

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi mendorong berbagai organisasi mengintegrasikan sistem digital guna mendukung operasional dan pelayanan publik [1]. Perubahan tersebut meningkatkan efisiensi proses kerja sekaligus kualitas layanan. Kendati demikian, perkembangan ini menghadirkan tantangan baru, terutama terkait keamanan informasi, seperti risiko kebocoran data hingga ancaman serangan siber yang kian kompleks [2]. Kondisi tersebut menempatkan keamanan informasi sebagai bagian krusial dalam tata kelola organisasi modern karena berkaitan langsung dengan perlindungan data, keberlanjutan operasional, serta tingkat kepercayaan publik terhadap organisasi [5].

Keamanan informasi tidak lagi dapat dipandang hanya dari aspek teknis semata. Penerapannya turut melibatkan kebijakan, prosedur kerja, pengelolaan sumber daya manusia, hingga manajemen risiko yang dijalankan secara terintegrasi agar sistem perlindungan berjalan lebih efektif [3]. Seluruh komponen tersebut membentuk sistem yang menentukan tingkat ketahanan perlindungan informasi dalam suatu organisasi. Oleh karena itu, evaluasi kesiapan keamanan informasi perlu dilakukan guna mengukur tingkat kematangan pengelolaan keamanan yang telah diterapkan [4]. Melalui evaluasi yang disusun secara sistematis, organisasi dapat memahami posisi aktualnya sekaligus mengidentifikasi area yang masih memerlukan perbaikan. Tanpa proses evaluasi tersebut, celah pengendalian berisiko tidak terdeteksi dan tidak terpetakan secara menyeluruh [5].

Salah satu standar internasional yang umum dijadikan acuan dalam pengelolaan keamanan informasi adalah ISO/IEC 27001:2022 [6]. Standar ini menyediakan kerangka kerja Sistem Manajemen Keamanan Informasi (SMKI) berpendekatan manajemen risiko untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi secara menyeluruh [7]. Melalui penerapan ISO/IEC 27001:2022, organisasi dapat membangun sistem keamanan yang terdokumentasi dengan baik, terukur efektivitasnya, serta dapat dikembangkan secara berkelanjutan [8]. Keberadaan kerangka kerja yang jelas ini menjadikan pengelolaan keamanan informasi lebih terarah dan konsisten dalam jangka panjang.

Di Indonesia, penilaian tingkat kesiapan keamanan informasi dapat dilakukan dengan menggunakan instrumen Indeks KAMI 5.0 yang dikembangkan oleh Badan Siber dan Sandi Negara (BSSN) [22]. Instrumen ini dirancang untuk mengukur tingkat kematangan keamanan informasi organisasi dengan mengacu pada kerangka kerja ISO/IEC 27001:2022 [18]. Melalui Indeks KAMI 5.0, berbagai aspek dievaluasi secara sistematis, meliputi tata kelola, manajemen risiko, kerangka kerja keamanan informasi, pengelolaan aset, dukungan teknologi, hingga perlindungan data pribadi [14]. Pendekatan ini membantu organisasi menilai sejauh mana praktik keamanan informasi telah diterapkan secara konsisten dan terarah.

Sejumlah penelitian terdahulu telah memanfaatkan Indeks KAMI untuk menilai keamanan informasi pada berbagai institusi, seperti instansi pemerintah, perguruan tinggi, dan rumah sakit[15]. Hasil penelitian menunjukkan bahwa sebagian besar organisasi masih berada pada tahap kematangan awal hingga menengah, yang menandakan perlunya upaya penguatan, khususnya pada aspek manajemen risiko dan tata kelola keamanan informasi [21]. Temuan lain turut memperlihatkan bahwa evaluasi dengan Indeks KAMI efektif dalam memetakan kesenjangan antara praktik operasional eksisting dan standar ISO/IEC 27001[14]. Melalui pendekatan tersebut, organisasi dapat mengidentifikasi area yang perlu dibenahi secara lebih jelas agar pengelolaan keamanannya selaras dengan standar yang berlaku.

Sebagian besar penelitian terdahulu berfokus pada sektor pemerintah daerah dan institusi pendidikan[14]. di samping beberapa kajian pada fasilitas kesehatan yang menekankan pengukuran tingkat kematangan keamanan informasi melalui Indeks KAMI[8]. Sementara itu, pembahasan mengenai evaluasi kesiapan keamanan informasi pada lembaga penyiaran publik, khususnya di tingkat daerah, masih terbatas. Padahal, lembaga penyiaran publik memiliki profil risiko tersendiri. Perannya dalam menyebarkan informasi kepada masyarakat menuntut tingkat keandalan yang tinggi, sedangkan ketergantungannya pada sistem digital untuk mendukung operasional penyiaran menjadikan aspek keamanan informasi sangat krusial[19].

