

CHAPTER 3 – RESEARCH METHODS

This chapter explains the research design and research framework, analysis methodology, the general system overview, the method proposed in detail, as well as the process of collecting data, evaluation and to validate the results of research.

3.1. Research Design.

According to (Creswell, 2014), research design is a comprehensive plan or strategy for conducting research to systematically answer research questions. Creswell divides research design into three main approaches: quantitative, qualitative, and mixed methods. Quantitative approaches focus on hypothesis testing through numerical data and statistical analysis, while qualitative approaches seek to understand phenomena in depth through interviews, observations, and case studies. Mixed methods approaches combine both strategies to gain a more comprehensive understanding. Creswell also emphasizes the importance of a fit between the research problem, methodological approach, and data collection strategy.

Meanwhile, (Hevner *et al.*, 2004) introduced Design Science Research (DSR) as a research design in the context of information systems, which emphasizes the creation and evaluation of artifacts to solve practical problems. Hevner outlined seven key guidelines for DSR, including the imperative to produce relevant artifacts, ensure methodological rigor, systematically evaluate artifacts, and effectively communicate research contributions to the academic and professional community. DSR combines aspects of engineering design and science, where researchers not only observe but also create solutions to real-world organizational problems. The research design that includes a mixed analysis methodology, the general system overview, the method proposed in detail, as well as the process of collecting data and evaluation to validate the results of research. The following is the design research in this study, namely threat modeling driven risk management for securing of CMS.

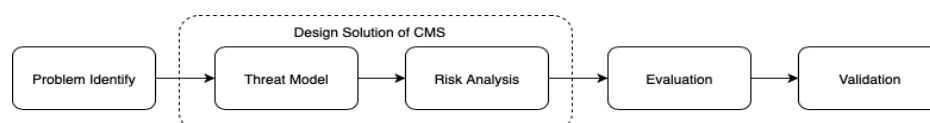


Figure 3.1. Research Design.(Hevner et al., (2004)

3.2. Research Framework.

Based on the design research above, this thesis uses a mix method focus on risk assessment using the threat modeling approach. This approach is designed to identify, analyze, and prioritize potential threats and vulnerability that can affect system security of CMS. By combining modeling threats , vulnerability assessment and risk evaluation scores of scores, this research aims to provide a comprehensive framework in evaluating risks and developing effective mitigation strategies.

This framework is based on several previous study methodologies in table 2.7, using a hybrid framework with a risk-centric approach. Based on table. 2.1 comparative mapping RMF to Threat Model, figure 3.2 will explain the framework for carrying out risk assessment procedures that integrate threat modeling. This framework includes systematic steps, ranging from the identification of assets, threat analysis, vulnerability analysis to the assessment of impacts and the possibility of risk. **The research will employ the STRIDE methodology for identifying security threats, inspired by its successful application in Industrial Control Systems highlighted by (Kim, Kim and Kim, 2022).** This research will use step by step methodology to identify security threats, which as explained by (Kim, Kim and Kim, 2022) , (Khalil *et al.*, 2023) and (Eom *et al.*, 2019). This framework includes methodologies with criteria are business of corporate strategy, operational and technical.

