ABSTRAK

Website risk management di PT XYZ menghadapi berbagai permasalahan yang dapat mempengaruhi keberlanjutan operasionalnya. Adanya kemungkinan yang dapat terjadi pada hasil penetrasi *website* yaitu serangan *DoS/DDoS, Phishing, Malware, Ransomware*, dan *SQL Injection*. Untuk mengatasi permasalahan tersebut, penelitian ini menggunakan kerangka kerja ISO 31000:2018 sebagai pedoman dalam proses manajemen risiko, yang menyediakan pendekatan sistematis untuk mengidentifikasi, menilai, dan mengelola risiko dengan tujuan meminimalkan dampak negatif. Hasil dari penerapan kerangka kerja ini menunjukkan solusi komprehensif, seperti implementasi *Web Application Firewall (WAF)* untuk melindungi dari serangan *DoS/DDoS* dan *SQL Injection*, penerapan *antivirus* dan *anti-malware* untuk mencegah infeksi *malware*, serta *backup* data rutin dan pengecekan keamanan siber secara berkala untuk mengurangi risiko *ransomware* dan ancaman keamanan siber lainnya. Dari hasil analisis memberikan solusi bagi PT XYZ, karena memungkinkan perusahaan untuk lebih memahami berbagai kemungkinan risiko dan menetapkan tindakan penanganan yang tepat, sehingga meningkatkan ketahanan operasional *website* perusahaan serta mengurangi potensi kerugian yang mungkin timbul akibat risiko-risiko tersebut. Implementasi kerangka kerja ISO 31000:2018 diharapkan dapat memberikan manfaat jangka panjang bagi perusahaan dalam menjaga integritas, keamanan, dan ketersediaan sistem informasi yang digunakan.

Kata kunci : *Cybercrime*, ISO 31000:2018, Manajemen Risiko, Penetrasi, *Website*.