Information Systems Security Risk Management Using the COBIT 2019 Framework and NIST 800-30 on the Website People's Representative Council NTB

Alvionita Safira Wahab*, Raphael Bianco Huwae, Andy Hidayat Jatmika
Dept Informatics Engineering, University of Mataram
Jl. Majapahit 62, Mataram, Lombok NTB, INDONESIA
Email: alvionitasafirawahab@gmail.com, [raphael,andy]@unram.ac.id

Corespondence Author

This research analyzes information security risk management on the website of the Regional People's Representative Council (DPRD) of West Nusa Tenggara (NTB) using the COBIT 2019 and NIST 800-30 frameworks. The main objective of this research is to identify weaknesses in existing security controls and provide recommendations for improvements to deal with cyber threats, specifically DDoS, cross-site scripting (XSS), deface, and SQL injection attacks, which can disrupt service availability and data security. The research methods included interviews with five key stakeholders who have responsibilities in information security, as well as the distribution of questionnaires to ten IT staff. Data from the interviews and questionnaires were analyzed using risk mapping according to the COBIT 2019 framework and NIST 800-30 to identify capability gaps. The results showed specific weaknesses in the management of controls against XSS and DDoS threats, especially in the aspects of monitoring and incident response. The research conclusions emphasize the need to improve risk management through the addition of more up-to-date security technology, increased security awareness and training for staff, and regular security audits to ensure the sustainability of risk management. Recommendations include the implementation of a more sophisticated threat detection system, periodic training for staff, and a more structured incident response procedure to improve security and ensure continuity of public services through the DPRD NTB website.

***Key words*: Risk Management, Information Security, COBIT 2019, NIST 800-30, Cyber Threats.**

I. INTRODUCTION

An information system is a structure that integrates resources, including people and computer technology, to process data into information that supports the company in achieving its targets. With good coordination, information systems can increase institutional efficiency [1].

Information technology governance includes policies, processes, and activities that support IT operations to align with expected business strategies. Good IT management helps achieve the goals of agencies that utilize IT in their business processes [2]. Information technology is a crucial element for institutions in supporting the achievement of their vision, mission, and strategic goals. Optimal IT utilization requires proper governance, evaluated periodically [3].

Reliance on IT increases risks that can negatively impact agency performance. Such risks, such as financial loss or decreased service quality, can prevent agencies from achieving their goals [2]. Risk is the potential loss arising from threats to vulnerabilities in the system. This risk includes threats to the storage, disclosure, and processing of information [4].

In the government sector, this risk is increasingly evident as cybersecurity threats increase, which can negatively impact the performance of the institution. Local governments often face cybersecurity threats to websites, such as defacement and malware attacks. These threats disrupt the website's main functions, such as support for the Electronic Office Manuscript Information System (TNDE). In addition to cyber threats, other technical challenges include reliance on third-party network infrastructure and inadequate data center temperature control. Efforts to strengthen security controls, such as encryption and regular monitoring, are needed to ensure the operational sustainability of the system. [5].

To better manage these threats, risk management becomes a necessary approach to maintain a balance between opportunities and threats. Risk management aims to achieve a balance between efficiency and opportunity, while minimizing vulnerability. The risk management process includes identifying, assessing, and controlling risks, which, when properly implemented, can improve decision-making and enhance agency performance [6].

One framework that is often used in IT risk management is COBIT 2019, which plays an important role in overall IT governance. COBIT 2019 offers a design factor process that serves to find out which processes in the agency/company have a large enough impact on the agency's processes that need to be the main focus as well as the focus of improvement in the running of the agency. This framework supports IT governance and provides recommendations for improving IT governance [6].

In addition to COBIT 2019, NIST is also a guide that is widely used in various global institutions to manage information technology risks with a more comprehensive approach. NIST is an internationally recognized risk management guide that focuses on managing IT risks. The NIST process is very comprehensive, covering threat identification to control recommendations to reduce risk [5].

The need to conduct an information security audit arose from the importance of maintaining the integrity and reliability of the DPRD NTB website. An audit is required to identify potential risks that could negatively impact service continuity and data security. Without a thorough audit, there is a risk that significant security gaps will go undetected, which in turn could be exploited by irresponsible parties. In addition, the identification of weaknesses in risk management is also an important foundation for the NTB Legislative Council to develop more effective mitigation strategies. Through this audit, it is expected that the NTB DPRD can obtain a comprehensive view of the current state of their security system, including understanding the specific challenges and obstacles faced in an effort to maintain website security from cyber threats.