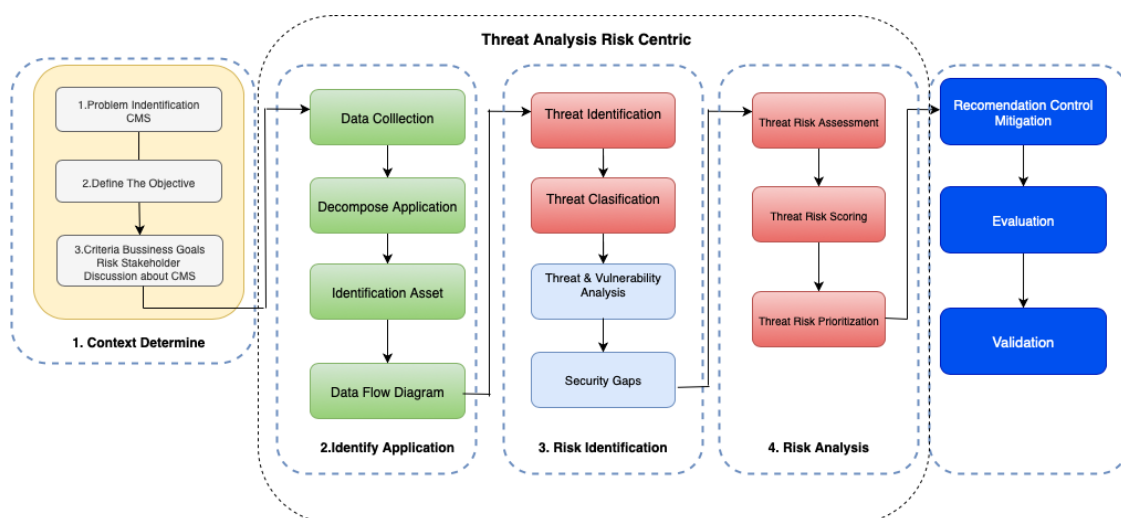


Figure 3.2. Research Framework.

3.3. Context Determination

This section acts as the initial foundation of the research, with the main aim to set specific backgrounds and operational configurations of the CMS system which is the object of study. This process includes determining the research context by formulating the scope of the assessment, identifying the main stakeholders, and conducting a review of relevant documentation. These steps are important to ensure that research has a strong and structured foundation.

The expected results of this phase are clearly defined context documents, which include the description of the operational environment, the use of the system, and CMS data needed to conduct a comprehensive assessment. This document will be the main reference in the stages of further research, ensuring that every aspect of the assessment is carried out with a deep understanding of the system and the environment.

3.3.1. Define the Context

This subsection is the initial stage in the threat modeling process. The aim is to build a deep understanding of the operational environment of the CMS system at PT.XYZ. This process involves identification of CMS goals, users involved, the type of data managed, as well as specific functions provided by the system in supporting organizational operations. This process is carried out with a focus group discussion internal company that include the IT team, the system procedures team (SOP, Risk Management), the General Manager, and the News Production Manager.

The results of this stage are context definition objective that include the core of the role of CMS, business securities goals, risk criteria stakeholder, data processed and stored, as well as a general picture of how this system operates and the system's constraints. This document serves as the basis for conducting focused and relevant risk assessments, ensuring that threat analysis is conducted with a comprehensive understanding of the company's systems, environment and business processes.

3.4. Data Collection

This subsection is the second stage in the threat modeling process. This section focuses on the collection of all information needed to support the risk assessment process. This

stage involves the collection of detailed documentation related to CMS architecture, manual of CMS , log system, data stored and processed, as well as system interaction with other components. The result of this phase is a collection of data that has been curated, which provides a comprehensive picture of the operational characteristics of CMS.

This dataset plays a crucial role because it will be the basis for identifying potential threats of security and vulnerability in the next stage in the framework of threat modeling. With complete and structured information, the risk analysis process can be done more accurately, effectively and in line with the company's business processes.

3.5. Decompose the Application

After obtaining data about the CMS system, the next step according to the STRIDE threat model method is to decompose the application. The decompose the application focuses on breaking the CMS application into its basic components. The aim is to identify important assets, such as data and services, determine the entry point that has the potential to become an attack vector, and map the flow of data in the application. To achieve this, collaboration is needed with architects or system developers, utilizing application documentation, and making detailed data flow diagrams.

The results of this section are a number of diagrams and comprehensive lists that describe the key elements of the CMS application. This output provides a clear and structured picture, which will be the basis for risk identification in the next stage.

3.5.1. Identification Asset

The first part focuses on identifying the main assets in the CMS system. These assets include data repositories, software components, network connections, and other elements that are important for the operation of the system and have strategic value for the organization. This process requires data collection of these assets and in depth understanding of the role of significance in the context of PT.XYZ's business operations.

The result of this stage is a list of complete and detailed assets, which will be the basis for determining where security measures need to be applied in priority. This list helps

ensure that security efforts are focused on the most critical and potentially vulnerable assets.

