

## Chapter 3

### RESEARCH METHODS

This chapter elucidates the study framework, comprising a dynamic analytic technique, a system overview, a detailed recommended approach, and evaluation criteria for validating experimental results.

#### 3.1 Research Framework

The research framework utilized in this thesis is illustrated in Figure 3.1. It encompasses a comprehensive approach, including a literature review, gap analysis, framework modification, as well as evaluation and validation processes.

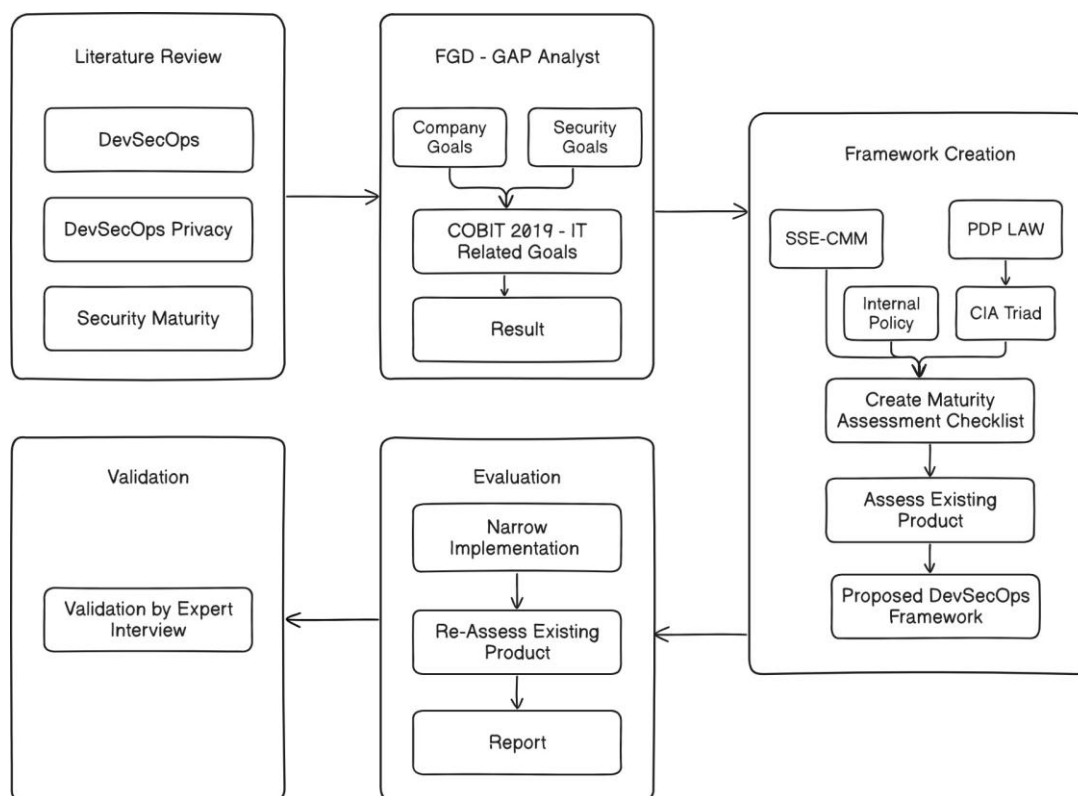


Figure 3.1: Research Framework

In this research framework, we plan to conduct a Focus Group Discussion (FGD) to identify the organization's current challenges and objectives. Building on these insights, we incorporate privacy protection requirements—drawn from PDP law—into the CIA

triad, as well as reference internal policies. These elements then be combined to form a maturity assessment checklist, which be measured using the SSE-CMM framework. Next, we apply this maturity assessment to existing products at PT XYZ, offering recommendations based on the results and proposing a DevSecOps framework for future use.

Following these recommendations, the relevant product teams can prioritize the maturity checklist items that best align with their immediate needs. Once the recommended improvements are implemented, we reassess the product's security posture and compile a comprehensive report. Finally, our framework be validated by subject-matter experts to ensure its effectiveness and relevance by doing the interview.

