

ABSTRAK

Pada proses manajemen keamanan sistem informasi terdapat beberapa masalah yang muncul seperti permasalahan lemahnya strategi dalamantisipasi ancaman gangguan dan serangan terhadap data informasi pada suatu perusahaan, yang membuat banyaknya risiko IT terjadi. Dalam penyusunan sistem manajemen keamanan informasi seharusnya didasari oleh hasil analisis dan mitigasi risiko, agar strategi keamanan yang diusulkan dapat secara efektif menurunkan risiko yang telah diidentifikasi. Dalam penelitian kali ini dilakukan pengumpulan data dengan metode wawancara, observasi dan survei. Setelah data terkumpul maka dilakukan penilaian kematangan sistem manajemen keamanan informasi menggunakan indeks KAMI untuk mendapatkan hasil *maturity level*-nya, dan melakukan penilaian risiko dengan metode FMEA (*Failure Modes and Effect Analysis*). Dari hasil yang didapatkan dari penilaian *maturity level* pada PT. XYZ yaitu rata-rata *maturity level* nya satu (*Initial Process*) dan penilaian risiko menggunakan metode FMEA dengan hasil empat risiko dengan nilai “*very high*” maka dilakukan mitigasi risiko dengan menggunakan standar ISO 27002:2022 dengan dilakukan kepada risiko yang memiliki nilai RPN *Medium* s.d. *Very High* dan Tata kelola dari *maturity level* yang diharapkan dapat membantu PT.XYZ meningkatkan dan melakukan perbaikan pada sistem manajemen keamanan informasinya.

Kata Kunci : sistem manajemen keamanan informasi, risiko IT, ISO 27002:2022, FMEA, *maturity level*, indeks KAMI.