adalah keutuhan berita hasil liputan langsung yang diakses tidak lengkap. Keutuhan berita hasil liputan yang tidak lengkap akan berdampak pada turunya rating acara siaran serta mempengaruhi kualitas acara tersebut. Dari sisi *Availability* adalah keterlambatan peyediaan informasi, berita, siaran langsung, hiburan, dan iklan. Hal ini dapat menyebabkan terjadinya risiko menurunnya tingkat kepercayaan pendengar dan *stakeholder* pada RRI Surabaya, serta menyebabkan kerugian bagi RRI Surabaya.

Selama ini bagian PMB belum pernah melakukan analisa penyebab terjadinya permasalahan tersebut, oleh karena itu bagian PMB tidak mengetahui bagaimana tingkat keamanan informasi yang dimilikinya. Evaluasi keamanan informasi dapat dilakukan dengan Audit Keamanan Informasi, hal ini diperlukan untuk memenuhi Surat Perintah Perusahaan RRI Surabaya Nomor: 18/SPI/02/2014 tentang kebijakan keamanan informasi. Apabila bagian

multimedia baru tidak memenuhi prosedur yang terdapat pada Surat Perintah Perusahaan RRI Surabaya Nomor: 18/SPI/02/2014 tentang Kebijakan Keamanan Informasi, dikhawatirkan menyebabkan risiko tidak adanya aspek kerahasiaan (*confidentiality*), keutuhan (*integrity*), dan ketersediaan (*availability*) dari informasi menjadi terganggu (ISO/IEC 27002, 2005). Agar audit keamanan informasi dapat berjalan dengan baik diperlukan suatu standar untuk melakukan audit tersebut (Tanuwijaya dan Sarno, 2010). Tidak ada acuan baku mengenai standar apa yang akan digunakan atau dipilih oleh perusahaan untuk melaksanakan audit keamanan informasi (Sarno dan Iffano, 2009).

Standar ISO 27002:2005 dipilih dengan pertimbangan bahwa didalamnya berisi panduan praktis (*code of practice*) teknik keamanan informasi. Pertimbangan lainnya adalah ISO 27002:2005 menyediakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) untuk digunakan oleh mereka yang bertanggung jawab untuk proses implementasi, dan pemeliharaan *Information Security Management Systems* (ISMS) pada suatu organisasi (Sarno, 2009). Standar ini tidak mengharuskan bentuk-bentuk kontrol yang tertentu tetapi menyerahkan kepada pengguna untuk memilih dan menerapkan kontrol yang tepat sesuai kebutuhannya khususnya pada bagian PMB.

Dengan adanya audit keamanan informasi pada bagian PMB di RRI Surabaya melalui penyusunan Tugas Akhir maka diharapkan dapat mengukur tingkat keamanan informasi yang ada, sehingga akan menentukan apakah Sistem Manajemen Keamanan Informasi (SMKI) yang diterapkan sesuai dengan hasil yang diharapkan. Hasil audit ini diharapkan menjadi masukan yang dapat

digunakan untuk meningkatkan keamanan informasi pada bagian PMB di RRI Surabaya.

Mengacu pada hasil review, survei dan wawancara yang telah dilakukan, maka klausul yang ditetapkan sebanyak 3 klausul yaitu keamanan sumber daya manusia (klausul 8) untuk memastikan bahwa informasi hanya diakses oleh orang yang memiliki hak akses, wilayah aman (klausul 9) untuk menjaga informasi selalu utuh dan akurat, kontrol akses (klausul 11) untuk memastikan bahwa informasi selalu tersedia jika diperlukan dan khusus diakses bagi orang yang berwenang. Ketiga klausul yang ditetapkan ini telah memperoleh persetujuan dan kesepakatan bersama oleh Kepala seksi PMB yang akan tertuang dalam dokumen *engagement letter*.

Dengan adanya audit keamanan informasi pada bagian PMB di RRI Surabaya melalui penyusunan Tugas Akhir maka diharapkan dapat mengukur tingkat keamanan informasi yang ada, sehingga akan menentukan apakah Sistem Manajemen Keamanan Informasi SMKI yang diterapkan sesuai dengan hasil yang diharapkan. Hasil audit ini diharapkan menjadi masukan yang dapat digunakan untuk meningkatkan keamanan informasi pada bagian PMB di RRI Surabaya.

1.2 Perumusan Masalah

Berdasarkan penjelasan pada latar belakang, maka perumusan masalah yang didapat adalah sebagai berikut:

1. Bagaimana membuat perencanaan Audit Keamanan Informasi pada bagian PMB di RRI Surabaya berdasarkan ISO 27002:2005?

2. Bagaimana melaksanakan audit keamanan informasi pada bagian PMB di RRI Surabaya berdasarkan standar ISO 27002:2005?
3. Bagaimana menyusun hasil audit keamanan informasi yang dilakukan pada bagian PMB di RRI Surabaya berdasarkan standar ISO 27002:2005?