### 3.2 Literature Review

The Literature Review phase involves a thorough exploration of existing knowledge essential for advancing security maturity through the integration of DevSecOps principles. It focuses on three key areas: the foundational concepts and practices of DevSecOps, frameworks for assessing security maturity, and the application of these principles within organizational contexts. Examining DevSecOps provides insights into how development, security, and operations can be effectively integrated to enhance software security and agility. Reviewing security maturity frameworks offers a structured approach to evaluating and improving an organization's security capabilities over time. This analysis is complemented by exploring real-world implementations and case studies, ensuring alignment with best practices and industry standards. By synthesizing this information, the Literature Review establishes a strong theoretical foundation, guiding the identification of relevant strategies, tools, and metrics tailored to improving security maturity through DevSecOps. This phase ensures that the subsequent framework development and implementation are deeply rooted in validated methodologies and practical applications, paving the way for meaningful and sustainable improvements.

### 3.3 GAP Analyst

The Gap Analysis phase is designed to identify discrepancies between the organization's current situation and the desired state, guided by DevSecOps principles, COBIT 2019 IT-related goals and domains, industry best practices, and organizational objectives. This process begins with a series of Focus Group Discussions (FGDs) involving key stakeholders, including managerial, operations, and security teams, to gather diverse perspectives on the organization's current practices, challenges, and aspirations.

During the FGDs, the company's broader objectives are aligned with specific security goals, ensuring that security enhancements support overarching business priorities. These goals are mapped against COBIT 2019 IT-related goals and domains, providing a structured framework for assessing alignment and identifying areas of misalignment or underperformance. COBIT 2019's focus on IT governance and management ensures that the identified gaps are grounded in best practices and standards.

The criteria for selecting participants for this FGD are as follows:

- **Role and Experience:** The participant should possess thorough knowledge of PT XYZ unique security challenges and requirements, enabling them to evaluate whether the proposed metrics effectively align with the organization's security objectives.
- **Familiarity with PT XYZ Environment:** It is vital that the expert has firsthand experience with PT XYZ infrastructure, policies, and security culture. This background ensures their feedback on the metrics is properly grounded in XYZ's unique environment.

The result is a comprehensive gap analysis document that highlights critical discrepancies between current practices and desired outcomes, organized within the context of COBIT 2019 domains. By systematically assessing and prioritizing gaps, this phase enables the organization to focus on addressing high-impact areas that align with both security and company goals. This structured and methodical approach sets the foundation for targeted improvements, guiding the implementation of DevSecOps

practices and the advancement of security maturity to meet both operational and strategic objectives.

### **3.4 Framework Creation**

#### **3.4.1 Create Maturity Assessment Checklist**

The framework modification phase focuses on enhancing the security maturity framework by incorporating structured maturity assessment questions on different domain. These questions are crafted to align with the principles of the SSE-CMM (Systems Security Engineering Capability Maturity Model), ensuring a robust evaluation of security practices and processes. The questions also integrate the organization's internal policies, allowing the framework to reflect unique governance and compliance requirements while maintaining relevance to operational contexts.

Additionally, the framework is rooted in the foundational principles of the Confidentiality, Integrity, and Availability (CIA) triad. This ensures that the assessment thoroughly evaluates the organization's ability to safeguard data, maintain system integrity, and ensure operational availability. By embedding these elements, the modified framework provides a holistic and adaptable tool for assessing and improving security maturity, aligning with both industry standards and organizational goals.

#### **3.4.2 Assess Existing Product**

During this phase, a comprehensive maturity assessment that we already create from the previous stage is carried out to evaluate the current state of the existing product. This process aims to measure the maturity levels of individual programs within the product, assessing their alignment with defined benchmarks and security standards. Additionally, the phase evaluates the effectiveness of the maturity assessment itself, ensuring it provides meaningful insights and actionable data to drive improvements. This assessment is guided by the principles and metrics developed in earlier phases and focuses on determining how well the current processes align with the framework's objectives. The results of the assessment provide valuable insights into areas requiring further improvement and serve as a baseline for measuring the success of the framework's implementation.

