LIST OF TERMS

Security Operations Center(SOC)	A centralized function that monitors, detects, and responds to cybersecurity incidents within an organization. In this thesis, it refers to a model tailored for government institutions.
Tier-Based SOC	A stratified approach to SOC capability, where institutions implement functions based on their operational maturity—commonly classified into Tier 1 (basic), Tier 2 (coordinative), and Tier 3 (strategic).
Systematic Literature Review (SLR)	A methodical process for identifying, evaluating, and synthesizing relevant research to answer specific research questions.
Threat Intelligence (TI)	Information that provides insight into existing or emerging cyber threats. Can be passive (consumption only) or active (production and sharing).
Security Information and Event Management (SIEM)	A technology that aggregates log data, detects anomalies, and supports alerting and forensic investigation. Included in the broader category of Security Monitoring.
Computer Security Incident Response Team (CSIRT)	A team responsible for handling cybersecurity incidents in an organization or sector. In Indonesia, often coordinated by BSSN.
Distributed Denial of Service (DDoS)	A cyberattack aimed at overwhelming a service or system with traffic, rendering it inaccessible. One of the dominant threat profiles addressed in this study.
MITRE ATT&CK	A globally recognized knowledge base of adversary tactics and techniques used to support threat modeling and SOC function alignment.
NIST CSF	National Institute of Standards and Technology Cybersecurity Framework, which categorizes cybersecurity functions into Identify, Protect, Detect, Respond, and Recover.
Digital Forensics	The process of identifying, preserving, analyzing, and presenting digital evidence from cybersecurity incidents. Included as a SOC module.
Incident Response	The structured handling of cybersecurity incidents to contain, mitigate, and recover from attacks. One of the primary modules in SOC design.
Governance & Compliance	Refers to institutional mechanisms ensuring security policy, asset identification, audit, and adherence to regulations. Included across all SOC tiers.

Escalation	A process for transferring incident handling or threat analysis to a higher capability level (e.g., from Tier 1 to Tier 2) based on severity or resource requirements.
Modular Design	A system architecture where SOC functions are divided into distinct, reusable components that can be implemented independently or incrementally.
Demonstration	A simulation or implementation used to evaluate how the SOC model performs under specific threat scenarios in a real-world government setting.
Evaluation	A structured process in which institutional representatives assess the SOC model's feasibility, relevance, and applicability using scoring instruments and qualitative judgment.
Metrics	Indicators or performance measures used to monitor and improve SOC operations and institutional readiness. Introduced as a refinement element in the model.
Innovation and Research	A newly added element to the SOC model, aimed at ensuring adaptability through continuous improvement, experimentation, and policy-tech alignment.
Innovation and Research	A newly added element to the SOC model, aimed at ensuring adaptability through continuous improvement, experimentation, and policy-tech alignment.
SOC-CMM (Security Operations Center – Capability Maturity Model)	A widely adopted maturity model designed to assess and improve the capabilities of SOCs across multiple domains, including people, process, technology, and business functions. It serves as a high-level diagnostic tool for organizational SOC posture.
C2M2 (Cybersecurity Capability Maturity Model)	A framework developed to evaluate and enhance an organization's cybersecurity capabilities, originally tailored for the energy sector but extensible to other domains. It focuses on risk management, situational awareness, and institutional resilience.