CHAPTER 1

INTRODUCTION

This chapter presents the foundational component of the study. It introduces the research motivation, formulates the problem, defines the study's scope and approach, and outlines its ethical and scholarly contributions. These components are structured to establish the context, direction, and significance of developing a Security Operations Center (SOC) model tailored to Indonesian government agencies.

1.1 Motivation

The urgency for state cyber-defence has been underscored by Nugraha et al. (2016), who used an adaptive wideband Delphi method to identify Indonesia's cybersecurity requirements in response to foreign surveillance threats. Their findings emphasize that effective protection requires not only technical measures but also strong governance and legal frameworks. These insights reinforce this study's motivation to design a context-aware SOC model that addresses both technological and institutional challenges in the public sector [1].

In recent years, government agencies have become frequent targets of sophisticated cyberattacks, including phishing, ransomware, malware, and denial of service (DoS). These attacks have led to data breaches, operational disruption, financial loss, and a decline in public trust. Moreover, such threats have strategic implications, as they may compromise national security and resilience, particularly in the context of growing geopolitical tensions and cyber warfare capabilities [2–4].

However, existing SOC models are often designed for private enterprises and may not align well with the structural, resource, and governance constraints typical of public-sector agencies. Literature also indicates that SOC implementation can fail when there is a misalignment between the SOC model and organizational readiness [5, 6]. Additionally, international guidelines on SOC development remain fragmented, and scholarly research in this area still tends to rely on generalized best practices or vendor-based frameworks [7, 8].

Accordingly, this study addresses the absence of a proportionate and context-sensitive SOC framework tailored to the structural and operational realities of Indonesian government agencies. It aims to explore what specific cyber threat profiles affect public agencies, what core components are necessary to design an effective SOC, and how such a model can be developed to accommodate the varied capabilities, constraints, and priorities of different levels of government in Indonesia.

1.2 Research Problem

Cybersecurity has become a critical national concern, particularly for the government sector in Indonesia, which consistently records the highest number of cyber incidents compared to other sectors. According to the National Cyber and Crypto Agency (BSSN), the government sector was the most targeted domain in both 2023 and 2024, accounting for the largest proportion of anomalies and cyber threats detected at the national level [9, 10]. This persistent exposure underscores the vulnerability of public institutions and the strategic importance of strengthening cyber resilience across government entities.

While Security Operations Centers (SOCs) are widely recognized as essential infrastructures for centralized threat detection, monitoring, and response [5, 11], most existing SOC models are designed for enterprise or defense settings. These models typically assume high resource availability, advanced technical capabilities, and mature governance structures. However, these assumptions are often misaligned with the conditions faced by many Indonesian government agencies, which struggle with limited cybersecurity expertise, fragmented coordination, and budgetary constraints [7, 12, 13].

In addition, although the literature offers various SOC components and frameworks, there is no consolidated synthesis of critical component that can guide the design of context-appropriate SOC models. Furthermore, current SOC frameworks rarely provide modular and scalable structures that are adaptable to the diverse operational and institutional realities of decentralized government environments, particularly in developing countries [7, 14, 15].

To address these gaps, this research is guided by the following problem statements:

P1: Government agencies are increasingly targeted by diverse and sophisticated cyber threats; however, there is limited systematic understanding of which specific threat profiles most critically affect their cybersecurity posture.

P2: While existing literature introduces various SOC frameworks and components, it lacks an integrated synthesis of the critical elements necessary for the development of an effective and contextually relevant model.

P3: Currently, there is a lack of structured SOC models specifically tailored to the structural and operational realities of Indonesian government agencies.

1.3 Research Objectives

This study aims to address the cybersecurity challenges faced by Indonesian government agencies by developing a proportionate and context-sensitive Security Operations Center (SOC) model. The specific objectives of this research are as follows:

O1: To identify and analyze the cybersecurity threat profiles that most significantly affect

government agencies.

O2: To identify and synthesize the critical components required for the development of an effective Security Operations Center (SOC).

O3: To design and evaluate a modular and tier-based SOC model through a structured process that aligns with the structural and operational conditions of Indonesian government agencies.

1.4 Research Questions

To achieve the research objectives outlined above, this study is guided by the following research questions:

RQ1: What cybersecurity threat profiles most significantly affect government agencies?

RQ2: What are the critical components required to design an effective Security Operations Center (SOC)?

RQ3: How can the process of designing and evaluating a SOC model be structured to ensure its proportionality to the structural and operational conditions of Indonesian government agencies?

1.5 Research Scope

This study is focused on the conceptual development, validation, and demonstration of a modular and tiered Security Operations Center (SOC) model specifically tailored for Indonesian government agencies. The research emphasizes the design of an adaptable SOC framework that aligns with the varied operational capabilities, governance structures, and resource constraints commonly found in public-sector environments.

