ABSTRAK

Industri perbankan adalah salah satu sektor vital bagi pertumbuhan ekonomi suatu negara. Hal tersebut menyebabkan sektor perbankan selalu rentan dengan risiko. Menilik dari triad keamanan informasi, setiap data dan informasi terkhusus dalam sektor perbankan harus dapat dijamin kerahasiaan, keaslian dan ketersediaannya. Bank Syariah memiliki departemen CISO (*Chief of Information Security Officer)* sebagai dept yang bertugas untuk melakukan pengamanan iklim digital Bank Syariah. Melihat masivnya praktik kejahatan siber tentu pemahaman yang baik akan risiko pada dept CISO akan berkontribusi dalam penguatan sistem manajemen keamanan informasi secara umum. Membuat organisasi jadi lebih siap dalam menghadapi, memitigasi dan mengambil keputusan kedepannya. Mempertimbangkan hal tersebut penelitian ini bertujuan untuk dapat mengimplementasikan framework atau standar ISO/IEC 27005:2018 dan melakukan penilaian risiko menggunakan metode FMEA *(Failure Modes and Effect Analysis)* di departmen CISO. Hasil dari penelitian berupa tinjauan dari segi risiko pada departemen CISO bank syariah dan dokumen mitigasi untuk setiap ancaman dan aset. Ditemukan sekitar 45 risiko yang ada pada departemen CISO pada Bank Syariah. Risiko tersebut dapat dikategorisasikan menjadi kelas *Very High, High, Medium, Low* dan *Very Low* sesuai nilai RPN. Pada kasus ini tidak ditemukan risiko *very high* maupun *high,* hanya satu risiko *medium,* 28 risiko *Low* dan enam belas risiko *Very Low.* Bank Syariah sudah memiliki proteksi keamanan yang baik dan holistik.

Kata Kunci: **Risiko, Manajemen Risiko, aset, ancaman, ISO/IEC 27005:2018**