3.5.2. Data Flow Diagram

This section focuses on visual mapping data flow in the CMS system. The aim is to describe the movement of data from the entry point to the exit point, including the processing, storage, and transmission of data throughout the system. This helps identify potential points in which data can be threatened or vulnerable to violations.

The data flow diagram produced is very important to understand the interaction and dependence of complex between various system components. This clear visualization will be an effective tool in the next stage of identification and risk analysis, ensuring that potential threats can be identified more accurately and comprehensively.

3.6. Risk Identification

In this section, the main task is to identify and document potential security threats that can affect applications systematically. This process involves the use of checklists, previous incident reports, as well as other sources of information to uncover various possible threats that can threaten integrity, availability, and confidentiality of the CMS system. The result of this stage is a list of threat lists that include all identified threats. These threats are categorized and explained in a structured format, which will facilitate further analysis to determine the right mitigation steps.

3.6.1. Threat Identification

This subsection aims to register all potential threats that can exploit the vulnerability of CMS system assets and previously identified entry points. This process includes in depth exploration of various sources of threats, including threats from internal, external actors, and potential technical failures. Techniques such as data analysis of historical security incidents and the application of known threat models, such as STRIDE for application analysis, LINDDUN for data privacy and DREAD, are used to ensure a comprehensive threat risk. The result of this process is the initial list of potential threats, where each threat is explained in detail related to the nature and potential impact. This list is the basis for further analysis in determining effective mitigation steps.

The misuse case approach is an effective method in carrying out threat modeling on the software system, because it allows threat analysis to be carried out from the perspective of perpetrators who intend to be evil (malicious actor). In this thesis, misuse case is used to identify and how the system can be misused, completing the traditional use case approach that only describes the expected system behavior. Misuse Case introduces the elements of the evil actor who interact with the system through the threat scenario, which is then associated with a legitimate use case to uncover the potential for abuse and security gap.

Some studies support the effectiveness of this method, as explained by (Andrade *et al.*, 2023) to analyze the importance of integrating security modeling by software developers into the elicitation processes facilitated through the utilization of abuse stories. The decision to collect data using a use case approach in threat modeling for CMS is based on the methodology proposed by (Mai *et al.*, 2018) in the paper "Modeling Security and Privacy Requirements: A Use Case-Based Approach." This approach effectively integrates security concerns into the early stages of system analysis by extending traditional use case diagrams to encompass potential malicious actors and their objectives. Through use cases, one can explicitly capture undesirable behaviors and threats such as unauthorized data access, privilege escalation, or injection attacks, which may not be apparent in standard functional requirements. By identifying use cases and their mitigations, analysts can better understand system vulnerabilities and formulate security requirements systematically. This data collection used a misuse case model through a group discussion forum between **developers and the IT security team** at PT XYZ. The following is the form used in this research show on table 3.1 :

Table 3.1. Misuse Case Form

Misuse Case	
Process / Component	
Threat Name	
Description Threat	
Assets	
Actor	
Threat Category	
Impact	

3.6.2. Threat Clasification.

This section focuses on organizing the threats that have been identified into a structured format. This table functions as a tool to categorize, measure, and document each threat systematically. Usually, description such as threat's, descriptions, affected assets, possibilities for occurrence, potential impacts, as well as existing countermeasures.

A well organized table not only facilitates a clearer understanding of each threat, but also becomes the foundation for the next stage of assessment and priority threats. The end result is a detailed threat list table, which provides a comprehensive picture of the potential risk of the CMS system. This list is prioritized for further analysis and actions in the risk management process.

3.6.3. Vulnerability Analysis .

This section focuses on finding identified vulnerabilities into a structured format. The assessment is carried out using forum grup discussion developer, IT team and scanning tools online OWASP. The results of this are in the form of a table that serves as a tool to categorize, measure, and document each threat systematically. Typically, this table includes columns such as threat's, vulnerability, and CVE (Current State of Vulnerability Verification).

3.6.4 Security Gap Analysis

The complexity of CMS often leaves security gaps that can be exploited by attackers. Therefore, in this research it is important to conduct a security gap analysis to identify threat, vulnerabilities, compare with security best practices such as OWASP Top 10, and systematically assess risks as part of threat modeling and risk management.

