**EVALUASI PENERAPAN KEAMANAN INFORMASI PADA SIMRS RUMAH SAKIT XYZ BERDASARKAN STANDAR ISO/IEC 27001:2022 DENGAN MATURITY MODEL**

# ABSTRAK

Sistem Informasi Manajemen Rumah Sakit (SIMRS) mendukung pelayanan kesehatan dan pengelolaan data pasien sehingga memerlukan pengamanan untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi. Penelitian ini bertujuan mengidentifikasi kondisi aktual dan tingkat kematangan keamanan informasi pada SIMRS Rumah Sakit XYZ, menganalisis kesenjangan terhadap target, serta menyusun rekomendasi perbaikan berdasarkan ISO/IEC 27001:2022. Penelitian menggunakan metode deskriptif evaluatif dengan pengumpulan data melalui wawancara terstruktur, studi dokumentasi, dan observasi. Evaluasi dilakukan terhadap 53 kontrol terpilih Annex A menggunakan skala *maturity level* yang diadaptasi dari Indeks KAMI dan prinsip evaluasi ISO/IEC 27004:2016. Hasil penelitian menunjukkan nilai aktual 159 dari nilai maksimum 265 dengan rata-rata 3,00, sehingga penerapan keamanan informasi berada pada Level 3 atau Terdefinisi dan Konsisten. Target Level 4 ditetapkan sebesar 212 dengan total *gap* 53. Penelitian menghasilkan rekomendasi berdasarkan area prioritas dan lima rancangan SOP, yaitu pengelolaan kerentanan dan pembaruan keamanan, ** pembaruan keamanan, evaluasi kepatuhan dan kesadaran pengguna, pencatatan, penutupan, dan evaluasi insiden, pengujian pemulihan data dan layanan, serta pengelolaan akses dan kerahasiaan pihak ketiga.

Kata Kunci: Keamanan Informasi, ISO/IEC 27001:2022, SIMRS, *Maturity Model*, *Gap Analysis*

**Evaluation of Information Security Implementation in the Hospital Management Information System (HMIS) of XYZ Hospital Based on ISO/IEC 27001:2022 Using a Maturity Model**

## ABSTRACT

The Hospital Management Information System (SIMRS) supports healthcare services and patient data management, requiring security measures to maintain the confidentiality, integrity, and availability of information. This study aims to identify the current condition and maturity level of information security in the SIMRS at XYZ Hospital, analyse the gap against the target, and develop improvement recommendations based on ISO/IEC 27001:2022. A descriptive evaluative method was used, with data collected through structured interviews, document reviews, and observations. The evaluation covered 53 selected Annex A controls using a maturity-level scale adapted from the Indonesian Information Security Index (*Indeks KAMI*) and the evaluation principles of ISO/IEC 27004:2016. The results showed an actual score of 159 out of a maximum of 265, with an average score of 3.00, placing information security implementation at Level 3 (Defined and Consistent). The Level 4 target score was set at 212, resulting in a total gap of 53. The study proposes priority-based recommendations and five SOP drafts covering vulnerability and security update management, user compliance and security awareness evaluation, incident recording, closure, and evaluation, data and service recovery testing, and third-party access and confidentiality management.

Keywords: Information Security, ISO/IEC 27001:2022, Hospital Management Information System (SIMRS), Maturity Model, Gap Analysis