BAB V
PENUTUP

5.1 Kesimpulan

Kesimpulan yang dapat diambil setelah menyelesaikan penelitian adalah kesadaran keamanan informasi pada *Customer Services* masih **rendah**. Dengan memperhatikan nilai ***Risk Priority Number (RPN)***, hasil analisa mengenai kontrol SDM oleh perusahaan terhadap kesadaran keamanan informasi pada pegawai menunjukkan nilai 480 dengan nilai critical ***Very High***, sementara penilaian mengenai Standar Operasional Prosedur (SOP) menunjukkan nilai RPN 120 dan nilai critical ***High***, SOP yang belum terdokumentasi dan belum diterapkan akan sangat membahayakan bagi perusahaan. Sementara penialaian aset yang terfokus pada 5 aset utama menunjukkan hasil *critical* ***high*** masih banyak. Dengan hasil analisa menggunakan metode FMEA ini, dapat diketahui celah keamanan yang masih rendah dan rentan terhadap serangan, analisa ini dapat membantu perusahaan dalam upaya meningkatkan kualitas kemanan informasi perusahaan.

Peneliti menggunakan metode FMEA karena dapat digunakan sebagai *tools* analisis yang bersifat preventif dalam mengidentifikasi potensi kegagalan. FMEA adalah pendekatan yang bertujuan untuk mengevaluasi dan memprioritaskan risiko dalam suatu potensi kegagalan. Sementara penggunaan *Framework* ISO/IEC 27001:2013 digunakan sebagai patokan atau standar yang menjadi acuan setiap nilai kerentanan yang dinilai. Beberapa pertanyaan yang diberikan saat penelitian merupakan hasil kutipan dari pertanyaan yang digunakan pada Indeks KAMI, setiap pertanyaan yang dikutip di sesuaikan dengan kondisi yang ada. Penentuan nilai RPN dilakukan dari hasil wawancara, kuesioner, dan observasi.

5.2 Saran

Penelitian ini masih terbatas pada security awareness customer secara umum dan dilakukan di masa pandemi covid-19, pertanyaan yang di ajukan masih mengutip dari ISO/IEC 27001:2013 pada indeks KAMI, akan lebih maksimal apabila pertanyaan yang di ajukan adalah pertanyaan yang terfokus pada

pengetahuan keamanan informasi yang di ambil dari beberapa standar keamanan lain, seperti TOGAF (The Open Group Architecture Framework), NIST (National Institute of Standards and Technology)

Penelitian selanjutnya dapat melakukan analisa kesadaran keamanan informasi pada masa *New-Normal*, serta penelitian yang dilakukan akan lebih efektif apabila dilakukan analisa dari beberapa *framework* yang telah disebutkan, Dengan demikian maka kekuatan penelitian dan nilai yang didapatkan akan lebih akurat serta dapat menjadi landasan baru bagi penilaian kesadaran keamanan informasi untuk alat audit perusahaan.