# ABSTRACT

Government agencies in Indonesia are increasingly vulnerable to sophisticated cyber threats such as phishing, ransomware, distributed denial-of-service (DDoS) attacks, and advanced persistent threats (APTs). These attacks exploit institutional limitations, including fragmented governance, lack of technical capabilities, and reliance on legacy infrastructure. Existing Security Operations Center (SOC) models, which are often complex and vendor-centric, are misaligned with the structural and resource realities of the Indonesian public sector. This study proposes a modular, tier-based SOC model designed to address the cybersecurity needs of Indonesian government institutions. The model is intended to be scalable, context-sensitive, and adaptable to varying levels of institutional maturity. Employing the Design Science Research (DSR) methodology, the study follows six structured stages: problem explication, requirements definition through a systematic literature review (SLR), initial model design (SOC v0.1), expert validation and refinement (SOC v0.2), demonstration in a real-world local government setting, and structured evaluation. The model is guided by international frameworks such as the NIST Cybersecurity Framework (CSF) and MITRE ATT&CK. The resulting SOC Model v1.0 comprises capability-based tiers (Tier 1, 2, and 3) and seven foundational components: People, Process, Technology, Governance, Collaboration, Metrics, and Innovation. Feedback from expert reviews and practical demonstration confirmed the model's relevance, feasibility, and scalability within the Indonesian government context. Theoretically, this study advances public-sector SOC design by integrating international standards into a context-aware framework. Practically, it delivers a validated and deployable SOC model tailored to the operational constraints of developing country governments, offering a proportional alternative to generic and proprietary SOC architectures.

**Keywords:** Cybersecurity, Government, Security Operations Center, Modular SOC, Tier-Based SOC Model