1.3 Batasan Masalah

Berdasarkan perumusan masalah diatas, maka tujuan dalam audit keamanan sistem informasi ini, agar tidak menyimpang dari tujuan yang akan dicapai maka pembatasan masalah dibatasi pada hal-hal sebagai berikut:

1. Bagian Sistem informasi yang diaudit adalah Pengembangan Multimedia Baru di RRI Surabaya.
2. Periode data yang digunakan untuk audit keamanan sistem informasi, Januari 2013 sampai Januari 2014
3. Tahapan audit yang digunakan adalah tahapan Davis dkk. 2011.
4. Metode audit dilakukan sampai tahap *Report drafting and issuance* atau tahap laporan audit.

1.4 Tujuan

Berdasarkan rumusan masalah yang ada maka tujuan yang akan dicapai dalam audit keamanan sistem informasi pada bagian PMB di Radio Republik Indonesia (RRI) Surabaya adalah sebagai berikut:

1. Menghasilkan perencanaan Audit Keamanan Informasi pada bagian Pengembangan Multimedia Baru berdasarkan standar ISO 27002:2005 yang terdiri dari menentukan ruang lingkup, mengumpulkan data, dan menentukan langkah-langkah pelaksanaan audit.

2. Melaksanakan Audit Keamanan Informasi pada bagian Pengembangan Multimedia Baru berdasarkan standar ISO 27002:2005 dengan menganalisa hasil wawancara berupa bukti, dan temuan-temuan audit.
3. Menyusun hasil Audit Keamanan Informasi pada bagian Pengembangan Multimedia Baru berdasarkan standar ISO 27002:2005 dengan melakukan analisa dan evaluasi dari bukti dan temuan yang ada sehingga didapat hasil audit yang berupa temuan dan rekomendasi.

1.5 Manfaat

Berdasarkan tujuan audit keamanan sistem informasi ini maka didapatkan beberapa manfaat sebagai berikut:

1. Untuk bagian pengembangan multimedia baru di Radio Republik Indonesia (RRI) Surabaya
 - a. Membantu untuk mengetahui beberapa ketidak sesuaian prosedur pemrosesan informasi berdasarkan hasil temuan yang ada.
 - b. Mendapatkan kontribusi untuk meningkatkan keamanan sistem informasi dengan standar ISO 27002:2005.
 - c. Memperoleh acuan untuk menangani permasalahan yang terjadi di bagian PMB.
 - d. Memberikan kontribusi untuk meningkatkan keamanan sistem informasi dengan standar ISO 27002:2005.
 - e. Hasil analisa dan penelitian yang dilakukan dapat menjadi bahan masukan bagi pihak RRI Surabaya khususnya bagian PMB dan rekomendasi untuk menangani masalah yang telah ditemukan.

2. Bagi mahasiswa (Peneliti)
 - a. Dapat memahami sistem kerja yang ada di instansi penyiaran radio.
 - b. Dapat menerapkan sekaligus mengembangkan ilmu yang dipelajari selama perkuliahan khususnya di bidang Audit Keamanan Informasi dengan standar ISO 27002:2005 sesuai dengan judul penelitian Tugas Akhir.
 - c. Menambah wawasan dan pengetahuan untuk mempersiapkan diri baik secara teoritis dan praktis.

1.6 Sistematika Penulisan

Di dalam penulisan Tugas Akhir ini secara sistematika diatur dan disusun dalam 5 (lima) bab, yaitu:

BAB I : PENDAHULUAN

Pada bab ini membahas tentang latar belakang masalah, rumusan masalah serta batasan terhadap masalah yang akan dibahas, tujuan dari pembahasan masalah yang diangkat, dan sistematika penulisan laporan tugas akhir ini.

BAB II : LANDASAN TEORI

Pada bab ini dibahas mengenai teori-teori yang berkaitan dengan Audit Keamanan Sistem Informasi, diantaranya yaitu penjelasan tentang Audit, Sistem Informasi, Audit Keamanan Informasi, Pengembangan Multimedia Baru, Standar Sistem Manajemen Keamanan Informasi, ISO/IEC 27002:2005.

BAB III : METODE PENELITIAN

Pada bab ini berisi penjelasan mengenai langkah-langkah yang dilakukan dalam audit keamanan informasi yang meliputi perencanaan audit, persiapan audit, pelaksanaan audit serta pelaporan audit.

BAB IV : HASIL DAN PEMBAHASAN

Pada bab ini dibahas tentang analisa dan evaluasi hasil temuan serta rekomendasi dari kegiatan audit keamanan informasi pada bagian Pengembangan Multimedia Baru di RRI Surabaya.

BAB V : PENUTUP

Pada bab ini berisikan kesimpulan penelitian yang telah dilakukan terkait dengan tujuan dan permasalahan yang ada, serta saran sehubungan dengan adanya kemungkinan audit keamanan informasi pada masa yang akan datang.

