CHAPTHER I

INTRODUCTION

1.1 Background

In today rapidly developing digital era, information technology has become an essential part of human life. Nearly all human activities social, economic, and governmental rely on globally connected digital systems. One of the consequences increasing amount of personal data being stored, processed, and shared digitally. Information such as full names, addresses, identification numbers, job positions, family data, and financial details are now easily accessed and stored across various digital platforms, from social media to cloud-based personnel systems. However, this advancement also brings significant challenges regarding the security of personal data. This technological advancement also presents significant challenges related to personal data security. Personal data is highly susceptible to misuse by irresponsible parties such as hackers, online scammers, or even internal personnel within an organization. Data breaches can result in serious consequences, including identity theft, financial fraud, and reputational damage for both individuals and institutions. The security of personal data is particularly critical for employees working in government institutions, as it involves not only individual safety but also the integrity and public trust in the institutions themselves. The HR division plays a vital role in this context, as it stores and manages sensitive information such as employment history, salary details, bank account numbers, and other personal documents.

Timor-Leste received a very low score of 0 out of 20 regarding technical impleme-

tation according to the Global Cybersecurity Index. This indicates that government institutions are still lacking in utilizing encryption technology, access control systems, and methods for handling security incidents.

The result from Jain et al. (2025) are closely tied to this study, highlighting major flaws in fundamental cybersecurity measures like encryption and access control. These specific measures are essential for protecting sensitive employee information held in HR system. Without these protection in place, there is heightened threat of unauthorized access, information breaches, or improrer use within the organization, underscoring the importance of this research for enhancing institutional practices. This situation highlights the low level of awareness and implementation of the importance of information security within government digital systems. The lack of security standards, limited human resources in information technology, and low implementation of security policies present real challenges. Given this reality, there is a significant research gap as no prior study has applied a systematic approach such as the OCTAVE Allegro framework has examined the risks to personal data of public sector employees in Timor-Leste. However implementing the OCTAVE Allegro framework in government present several obstacle. A primary challenge is the staff limited skill and low awareness of best practices for information security.

Numerous government workers may not fully grasp the significance of categorizing asset, controlling access or reporting incidents, which could impede precise threat detection. Additionally the lack of current documentation, like access logs or official data protection policies, may diminish the analysis effectiveness. Nonetheless OCTAVE Allegro is a good fit because it adjust well to

environment with limited resources and can include insight from both technical and non technical persperctive.

OCTAVE Allegro (Operationally Critical Threat, Asset, and Vulnerability Evaluation) method. This method is designed to identify, threats assess, evaluate vulnerability and respond to risks concerning sensitive information, including employee personal data managed within the HR division of a government institution in Timor-Leste. Thus, this study seeks to identify and assess hazards to staff personal data within a Timor-Leste government agency by means of a systematic risk analysis using the OCTAVE Allegro framework. Understanding the weaknesses in current data handling methods and evaluating the degree of risk will help to offer clear cut mitigating actions. These study results should help public institutions to improve information security policies, therefore ensuring compliance with constitutional data protection rights and raising public trust in government systems. OCTAVE Allegro is selected for this study because it is considered more suitable for the context and needs of HR divisions in government sectors. Unlike other methods such as NIST SP 800-30, which are highly technical and typically used by IT teams, OCTAVE involves all organizational elements both technical and non- technical in identifying assets, assessing threats, and formulating risk mitigation policies. This makes OCTAVE more inclusive and applicable within diverse governmental environments.

According to Ali et al. (2026), OCTAVE Allegro provides a risk based approach that can be tailored to organizations that focus on protecting sensitive information. This approach enables institutions to align their security practices with operational goals and existing internal policies. Therefore, the OCTAVE

Allegro method not only helps in identifying threats but also strengthens integrity and trust in the comprehensive management of personal data.

In Timor-Leste, personal data protection is legally established in the Constitution of the Democratic Republic of Timor-Leste, specifically Article 38 on the Protection of Personal Data. This article states: "The law defines the concept of personal data and the conditions applicable to its processing." This underscores the importance of maintaining the confidentiality and integrity of personal data, particularly in the context of government employees. In the event of a data breach, the responsible institution may face legal sanctions, highlighting the critical importance of secure personal data management.

1.2 Problem Identification

From the background described, the core problem identified is the lack of a structured risk analysis and planning process concerning the security of employee personal data in the Government Instituition of Timor-Leste. This analysis is essential for assessing existing vulnerabilities in information security, which can be addressed using the OCTAVE Allegro method.

1.3 Problem Scope

This research will focus on the Human Resources Division within a government institution, specifically targeting the management of employee personal data. However, the analysis will be carried out through the OCTAVE Allegro framework, which emphasizes a qualitative, organizational level evaluation of risks related to how digital assets are handled, accessed, and protected within the institution.

1.4 Problem Formulation

To achieve the objectives of this research, it is important to formulate research questions that will serve as a guide throughout the analysis process and ensure that the research remains focused on the identified issues. The problem formulation in this study is developed based on the need to evaluate employee personal data security risks within the Human Resources Division of a government institution in Timor-Leste using the OCTAVE Allegro approach. Furthermore, this research aims to provide recommendations that can support the improvement of information security practices and strengthen the protection of employee personal data. Based on this explanation, the research problems are formulated as follows:

1. How does the OCTAVE Allegro method work in Analyzing Personal Data Security risks within a Government Institution,in Timor-Leste?
2. What Rekomendations can be made based on the Result of the Analysis using the OCTAVE Allegro method?

1.5 Research Objectives

Based on the identified problems, this study aims to address both theoretical and practical aspects. The theoretical objective is to enhance understanding and provide academic contributions regarding the application of the OCTAVE Allegro method in assessing employee personal data security risks within government institutions. On the other hand, the practical objective is to provide applicable recommendations for relevant institutions to strengthen the security and protection of employee personal data based on the results of the conducted risk analysis :

1. Theoretical Objective

To contribute to the theoretical development and understanding of the OCTAVE

method in the context of employee database security within government institutions.

2. Practical Objective

To provide actionable recommendations for relevant institutions to improve the security of employee databases, based on risk analysis conducted using the OCTAVE Allegro method.

1.6 Research Benefits

In addition to conducting the research, this study is expected to provide benefits from both theoretical and practical perspectives. The theoretical benefits are related to the contribution of this study to the development of knowledge, particularly in the field of information security through the application of the OCTAVE Allegro method for assessing personal data security risks. Meanwhile, the practical benefits are associated with the implementation of the research findings to assist organizations or institutions in identifying risks, evaluating existing security measures, and strengthening the protection of employee personal data.

1. Theoretical Benefit

This research contributes to the development of insights in the field of Information Security particularly in the application of the OCTAVE Allegro method for personal data security risk analysis. It is expected that the results of this research can enrich academic references related to the identification of vulnerabilities and risk assessment in the management of employee personal data within organizational information systems.

2. Practical Benefit

In practical terms, this research assists organizations in evaluating vulnerabilities in the storage and management of employee personal data and in assessing whether existing security measures are adequate. Through the results of risk analysis, institutions can identify potential threats and vulnerabilities and implement appropriate improvements or security controls to enhance the protection of employee data in the future.