### 3.4.3 Proposed Framework

This assessment is essential for establishing a clear baseline of the organization's CI/CD current state. By pinpointing gaps, such as the absence of automated security checks, insufficient monitoring, or weak access controls, the organization gains a detailed understanding of where improvements are needed. Armed with this knowledge, the next logical step is to propose a tailored DevSecOps pipeline that integrates security seamlessly into the CI/CD processes.

The proposed DevSecOps pipeline would address the identified gaps by embedding security measures, such as automated vulnerability scanning, policy compliance checks, and robust access management, directly into the CI/CD workflows. This integration not only strengthens the security posture but also ensures that security becomes an integral and continuous part of the software delivery lifecycle, aligning with DevSecOps principles. By transitioning to this enhanced pipeline, the organization can achieve a more secure, efficient, and resilient development process.

### 3.5 Evaluation

The evaluation phase involves the practical implementation of the maturity assessment and the DevSecOps framework within a controlled, focused scope to ensure feasibility and effectiveness. This step acts as a critical proof-of-concept, allowing the organization to apply the designed framework and assessment methodology to a specific project, team, or product. By narrowing the scope, the evaluation ensures that the implementation process is manageable and that any challenges or limitations can be identified and addressed before scaling the framework across the organization.

#### 3.5.1 Narrow Implementation

Simultaneously, the DevSecOps framework is implemented within the same focused scope. This involves integrating security practices such as automated and manual security testing, policy enforcement, and continuous monitoring into the CI/CD pipeline of the selected project or team. The framework is tested for its ability to enhance collaboration among development, security, and operations teams while maintaining or improving delivery speed and quality. By closely monitoring the implementation,

the organization can gather feedback on the framework's effectiveness, usability, and alignment with business goals.

### 3.5.2 Re-Assess Existing Product

Re-Assessing Existing Product Steps involves taking a deeper, more comprehensive look at the previously implemented framework, which had a relatively narrow scope. By thoroughly evaluating its effectiveness, identifying potential areas for improvement, and exploring how it can be expanded or refined, this reassessment ensures the framework remains adaptable, functional, and aligned with evolving product goals.

### 3.5.3 Report

The evaluation phase also includes regular review sessions and feedback loops with stakeholders to ensure the framework addresses their needs and challenges effectively. Any issues or areas of resistance encountered during this phase are documented, analyzed, and addressed to refine the framework. The insights gained from this targeted implementation are critical for ensuring the framework's scalability and adaptability across the organization, laying a strong foundation for broader deployment in the future.

## 3.6 Validation

Validating a research framework entails confirming its reliability, relevance, and effectiveness in supporting the research process and achieving the desired objectives. This process includes obtaining feedback and insights from subject matter experts in the field to ensure the framework's credibility and applicability. In this study, the validation involves conducting interviews focused on the proposed DevSecOps framework, which integrates a maturity assessment. These interviews aim to evaluate the framework's practicality, alignment with industry standards, and ensuring its overall robustness and effectiveness.

The criteria for selecting participants for this validation are as follows:

- **Role and Experience:** Participants must be experienced security professionals and have the experienced in the DevSecOps domain. They should possess deep expertise in addressing the unique security challenges and requirements

of DevSecOps and security area. Their insights are crucial for evaluating how effectively the proposed DevSecOps framework aligns with industry standards and ensuring its overall robustness and applicability.

The primary outcome of this research is the creation of a comprehensive framework that unifies both security and maturity assessments, ensuring robust protection and UU PDP compliance before an application enters production. This integrated approach not only identifies and addresses vulnerabilities within the application itself but also verifies that the infrastructure meets all necessary standards to prevent data breaches or credential leaks. By minimizing these risks, organizations can avert potential UU PDP violations and maintain a thoroughly secured, mature, and compliant deployment. The success criteria for applications that adhere to the DevSecOps pipeline is achieved when their maturity level reaches the "Planned and tracked" stage or the average is 2 on the capability level. At this level, applications should provide sufficient evidence to support comprehensive security assessments. By meeting these criteria, the product can ensure that their applications are not only secure but also capable of undergoing thorough evaluations, thereby reinforcing their commitment to maintaining high security standards and compliance with relevant regulations.