

# **BAB I**

## **PENDAHULUAN**

### **1.1 Latar Belakang Masalah**

Kemajuan teknologi informasi yang pesat telah memberikan dampak besar terhadap berbagai sektor kehidupan, termasuk sektor publik dan kesehatan. Teknologi ini tidak hanya dimanfaatkan untuk meningkatkan efisiensi dan produktivitas, tetapi juga menjadi faktor utama dalam mendorong transformasi digital secara menyeluruh. Masyarakat kini sangat bergantung pada sistem digital dalam aktivitas sehari-hari, sehingga menuntut tersedianya sistem informasi yang responsif, efisien, dan dapat diandalkan [1]. Dalam konteks ini, teknologi informasi tidak lagi hanya menjadi alat bantu administratif, tetapi telah bertransformasi menjadi elemen strategis yang mendukung percepatan layanan, efisiensi proses bisnis, serta peningkatan kesadaran akan pentingnya aspek keamanan informasi [2].

Transformasi digital di sektor kesehatan turut berkembang seiring dengan pemanfaatan teknologi informasi dalam mendukung layanan kesehatan. Pusat Kesehatan Masyarakat (Puskesmas) sebagai fasilitas kesehatan tingkat pertama telah mulai menerapkan berbagai sistem informasi elektronik seperti Sistem Informasi Manajemen Puskesmas (SIMPUS), E-Puskesmas, hingga integrasi data ke dalam platform nasional SATUSEHAT. Digitalisasi ini diharapkan dapat meningkatkan kualitas pelayanan dan efisiensi kerja petugas kesehatan [3].

Namun, di balik manfaat tersebut, terdapat tantangan serius terkait aspek keamanan informasi. Data pasien yang dikelola oleh Puskesmas bersifat sensitif dan harus dijaga kerahasiaannya. Di tengah meningkatnya ancaman serangan siber dan kebocoran data, sistem informasi kesehatan menjadi salah satu target utama peretasan. Berdasarkan studi terdahulu [4], banyak institusi layanan kesehatan di Indonesia belum menerapkan standar keamanan informasi secara menyeluruh. Hal ini terutama disebabkan oleh belum optimalnya proses identifikasi risiko, lemahnya mitigasi terhadap insiden keamanan, rendahnya

kesadaran staf terhadap pentingnya keamanan informasi, serta belum adanya evaluasi risiko yang dilakukan secara berkelanjutan.

Puskesmas Gandapura di Kabupaten Bireuen merupakan salah satu fasilitas layanan kesehatan yang telah mengadopsi sistem informasi digital. Meskipun demikian, hingga saat ini belum tersedia mekanisme terdokumentasi secara sistematis yang digunakan untuk mengidentifikasi, menganalisis, dan mengevaluasi risiko keamanan informasi yang mungkin terjadi. Kondisi ini menyebabkan terbukanya potensi ancaman terhadap kerahasiaan, integritas, dan ketersediaan data kesehatan masyarakat. Risiko tersebut dapat bersumber dari faktor internal seperti kesalahan pengguna (*human error*) maupun faktor eksternal seperti serangan *malware*, *phishing*, serta akses tidak sah [5].

Salah satu pendekatan yang dapat digunakan untuk mengelola ancaman terhadap keamanan data secara sistematis adalah dengan menerapkan kerangka kerja ISO/IEC 27005:2019. Standar ini merupakan bagian dari seri ISO 27000 yang secara khusus berfokus pada proses manajemen risiko keamanan informasi. ISO 27005 dirancang untuk mendukung implementasi ISO/IEC 27001 dan memungkinkan organisasi merancang strategi pengamanan yang sesuai dengan kebutuhan serta konteksnya masing-masing. Serta menyediakan panduan lengkap dalam mengidentifikasi, menilai, dan menangani risiko-risiko yang mengancam aset informasi organisasi, termasuk data pasien di layanan kesehatan [6].