Sebagai lembaga penyiaran publik nasional, Lembaga Penyiaran Publik Radio Republik Indonesia (RRI) memegang peranan strategis dalam menyediakan informasi

yang akurat dan terpercaya bagi masyarakat[16]. Dalam menjalankan tugasnya, RRI memanfaatkan berbagai sistem informasi dan teknologi digital untuk mendukung proses penyiaran, pengelolaan arsip, serta distribusi konten[3]. Ketergantungan terhadap sistem digital menjadikan aspek keamanan informasi sangat krusial, tidak hanya untuk ranah teknis, melainkan juga demi mempertahankan kepercayaan publik dan keberlanjutan layanan [1].

RRI Lhokseumawe, sebagai bagian dari jaringan RRI nasional, turut memanfaatkan teknologi dalam aktivitas operasionalnya. Akan tetapi, hingga saat ini belum ada evaluasi terstruktur untuk mengukur tingkat kesiapan keamanan informasi yang mengacu pada ISO/IEC 27001:2022 dan Indeks KAMI 5.0. Kondisi tersebut memicu ketidakjelasan mengenai tingkat kematangan keamanan informasi yang telah dicapai serta potensi risiko yang belum teridentifikasi secara menyeluruh [3].

Berdasarkan kondisi tersebut, terdapat celah penelitian (*research gap*) berupa keterbatasan kajian yang secara khusus mengevaluasi kesiapan keamanan informasi pada lembaga penyiaran publik tingkat daerah, khususnya RRI Lhokseumawe. Oleh sebab itu, penelitian ini dilakukan untuk menilai tingkat kesiapan keamanan informasi menggunakan Indeks KAMI 5.0 yang mengacu pada ISO/IEC 27001:2022[5]. Hasil penelitian ini diharapkan dapat menyajikan gambaran tingkat kematangan, mengidentifikasi kesenjangan terhadap standar, serta merumuskan rekomendasi perbaikan yang terukur dan sistematis[2].

Selain itu, kondisi operasional LPP RRI Lhokseumawe saat ini memperlihatkan bahwa pengelolaan data masih didominasi proses manual. Meski demikian, hasil observasi terbaru menunjukkan bahwa instansi sedang berada dalam fase transisi menuju sistem informasi berbasis web. Walaupun sistem pusat berada di Jakarta, unit daerah menghadapi risiko kerentanan data yang tinggi selama masa migrasi, khususnya terkait adaptasi SDM terhadap pola kerja digital. Oleh karena itu, evaluasi kesiapan menggunakan Indeks KAMI 5.0 menjadi sangat mendesak untuk memastikan proses transisi berlangsung secara aman dan terstruktur[2].

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Bagaimana tingkat kesiapan dan kematangan keamanan informasi pada Lembaga Penyiaran Publik RRI Lhokseumawe berdasarkan standar ISO/IEC 27001:2022 menggunakan Indeks KAMI (BSSN)?
2. Rekomendasi apa yang dapat diberikan untuk meningkatkan kesiapan dan pengelolaan keamanan informasi di RRI Lhokseumawe berdasarkan hasil evaluasi yang dilakukan?

1.3 Tujuan Penelitian

Penelitian ini bertujuan untuk mencapai beberapa hasil yang diharapkan sebagai berikut:

1. Menilai tingkat kesiapan dan kematangan keamanan informasi pada Lembaga Penyiaran Publik RRI Lhokseumawe berdasarkan standar ISO/IEC 27001:2022 dan Indeks KAMI (BSSN).
2. Memberikan rekomendasi untuk meningkatkan kesiapan dan pengelolaan keamanan informasi di RRI Lhokseumawe berdasarkan hasil evaluasi

1.4 Batasan Masalah

Batasan masalah dalam penelitian ini ditetapkan sebagai berikut:

1. Penelitian ini hanya berfokus pada evaluasi kesiapan dan pengelolaan keamanan informasi pada tingkat organisasi, tanpa melakukan pengujian teknis keamanan sistem.
2. Kerangka kerja yang digunakan dalam penelitian ini terbatas pada ISO/IEC 27001:2022 dan Indeks KAMI (BSSN)
3. Objek penelitian dibatasi pada Lembaga Penyiaran Publik RRI Lhokseumawe
4. Ruang lingkup pengumpulan data melalui kuesioner dibatasi pada 7 (tujuh) orang responden kunci yang dipilih menggunakan teknik purposive sampling berdasarkan keterwakilan fungsi kerja di instansi.

1.5 Manfaat Penelitian

Manfaat Evaluasi Tingkat Kesiapan Keamanan Informasi Berdasarkan ISO/IEC 27001:2022 Menggunakan Indeks KAMI 5.0 (BSSN) pada Lembaga Penyiaran Publik RRI Lhokseumawe:

1. Menambah referensi dan wawasan akademik terkait evaluasi kesiapan keamanan informasi menggunakan ISO/IEC 27001:2022 dan Indeks KAMI pada lembaga publik.
2. Memberikan gambaran tingkat kesiapan keamanan informasi yang diterapkan di RRI Lhokseumawe
3. Menjadi bahan evaluasi dan pertimbangan manajemen dalam meningkatkan pengelolaan keamanan informasi
4. Memberikan rekomendasi strategis yang dapat digunakan sebagai dasar perencanaan peningkatan keamanan informasi