The goal is to security gap analysis relevant to the CMS, compare the current state with the CVE (Current State of Vulnerability Verification), an international standard identification system that documents and catalogs vulnerabilities, identify security gaps between actual and ideal conditions, assess the risk level based on impact and likelihood of exploitation, and provide mitigation recommendations based on risk priority (Chen *et al.*, 2018). Therefore, security gaps can indicate that the system lacks comprehensive

protection according to security standards such as the OWASP Top 10 or ISO/IEC 27001.

This section focuses on the results of data collection using vulnerability scanners, manual audits with developers and IT security teams, and log reviews, which can be displayed in tabular form. The resulting threat and vulnerability mapping is then compared with the OWASP Top 10 list as a reference for best practices. Security gap identification is carried out by determining the differences between the actual state and the best practice standards.

3.7. Risk Analysis

In this section, the identified threats are evaluated in depth to assess their potential impact and likelihood of occurrence. This process is done through a scoring system that measures the severity of each threat, taking into account factors such as the value of the assets affected, the ease of exploitation of the threat, and the potential consequences. The end result is a prioritized list of threats, where each threat is ranked according to its severity. This provides a clear direction for determining the focus of risk management efforts.

3.7.1. Threat Analysis

In this section will analyze the threats that have been identified from STRIDE for security and LINDDUN for data privacy threat modeling. This step involves mapping system components and data flows to determine where each type of threat can occur. After the threat is identified using STRIDE and LINDDUN, the next step is to evaluate the impact and likelihood of occurrence based on the DREAD risk score. Each threat is scored for each criterion, and the total score is used to determine the severity of the threat. The result is a prioritized list of threats,

Further analysis by combining business and technical perspectives using threat prioritization. These steps ensure that the identified threats are relevant to the business context and have a significant impact on the organization's.

3.7.2. Threat Scoring

In this section, the DREAD model will be used in the threat scoring process to evaluate the threats identified in the PT.XYZ CMS system. Each threat will be assessed based on five DREAD criteria, namely Damage Potential, Reproducibility, Exploitability, Affected Users, and Discoverability. This assessment aims to measure the severity of each threat objectively. Base on Security/OSSA Metric corelation with CMS :

Table 3.2. Criteria DREAD of CMS (Security/OSSA Metric)

Criteria	Criteria Description	Score	Level	Score Description	CMS Context
Damage Potential (D)	Estimated harm if the vulnerability is exploited	0		No damage or negligible effect	UI glitch with no data loss
		1-3	Low	Local impact, no business disruption	Article preview formatting issues
		4-6	Medium	Unauthorized read/write access to specific records	Edit draft of a single article
		7-8	High	System-wide content manipulation or defacement	Change headlines or images site-wide
		9-10	Critical	Full CMS data access (read/write/delete), compromise	Alter or delete all news content
Reproducibility (R)	Ease of reproducing the attack	0		Nearly impossible to reproduce	Race condition requiring precise timing
		1-3	Low	Needs specific environmental setup or insider access	Requires known session token or specific user role
		4-6	Medium	Manual reproduction with consistent steps	Form input must be specially crafted
		7-8	High	Easy to reproduce with known tools or scripts	Repeatable SQLi with Burp Suite or sqlmap
		9-10	Critical	Easily and reliably reproducible by anyone	Public exploit available, works every time
Exploitability (E)	Resources, skills, and tools required	0		Practically unexploitable	Requires physical access to isolated network
		1-3	Low	Needs advanced attacker skills or custom code	Low-level memory exploit
		4-6	Medium	Exploitable with moderate technical ability	Custom XSS payload with crafted URL
		7-8	High	Can be exploited with widely available tools	SQLi with sqlmap or XSS with browser injection
		9-10	Critical	No technical skills needed; just interact with CMS	Exploit via public-facing login with weak password
Affected Users (A)	Proportion of users/systems impacted	0		No users affected	Exploit is theoretical or internal-only
		1-3	Low	Single user impacted	Account takeover for one contributor
		4-6	Medium	Group of users affected or limited CMS functions	Editors cannot access dashboard
		7-8	High	Majority of users or audience affected	Article corruption visible to readers
		9-10	Critical	All users / public / full CMS disruption	Public-facing CMS taken down
Discoverability (D)	Likelihood attackers find the vulnerability	0		Hidden behind multiple security layers	Vulnerability in private microservice
		1-3	Low	Only visible through advanced recon or logs	Requires inspecting API traffic
		4-6	Medium	Visible in debug mode or through UI with effort	CMS error shows stack trace or SQL error
		7-8	High	Easily found with basic testing tools	Fuzzing detects form injection points
		9-10	Critical	Trivial to find — advertised or documented	Login form with no rate limiting; admin interface exposed