Studi terbaru oleh Bahaji [7], sistem informasi pelayanan kesehatan di Indonesia menghadapi berbagai tantangan serius dalam aspek keamanan data. Penelitian tersebut mengungkap bahwa kelemahan dalam keamanan informasi tidak hanya berdampak pada hilangnya kepercayaan publik, tetapi juga mengancam keberlangsungan pelayanan kesehatan itu sendiri. Risiko utama yang teridentifikasi mencakup kelalaian staf dalam penggunaan sistem, kurangnya pelatihan terkait keamanan informasi, serta meningkatnya serangan *siber* seperti *malware* dan ransomware yang menargetkan institusi kesehatan. Selain itu, tidak adanya kebijakan keamanan yang komprehensif dan terbatasnya anggaran untuk perlindungan sistem menjadi faktor yang memperbesar kerentanan terhadap insiden keamanan.

Studi ini juga menekankan bahwa banyak Puskesmas dan rumah sakit di Indonesia belum menerapkan standar keamanan informasi internasional secara menyeluruh, seperti ISO/IEC 27001 atau ISO/IEC 27005, sehingga proses identifikasi dan mitigasi risiko belum berjalan secara sistematis. Hal ini selaras dengan kondisi yang terjadi di Puskesmas Gandapura, yang telah mengadopsi sistem digital namun belum memiliki mekanisme formal dalam mengelola risiko keamanan informasi.

Penelitian terdahulu oleh Putri dan Kurniawan [8] menunjukkan bahwa penerapan ISO 27005 mampu membantu institusi layanan kesehatan dalam menyusun peta risiko yang komprehensif, menetapkan prioritas mitigasi risiko, serta meningkatkan efektivitas kontrol keamanan informasi. Berdasarkan permasalahan di atas maka peneliti tertarik untuk melakukan suatu penelitian dengan judul: **“Analisis Risiko Keamanan Informasi Pada Aplikasi Sistem Puskesmas Gandapura”** dengan menggunakan kerangka kerja ISO/IEC 27005:2019. Diharapkan hasil penelitian ini dapat menjadi dasar dalam pengambilan keputusan strategis untuk memperkuat sistem keamanan informasi di lingkungan Puskesmas.

## **1.2 Rumusan Masalah**

Berdasarkan latar belakang masalah yang telah diuraikan, penulis membuat masalah berikut:

1. Bagaimana hasil analisis risiko ancaman keamanan informasi di Puskesmas Gandapura menggunakan framework ISO/IEC 27005?
2. Apa saja rekomendasi untuk penanganan risiko keamanan informasi Puskesmas Gandapura menggunakan framework ISO/IEC 27005?

## **1.3 Batasan Masalah**

Untuk mempermudah penelitian, pembatasan masalah sangat penting. Batasan-batasan permasalahan diberikan agar sistem website yang akan dibangun memiliki tujuan yang jelas. Akibatnya, penulis membatasi batasan masalah menjadi berikut:

Penelitian ini berfokus pada analisis risiko keamanan informasi di Puskesmas Gandapura.

1. Standar yang akan digunakan yaitu ISO/IEC 27005.

#### **1.4 Tujuan Penelitian**

Berdasarkan rumusan masalah yang sudah dibuat, maka tujuan dari penelitian ini adalah sebagai berikut:

1. Untuk mengetahui bagaimana tingkat keamanan informasi pada sistem yang ada di Puskesmas Gandapura.
2. Dapat memberikan solusi untuk mencegah ancaman keamanan informasi pada sistem yang ada di Puskesmas Gandapura.

#### **1.5 Manfaat Penelitian**

Penelitian ini diharapkan dapat memberikan manfaat secara umum, baik dari segi pengembangan ilmu pengetahuan maupun penerapannya dalam praktik. Secara teoritis, penelitian ini dapat memberikan kontribusi pemikiran dalam pengembangan ilmu di bidang sistem informasi, khususnya yang berkaitan dengan analisis risiko keamanan informasi. Secara praktis, hasil penelitian ini diharapkan dapat menjadi referensi bagi pihak-pihak yang membutuhkan, memperluas wawasan pengetahuan, serta menjadi acuan bagi penelitian selanjutnya yang berkaitan dengan topik serupa.