## *ABSTRACT*

*Digital transformation has driven Shariah Financial Institutions to adopt web-based services for greater efficiency and service expansion. However, their information security readiness remains limited, making SFI vulnerable to cyberattacks that exploit weaknesses in public-facing systems. This study adopts an Open-Source Intelligence (OSINT) approach to identify vulnerabilities, detect potential external threats, and quantitatively estimate cyber risks to the IT assets of SFI. The research begins by determining the official domains of SFI based on secondary data from financial institution rankings, followed by exploration using various OSINT tools to collect technical information. The collected data is analyzed using a quantitative risk estimation model from ISACA, assessing risk levels based on vulnerability, threat potential, and digital asset value. A score range of 48–101 indicates low risk, 102–155 indicates medium risk, and 156–210 indicates high risk. The results show that Shariah Financial Institutions B ranks first with a risk score of 210, categorized as high risk followed by Shariah Financial Institutions F with a score of 112 in the medium-risk category and Shariah Financial Institutions D with a score of 75 in the low-risk category. These findings demonstrate that the value of IT assets does not always correlate with the level of risk, as it is significantly influenced by each institution's awareness and efforts to secure their information systems.*



*Keywords—* ***Open-Source Intelligence (OSINT), IT assets, Shariah Financial Institutions, information security, estimated risk***