In this study, risk management is the main strategy to maintain the balance between opportunities and threats using the COBIT 2019 and NIST 800-30 frameworks. COBIT 2019 plays a role in overall IT governance, while NIST 800-30 is more focused on information security risk management. It aims to combine these two frameworks in an effort to strengthen security risk management on the NTB Legislative Council website, so as to identify and manage the most significant cyber threats. In this research, the importance of information security audits in identifying system weaknesses, especially in the NTB Legislative Council, is also explained, which will help in the formulation of risk mitigation strategies.

II. Relate Works

This section reviews previous literature on risk management in institutions. Studies show that an effective risk management approach can improve risk mitigation, compliance and strategic decision-making. However, there is a gap in terms of consistency of risk management implementation and integration across all levels of the institution. This research seeks to address the gap by providing an integrated approach that ensures consistent and thorough identification, evaluation and management of risks in every aspect, thereby improving the effectiveness and preparedness of institutions in dealing with risks.

Eko Supristiowadi [7] Conducting research related to information security risk management on the Ministry of Finance's Agency Level Financial Application System (SAKTI). With the aim of identifying various risks that may be faced by SAKTI, as well as selecting appropriate controls to mitigate these risks. In this research the author uses the international standard framework ISO 27005 and NIST 800-30, to develop a systematic risk management process. The existing solution applies a systematic risk management framework based on ISO 27005 and NIST SP 800-30 standards, which includes risk identification, selection of mitigating controls, assignment of risk responsibilities, and cost analysis to improve information security at SAKTI.

Arie Vatresia [8] Conducted research related to the audit of the One-Stop Service Management System (SIMANTAP) at Bank Indonesia Bengkulu Province, focusing on the alignment of SIMANTAP objectives with agency objectives. It was found that SIMANTAP capability evaluation was needed to ensure efficient and effective service support, given the importance of IT in banking. The proposed solution includes applying the COBIT 5.0 framework and RACI method to measure system capability, as well as providing performance improvement recommendations, such as creating performance indicators and better documentation. The results show that SIMANTAP's capability is at level 4 (Predictable Process), with strategic steps needed to reach level 5 (Optimizing Process).

Budi Tjahjono [9] Conducting research on E-Government is an innovation in public services that utilizes digital technology to facilitate the process, but also brings various risks that threaten data security, such as data loss, theft, unauthorized access, and hardware damage. At the Communication and Informatics Office (Diskominfo) of XYZ District, this study identified the main threats stemming from human and electrical factors, indicating the need for a systematic risk management approach. Using the NIST SP 800-30 framework, the steps taken include risk identification, assessment and control. The results show that 60% of the risks come from human factors with a low level, while 60% of the risks from electricity are at a high level. This research emphasizes the importance of implementing appropriate mitigation strategies to protect data and information systems, in order to improve the security and reliability of public services to the community.

Alifiani Kurniati, bersama Lukito Edi Nugroho dan Muhammad Nur Rizal [10] Research related to information technology risk management in eGovernment aims to improve the efficiency and effectiveness of government services through the use of information technology. However, in its implementation, e Government in Indonesia faces a number of problems, such as unintegrated governance, suboptimal services, limited information technology human resources, and risks posed by technological developments 4.0, such as artificial intelligence (AI) and big data. To address these issues, international standards-based risk management is applied, such as ISO 31000 for general risk management and ISO 27000 for information security. Frameworks such as COBIT are also used to measure the maturity level of technology governance in government agencies. The results show that the application of ISO 31000 and ISO 27000 standards as well as the COBIT framework has successfully improved efficiency, information security and reduced operational risks in the implementation of e-Government in government agencies.

Academic literature has widely explored the application of risk management in various sectors, with each study offering specific solutions to the challenges faced. This research proposes a structured risk management-based solution to improve information security in the public sector, focusing on the application of frameworks such as NIST SP 800-30, ISO 27005, and COBIT 5.0. The approach is designed to identify, manage and mitigate risks arising in the implementation of information systems in government agencies, as well as ensure that the systems support the effectiveness of public services and protect data security.

