

ABSTRAK

Transformasi digital dalam industri perbankan telah mendorong peningkatan adopsi teknologi informasi, namun di sisi lain juga memperbesar risiko terhadap keamanan informasi dan privasi. Untuk menjawab tantangan tersebut, penelitian ini bertujuan memetakan regulasi-regulasi Otoritas Jasa Keuangan (OJK) yang relevan, seperti POJK No. 11/POJK.03/2022 dan SEOJK No. 29/SEOJK.03/2022, terhadap tahapan-tahapan dalam NIST Risk Management Framework (RMF). Pendekatan yang digunakan adalah kualitatif deskriptif dengan metode studi literatur dan analisis konten, dilengkapi dengan validasi melalui peer-review dan diskusi kelompok terarah (FGD) bersama praktisi industri. Hasil penelitian menunjukkan adanya kesesuaian substansial antara regulasi nasional dengan prinsip-prinsip NIST RMF, serta menghasilkan framework manajemen risiko keamanan informasi dan privasi yang dapat diimplementasikan secara menyeluruh di sektor perbankan digital Indonesia. Framework ini diharapkan mampu menjadi pedoman strategis bagi institusi perbankan dalam meningkatkan kepatuhan, efektivitas pengelolaan risiko, dan ketahanan siber secara berkelanjutan.

Kata kunci: keamanan informasi, manajemen risiko, NIST RMF, perbankan digital, regulasi OJK, privasi data

ABSTRACT (ENGLISH)

The digital transformation within the banking industry has driven widespread adoption of information technology, while simultaneously increasing risks to information security and privacy. To address these challenges, this study aims to map relevant regulations issued by Indonesia's Financial Services Authority (OJK), such as POJK No. 11/POJK.03/2022 and SEOJK No. 29/SEOJK.03/2022, to the phases of the NIST Risk Management Framework (RMF). This research adopts a qualitative descriptive approach using literature review and content analysis methods, complemented by validation through expert peer review and focus group discussions (FGD) with industry practitioners. The findings reveal a substantial alignment between national regulations and the principles of the NIST RMF, resulting in the development of an integrated information security and privacy risk management framework suitable for implementation across the Indonesian digital banking sector. The proposed framework is expected to serve as a strategic guideline for banking institutions to enhance compliance, risk governance, and cybersecurity resilience in a sustainable manner.

Keywords: information security, risk management, NIST RMF, digital banking, OJK regulation, data privacy.