ABSTRAK

Keamanan siber menjadi isu krusial di era digital, terutama bagi Indonesia yang menghadapi berbagai ancaman siber seperti *ransomware* dan *trojan*. Penelitian ini bertujuan mengidentifikasi parameter kunci untuk mengukur tingkat kematangan keamanan siber organisasi dengan menggunakan *Best-Worst Method* (BWM) sebagai metode evaluasi. Pendekatan ini mengintegrasikan berbagai *framework* seperti COBIT 2019, NIST *Cybersecurity Framework* (CSF), MITRE ATT&CK, dan lainnya, untuk menciptakan alat penilaian kesiapan keamanan siber yang menyeluruh. *Framework* yang dikembangkan dalam penelitian ini mencakup empat aspek utama, yaitu *Data security*, *Application and endpoint security*, *Network and perimeter security*, serta *Human layer*. Melalui evaluasi berbasis BWM, *framework* ini memberikan panduan strategis untuk meningkatkan kesiapan keamanan siber organisasi. Hal ini menunjukkan *framework* yang diusulkan mampu memberikan panduan strategis dalam meningkatkan kesiapan keamanan siber organisasi. Hasil penelitian ini berkontribusi pada pengembangan langkah mitigasi proaktif dan peningkatan manajemen risiko keamanan siber di berbagai industri. Diharapkan *framework* kesiapan keamanan siber ini mampu menjadi pedoman bagi organisasi dalam mengidentifikasi celah keamanan, menentukan prioritas mitigasi, dan merancang strategi yang efektif untuk menghadapi ancaman siber. *Framework* ini juga diharapkan dapat diadaptasi secara fleksibel oleh berbagai sektor, termasuk pemerintahan, layanan kesehatan, pendidikan, dan industri keuangan, yang memiliki kebutuhan keamanan siber yang beragam.

Kata Kunci - *Keamanan Siber, Tingkat Kematangan, Best-Worst Method, Framework Terintegrasi*