The scope of this study is limited to the context of Indonesian government institutions at both central and local levels, including ministries, national agencies, and regional governments. While international frameworks such as the NIST Cybersecurity Framework (CSF) and the MITRE ATT&CK framework serve as design references, the proposed model is contextually adapted to fit the cybersecurity maturity levels and institutional realities found in Indonesia.

Several of the initial insights used in the design process, particularly those related to cybersecurity threat profiles and critical SOC components, were derived from a systematic literature review (SLR) of global academic publications. This approach was adopted due to the limited availability of comprehensive national datasets and the international nature of cybersecurity threats in the public sector. To ensure contextual relevance, these findings were further interpreted through expert validation and scenario-based demonstration in the Indonesian government setting.

This research does not include the full-scale technical implementation, deployment, or integration of the SOC model across multiple agencies or live environments. Instead, the study focuses on the conceptual design, expert-based validation, and scenario-driven demonstration of the proposed model to assess its feasibility, scalability, and applicability within the public-sector cybersecurity governance landscape in Indonesia.

1.6 Research Approach

This study adopts the Design Science Research (DSR) methodology as its foundational research approach. DSR is well-suited for addressing complex, real-world problems by designing and evaluating purposeful artifacts. In this case, a Security Operations Center (SOC) model tailored for government agencies. While Johannesson and Perjons define a five-stage Design Science Research process, this study introduces expert validation as a distinct sixth stage to enhance model refinement before formal demonstration and evaluation [16].

This study adopts a modified six-stage process, with each stage contributing to the iterative design, validation, and evaluation of the proposed SOC model:

1. **Problem Explication:** Identifying the critical need for a proportionate and context-aware SOC framework in Indonesian government agencies, based on observed limitations and cybersecurity challenges.

2. **Requirement Definition:** Conducting a systematic literature review (SLR) to extract design component, threat profiles, and success factors from previous studies and international standards.

3. **Design:** Constructing an initial version of the SOC model (v0.1), incorporating modular components and tiered capabilities to reflect institutional diversity.

4. **Validation:** Engaging subject-matter experts from academia, government, and cybersecurity practice to evaluate the model's relevance, clarity, and feasibility.

5. **Demonstration:** Applying the model in a simulated environment involving local government stakeholders to assess usability and alignment with operational realities.

6. **Evaluation:** Analyzing feedback and observations to refine the model into its final version (v1.0), highlighting its strengths and identifying areas for future improvement.

The use of DSR is justified by the artifact-oriented and solution-driven nature of the research, which aims to contribute both to theoretical advancement and to practical governance tools for cybersecurity resilience in the public sector.

1.7 Ethical Considerations

This study adheres to the ethical standards required for academic research involving expert participation and institutional engagement. All individuals involved in the expert validation and demonstration phases, including multiple domain experts, were invited on a voluntary basis and provided with clear, informed consent regarding the purpose of the study, their roles, and the use of institutional attribution where applicable.

Some institutional affiliations of the experts were explicitly mentioned in the study to reflect the credibility and relevance of the validation process. These mentions were made with the knowledge and consent of the participants. No personally sensitive data or classified institutional information was collected, stored, or disclosed.

This research received ethical clearance in accordance with university guidelines. All secondary data, including academic literature, public frameworks, and threat models, were properly cited in accordance with standards of academic integrity.

1.8 Research Contributions

This study offers both theoretical and practical contributions to the field of cybersecurity governance in the public sector.

Theoretical Contributions: The research contributes to the academic discourse by developing a context-sensitive Security Operations Center (SOC) model that reflects the structural, institutional, and resource-based realities of Indonesian government agencies. It also extends the application of Design Science Research (DSR) methodology in cybersecurity studies, particularly within the domain of public-sector cyber resilience. The resulting model synthesizes threat landscape insights, governance constraints, and modular design principles into a unified artefact, contributing to the literature on adaptive cybersecurity frameworks.

Practical Contributions: On a practical level, this study provides a validated SOC model (v1.0) that incorporates modular components and tiered capability levels. The model enables government agencies to incrementally enhance their cybersecurity operations based on organizational maturity and resource availability. It also serves as a decision-support tool for policymakers and IT managers seeking to build or strengthen SOC functions in public environments. By aligning with international standards while remaining locally adaptable, the model offers a structured pathway for scalable SOC implementation across diverse government contexts.

1.9 Thesis Structure

This thesis is organized into six chapters, each contributing to the development and evaluation of a modular and tiered Security Operations Center (SOC) model tailored for In-

donesian government agencies using a Design Science Research (DSR) approach.

Chapter 1 – Introduction This chapter presents the background, motivation, research problem, scope, methodological approach, ethical considerations, and the contributions of the study. It establishes the rationale for developing a context-aware SOC model suited to the operational conditions of public-sector agencies.

Chapter 2 – Literature Review This chapter explores existing literature on cybersecurity threats affecting government agencies, SOC frameworks and maturity models, international standards such as NIST CSF and MITRE ATT&CK, and prior studies in public-sector cybersecurity governance. It also identifies knowledge gaps that justify the development of a new model.

