

ABSTRAK

Keamanan informasi pada instansi pemerintah merupakan aspek krusial dalam menjaga keberlangsungan operasional dan perlindungan data publik yang dikelola. Faktor manusia (*people*) menjadi salah satu tantangan terbesar dalam penerapan sistem manajemen keamanan informasi, khususnya terkait rendahnya kesadaran keamanan siber, penggunaan aplikasi tidak resmi, serta praktik berbagi akun dan kata sandi. Penelitian ini bertujuan untuk mengevaluasi penerapan Sistem Manajemen Keamanan Informasi (SMKI) pada kontrol keamanan aspek *people* (kontrol 6.1-6.8 ISO/IEC 27002:2022) serta kontribusinya terhadap perlindungan data pada aspek Confidentiality, Integrity, dan Availability (CIA) di Dinas Komunikasi Informatika dan Persandian Kota Yogyakarta (Dinkominfo).

Metode yang digunakan dalam penelitian ini melibatkan pendekatan deskriptif kualitatif dengan kerangka siklus *Plan-Do-Check-Act* (PDCA). Pengumpulan data dilakukan melalui wawancara terstruktur dengan enam narasumber dari bidang Persandian, Telekomunikasi, dan Kepegawaian, serta kuesioner berbasis bukti dokumen dan studi dokumentasi. Penilaian dilakukan dengan memetakan kondisi aktual terhadap kontrol dan panduan praktik terbaik yang tercantum dalam ISO/IEC 27001:2022 dan ISO/IEC 27002:2022, khususnya pada delapan kontrol aspek *people* dalam pengelolaan keamanan informasi.

Hasil penelitian ini menunjukkan bahwa enam dari delapan kontrol aspek *people screening* (6.1) syarat dan ketentuan kerja (6.2), kesadaran dan pelatihan (6.3), tanggung jawab setelah berakhir (6.5), perjanjian kerahasiaan (6.6), dan kerja jarak jauh (6.7) telah diterapkan sepenuhnya dengan tingkat kepatuhan 100%. Kontrol 6.8 (pelaporan kejadian keamanan informasi) mencapai 87,5%, sementara kontrol 6.4 (proses disipliner) mencapai 62,5%. Kesenjangan utama ditemukan pada belum tersedianya rincian jenis pelanggaran dan sanksi dalam prosedur disipliner, serta belum adanya kebijakan perlindungan bagi pelapor (*whistleblower protection*). Rekomendasi perbaikan disusun berdasarkan kesenjangan antara kondisi aktual dan standar ISO/IEC 27001:2022 dan ISO/IEC 27002, sehingga diharapkan dapat mendukung peningkatan efektivitas penerapan SMKI pada aspek *people* di masa mendatang.

Kata Kunci: Sistem Manajemen Keamanan Informasi, Perlindungan Data, ISO/IEC 27001:2022, ISO/IEC 27002:2022, Kontrol *People*, CIA *Triad*, Dinas Komunikasi Informatika dan Persandian.

ABSTRACT

Information security in government agencies is a crucial aspect in maintaining operational continuity and protecting public data under management. The human factor (people) remains one of the greatest challenges in implementing an information security management system, particularly regarding low cybersecurity awareness, the use of unauthorized applications, and the practice of sharing accounts and passwords. This study aims to evaluate the implementation of the Information Security Management System (ISMS) on people security controls (Controls 6.1–6.8 of ISO/IEC 27002:2022) and their contribution to data protection in terms of Confidentiality, Integrity, and Availability (CIA) at the Department of Communication, Informatics, and Cryptography of Yogyakarta City (Dinkominfosan).

The method employed in this study involves a qualitative descriptive approach using the Plan-Do-Check-Act (PDCA) cycle as an evaluation framework. Data were collected through structured interviews with six informants from the Cryptography, Telecommunication, and Personnel divisions, as well as evidence-based questionnaires and documentation analysis. Assessment was conducted by mapping the actual conditions against the controls and best practice guidelines contained in ISO/IEC 27001:2022 and ISO/IEC 27002:2022, specifically on the eight people controls within the information security management domain.

The results indicate that six out of eight people controls — screening (6.1), terms and conditions of employment (6.2), awareness and training (6.3), responsibilities after termination (6.5), non-disclosure agreements (6.6), and remote working (6.7) — achieved full compliance at 100%. Control 6.8 (information security event reporting) reached 87.5%, while control 6.4 (disciplinary process) reached 62.5%. Key gaps were identified in the absence of a detailed disciplinary violation catalog with corresponding sanctions, as well as the lack of a whistleblower protection policy. Improvement recommendations were formulated based on the gaps between current conditions and the ISO/IEC 27001:2022 and ISO/IEC 27002:2022 standards, with the expectation of supporting the enhancement of ISMS effectiveness on the people aspect in the future.

Keywords : Information Security Management System, Data Protection, ISO/IEC 27001:2022, ISO/IEC 27002:2022, People Control, CIA Triad, Department of Communication Informatics and Cryptography