DREAD scores five categories, which are summed together and divided by five, the result is a score from 0-10 where 0 indicates no impact and 10 is the worst possible outcome:

$$\text{RISK} = (\text{DAMAGE} + \text{REPRODUCIBILITY} + \text{EXPLOITABILITY} + \text{AFFECTED USERS} + \text{DISCOVERABILITY}) / 5$$

Furthermore, a risk score will be calculated based on the results of the identified threat assessment. This score will help determine the priority of threats, so that the security team can focus on the most critical threats and design effective mitigation measures. This process ensures that risk management efforts are carried out in a structured and targeted manner.

3.7.3. Threat Prioritization

In this section, after identifying the types of threats and risks associated with PT.XYZ's CMS system, the next step is to classify the threats and risks based on their severity, from highest to lowest. This classification helps in understanding which threats are the most critical and require immediate attention. Each threat will be assessed based on five DREAD criteria, namely Damage Potential, Reproducibility, Exploitability, Affected Users, and Discoverability. This assessment aims to measure the severity of each threat objectively.

Next, a table containing a list of threats and risks with the highest severity will be prioritized for further analysis. This analysis aims to determine appropriate and effective mitigation measures to reduce the negative impacts that may arise from these threats and risks. Thus, risk management efforts can be focused on the areas that are most vulnerable and have the potential to cause the greatest losses.

3.8. Determine Countermeasures

This section focuses on aligning risk mitigation strategies with best practices and recommended controls in the international standard ISO 27001:2022 and OWASP Top 10. This standard provides comprehensive guidelines on globally recognized information security practices. For each risk identified in the CMS system, relevant controls from ISO 27001:2022 are selected and tailored to the specific context and needs of PT.XYZ. Mitigation recommendations based on ISO 27001:2022 are for Management Level needs. Relevant controls from OWASP Top 10 are selected and tailored to the needs of PT.XYZ's **IT developer and system administration teams**.

Some examples of implementing these controls include implementing strict access control policies, encrypting sensitive data, establishing clear operational procedures, and conducting regular security training for employees.

The effectiveness of these mitigation strategies is assessed based on their compliance with the OWASP Top 10 and ISO 27001:2022 standard, ensuring that the approach used is not only robust but also meets recognized global standards. By adopting these practices, PT.XYZ can build a resilient and sustainable information security system, while minimizing the risks that may arise from security threats.

3.9. Research Evaluation

This section focuses on evaluating CMS based on best practices and controls recommended by international standards ISO 27001:2022 and OWASP Top 10. Both standards provide comprehensive guidance on globally recognized information security practices. By ensuring that CMS applications meet these security standards, business operational continuity can be maintained properly.

Compliance with these security standards not only increases system reliability but can also increase the business value of PT.XYZ. By having a secure system that meets international standards, companies can build customer trust, minimize security risks, and support sustainable business growth. Guided questions and discussion Table 3.3 provide the structure for these evaluation sessions.

Table 3.3. Topic Form for Evaluation Stakeholder PT XYZ.

No	Discussion Point	Topic Covered	Description
1	Scope	Objective goal of model	Examination of the scope and objectives of the threat modeling, ensuring alignment with the research goals.
2	Methodology	Appropriateness of Methodology	Evaluation of the suitability methodologies for this research.
3	Risk Analysis	Completeness Risk Prioritazion	Evaluation of how thoroughly the assessment covers all necessary threat categories frameworks for impact.
4	Control/Mitigation	Effectiveness of Mitigation Strategies point of you bussines perspective.	The adequacy of the proposed strategy to mitigate identified threats and vulnerabilities at the management level.