Chapter 3 – Methodology This chapter details the Design Science Research (DSR) methodology adopted in the study. It outlines each phase of the research process, including problem explication, requirement definition through a systematic literature review (SLR), model design, expert validation, demonstration, and final evaluation.

Chapter 4 – Results and Analysis This chapter presents the results from each DSR phase. It includes the initial SOC model design (v0.1), expert validation and model refinement (v0.2), outcomes from the demonstration scenario, and the final evaluation leading to the validated SOC Model (v1.0).

Chapter 5 – Discussion This chapter discusses the implications of the proposed SOC model in both theoretical and practical contexts. It highlights the model's scalability, relevance to different levels of government, and alignment with established cybersecurity frameworks.

Chapter 6 – Conclusion The final chapter summarizes the key findings and contributions of the research. It reflects on the study's limitations and offers recommendations for future research, including potential enhancements to the SOC model, broader validation, and implementation strategies across sectors or regions.

The overall structure of this thesis, including the relationship between research questions and key contributions, is illustrated in Figure 1.1. This diagram highlights how each chapter builds upon the previous one to support the design, validation, and implementation of the proposed SOC model for government institutions.

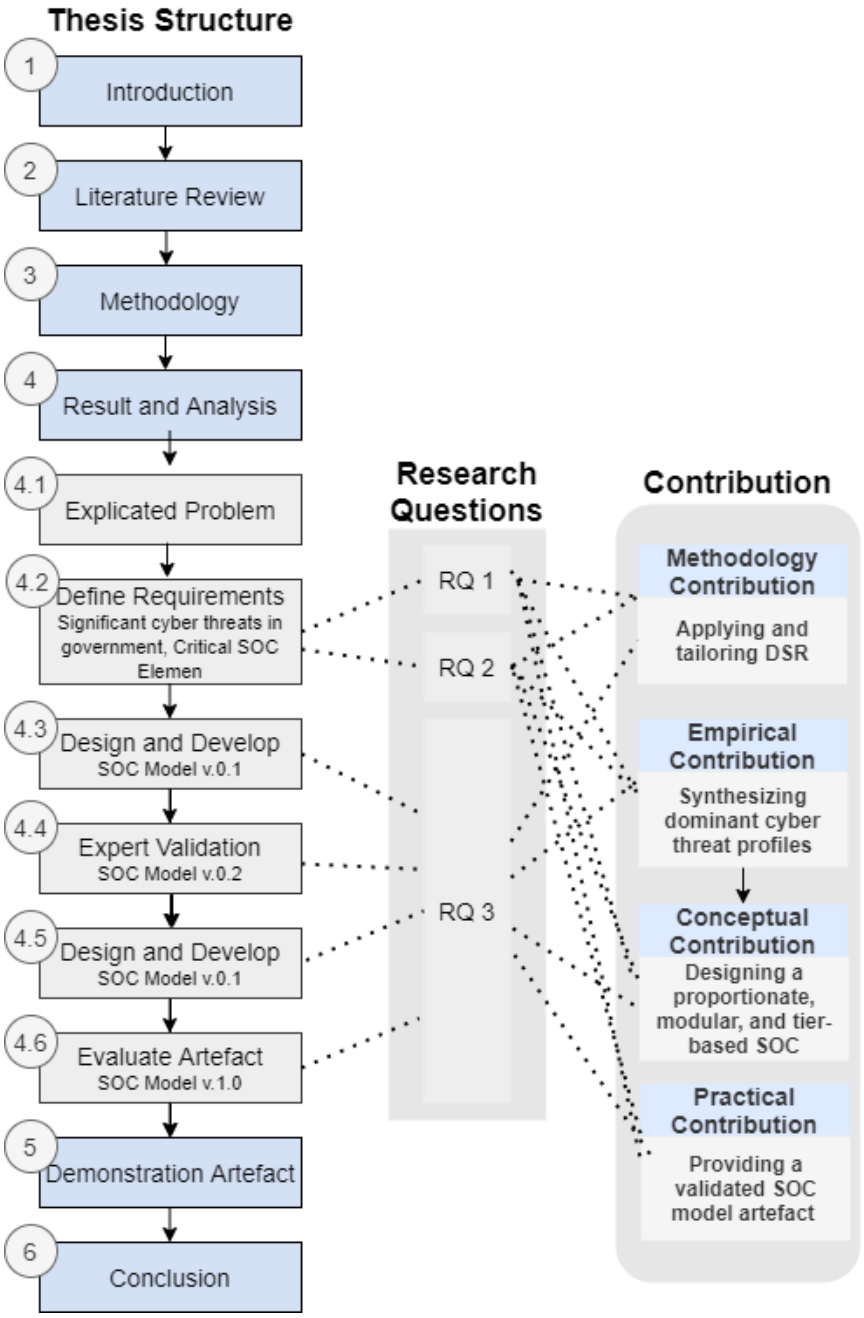

Figure 1.1: Thesis Stucture