

ABSTRAK

Security Operation Center (SOC) merupakan pusat pengendalian keamanan yang berfokus pada pengawasan atau monitoring, pendeteksian, analisis, serta respon cepat terhadap ancaman keamanan siber. SOC bertujuan untuk melindungi organisasi dari serangan siber yang dapat merugikan aset, reputasi, dan bisnis. SOC telah diterapkan pada PT *Non-Bank Financial Company (NBFC)* untuk keamanan sistem informasinya. Akan tetapi, pada PT NBFC masih memiliki permasalahan yaitu belum memiliki proses analisis dampak terhadap *Financial* dan *Regulatory Requirement* serta perhitungan biaya dan usaha yang diperlukan untuk pemulihan (*recovery*) pada *event/insiden* yang terdeteksi, belum ada *Key Performance Indicators (KPI)* dan *Key Risk Indicators (KRI)* yang ditetapkan oleh manajemen untuk memantau efektivitas kontrol akses fisik dan kesesuaian dengan standar yang berlaku, belum memiliki program resmi terkait insider threat (ancaman dari dalam organisasi). Oleh karena itu, penelitian ini mengevaluasi efektivitas SOC dalam mengatasi ancaman keamanan informasi pada PT *Non-Bank Financial Company (NBFC)* menggunakan *framework* ISO 27005:2018 dan NIST SP 800-30. Hasil penelitian yaitu *guidance framework* usulan untuk *assessment* SOC kombinasi dari *framework* ISO 27005:2018 dan NIST SP 800-30 yang terdiri dari beberapa tahap *research assessment, risk assessment, risk treatment and risk acceptance strategy* dan *monitoring*. Selain itu, penelitian ini menghasilkan penilaian *maturity level* dari *framework* ISO 27005:2018, NIST SP 800-30 dan *framework* usulan. Dari penilaian *maturity level* bahwa pada *framework* usulan mencapai *maturity* yang baik karena terdapat 2 domain yang mencapai nilai *target maturity* dan 1 domain yang telah berada pada level 4 - *Managed and Measurable*. Dilihat dari segi domain yang digunakan pada *framework* baru mencakup domain dari ISO 27005:2018 dan NIST SP 800-30 sehingga organisasi dapat memanfaatkan pendekatan yang lebih menyeluruh, yang melibatkan aspek strategis, manajerial, dan teknis dari manajemen risiko.

Kata Kunci: *Cyber Security, Maturity level, Perusahaan Finansial Non-Bank, Security Operation Center (SOC), Sistem Informasi*