3.10. Research Validation

Research validation ensures the reliability, relevance, and effectiveness of the research method, ensuring it meets its objectives. Steps for validating a research framework are seek feedback form subject matter expert or peers in the field. Their insights can assess the framework alignment with established theories, methodologies and potential effectiveness in addressing the research problem. During validation will be used forum discussion group involving.

1. Internal IT , IT developer and Stakeholder to validate the research result of evaluation.
2. External security expert to validate the research result of evaluation from external perspective.

This validation process combines insights from experts in the field with expert criteria in external software development expert, risk management expert, and threat modelling cyber security expert, conducted through interviews. The experts involved in the validation of this research are in depth competence and practical experience in several related domains. First, they need to have a comprehensive understanding of the principles of cyber security (cybersecurity fundamentals), including the concept of threats, vulnerability, exploitation (exploitation), impact, and security controls. Second, specific expertise in threat modeling methodology such as stride, dread, or others is very crucial, including the ability to identify relevant threat actors for CMS, potential attack vectors, and attack surfaces typical of CMS applications. Third, they must be proficient in Vulnerability Assessment and Penetration Testing (VAPT), specifically related to their websites and ecosystems, including in depth knowledge of general vulnerability (OWASP Top 10, CVE), exploitation techniques, and vulnerable analysis tools. Third, competencies in risk assessment and risk management are absolutely necessary, including the ability to assess the probability and impact of threats identified to organizational assets, as well as determining the level of risk (risk level) accurately and consistently. Fifth, a strong understanding of effective Mitigation control strategies and techniques for CMS is essential, including technical controls (such as hardening, patch management, WAF, input validation, strict access control) and non-technical (policies, training). Finally, direct experience in designing, developing, managing, or securing

CMS based systems is highly valued, because it provides a practical context of the challenges of implementation and operations in a real environment. The combination of theoretical expertise and practical experience of experts can provide credible and valuable validation to the research framework and results.

Based on the approach in the paper "Development and validation of a questionnaire to measure research impact" by (Solans-Domènech *et al.*, 2019), the scope of questions for validation of this thesis was carried out through systematic and evidence-based stages. The first step is item generation, which is formulating questions based on a literature review related to threat modeling, risk management, and CMS security, as well as interviews with stakeholders at PT XYZ. These questions reflect the main dimensions of the developed model, such as the effectiveness of the threat model in identifying risks, integration into the risk management process, and its impact on strengthening CMS security. Next, content validation was conducted by a panel of experts to assess the relevance and clarity of each question. After that, the resulting recommendations serve as a reference for implementation by upper management, information security practitioners, or relevant technical teams at PT XYZ to improve the security posture of the organization.

To performing validation method, several key question form was prepared to completing the steps in the research framework that are show in table 3.4.

Table 3.4. Question Form Validation.

No	Validation Point	Topic Covered	Validation Outcome
1	Scope	Objective goal of model	Scope and objectives are clarified, alignment is established for threat model determination.
2	Methodology	Appropriateness of Methodology	Validation of the suitability methodologies for this research.
3	Threat Identification	Completeness of Threat Identification and categories	Validation of the comprehensiveness in identifying all relevant security and

No	Validation Point	Topic Covered	Validation Outcome
			privacy threats to the CMS system.
4	Vulnerability Analysis and Gap Analysis	Review identified vulnerabilities and security gaps for accuracy and relevance.	Validation of existing vulnerabilities of CMS and Security Gap Analysis.
5	Risk Analysis	Validate risk prioritization.	Confirmation of risk scoring and prioritization.
6	Mitigation Strategies	Evaluate proposed mitigation strategies and control.	Validation of proposed control mitigation.

The research questions in this study significantly specify the research and indicate the expected outcomes. Topic questions address scope, methodology, threat identification, vulnerability analysis, risk analysis, and control mitigation strategies. The questions can be found in the following sections:

1. Questionnaire for Software Developer Expert **Appendix 7.**
2. Questionnaire for Cyber Security Expert **Appendix 8-11**