ABSTRAK

Transformasi digital mendorong Institusi Keuangan Syariah mengadopsi layanan berbasis *website* untuk efisiensi dan perluasan layanan. Namun, kesiapan keamanan informasi masih terbatas, membuat IKS rentan terhadap serangan siber yang memanfaatkan celah pada sistem publik. Penelitian ini mengadopsi pendekatan *Open-Source Intelligence* (OSINT) untuk mengidentifikasi kerentanan, mendeteksi potensi ancaman eksternal, serta menghitung estimasi risiko siber terhadap aset IT IKS secara kuantitatif. Penelitian ini diawali dengan penentuan *domain* resmi IKS yang ditentukan melalui data sekunder daftar peringkat lembaga keuangan, kemudian dilanjutkan dengan eksplorasi menggunakan berbagai OSINT *tools* untuk mengumpulkan informasi teknis. Data yang diperoleh dianalisis menggunakan model kuantitatif dari ISACA untuk mengukur tingkat estimasi risiko berdasarkan kerentanan (*vulnerability*), potensi ancaman (*threat*), dan nilai aset digital (*asset*). Rentang skor 48 – 101 menunjukkan kategori risiko rendah, skor 102 – 155 kategori risiko sedang, sedangkan skor 156 – 210 termasuk kategori risiko tinggi. Hasilnya menunjukkan bahwa Institusi Keuangan Syariah B urutan pertama memiliki nilai risiko sebesar 210 yang dikategorikan sebagai risiko tertinggi, diikuti oleh Institusi Keuangan Syariah F dengan skor 112 mewakili kategori risiko sedang, serta Institusi Keuangan Syariah D dengan skor 75 mewakili kategori risiko terendah. Temuan ini menunjukkan bahwa besarnya nilai aset IT tidak selalu berbanding lurus dengan tingginya tingkat risiko, melainkan sangat dipengaruhi oleh kesadaran dan upaya dalam mengamankan informasi yang diterapkan oleh masing-masing institusi.

Kata kunci—***Open-Source Intelligence*** **(OSINT),** ***asset*** **IT, Institusi Keuangan Syariah, keamanan informasi, estimasi risiko**