From previous literature, various proposed risk management approaches can provide insights into strengthening information security in the public sector. Research by Supristiowadi, Vatresia, Tjahjono, and Kurniati shows the relevance of applying international standard frameworks such as NIST 800-30, ISO 27005, and COBIT in systematically identifying, evaluating, and managing information security risks. This research adapts these methodologies by combining NIST 800-30 and COBIT 2019 to improve the security risk management capability of the NTB Website People's Representative Council. The integration of these approaches not only enables more thorough risk identification, but also provides a more measurable capability evaluation, ensuring that information security governance is aligned with public service objectives. Thus, the combination of COBIT 2019 and NIST 800-30 not only supports strategic governance, but also provides detailed technical guidance, making the risk management approach more holistic. Through this customization, this research is expected to provide a comprehensive and sustainable solution to improve the resilience and security of information systems in the government environment.

III. Research Method

This research uses a framework-based risk management approach to identify, assess and manage risks associated with information security. Several studies support the importance of this approach in improving data protection and information systems. For example, a study by I Nyoman Rai Widartha Kesuma [4] shows that implementing a systematic risk management framework can reduce the level of vulnerability to cyber threats. Figure 1 illustrates the stages of implementing a security risk management framework in this study as well as the recommended mitigation measures.

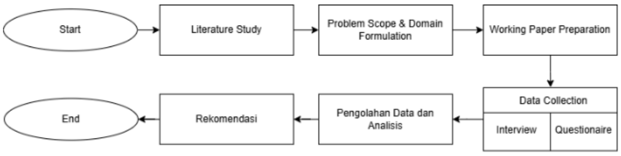
Start
Literature Study
Problem Scope & Domain Formulation
Working Paper Preparation
Data Collection
Interview
Questionaire
Pengolahan Data dan Analisis
Rekomendasi
End

Figure 1. Flow of Research Methods

A. Literature Study

Literature study in research includes searching, collecting, and analyzing relevant information from various sources related to the topic being researched. This stage is carried out as reference material and theoretical basis used in research related to security risk management, understanding of governance and information technology management, and other theories relevant to governance evaluation. This includes the theory for calculating the process capability scale and collecting questionnaire results using measuring tools from the Process Assessment Model (PAM) that are relevant to this research [7].

B. Problem Scope and Domain Formulation

After conducting a literature study, the author formulated the problems faced by the West Nusa Tenggara Regional People's Representative Council (DPRD NTB) in the form of research questions. These questions guided the direction of the research as well as the aspects to be explored further. The literature study is expected to provide answers to these questions. In addition, limiting the scope is necessary so that the scope of the research is not too broad, so that the research can be more organized, relevant, and focused.

Next, the author formulates the domains and processes used in this research. In COBIT 2019 there are five domains, namely APO (Align, Plan, Organize), BAI (Build, Acquire, Implement), DSS (Deliver, Service, Support), MEA (Monitor, Evaluate, Assess), and EDM (Evaluate, Direct, Monitor). The author chose the right domain according to the needs and alignment with the NIST 800-30 framework to ensure the research runs effectively and efficiently. This domain selection refers to the mapping of the NIST 800-30 framework to COBIT 2019. Measurement is carried out using Capability Performance Management (CPM), where each process in COBIT is used as a measurement material after the process in NIST 800-30 has been mapped.

C. Working Paper Preparation

This research paper refers to COBIT 2019 process mapping with NIST 800-30 subcategories to collect, process data, and assess risk management capabilities. Each capability score is validated through interviews and questionnaires based on COBIT 2019 Capability Performance Management (CPM) indicators, ensuring the appropriateness of the methodology and the accuracy of recommendations for improving risk management capabilities at the NTB Legislative Council. In addition, improvements to language consistency and removal of text repetition will be made.

D. Data Collection

An interview is a conversation that has a specific purpose, conducted directly either individually or in groups [4]. Data collection through interviews involved resource persons from the NTB Regional People's Representative Council (DPRD NTB) who were selected using purposive sampling method. With this method, the interviewees selected are those who have knowledge and expertise relevant to the research topic. The selection of the interviewees was based on their duties and responsibilities within the agency, especially those related to risk management, information security management, and data center development and operations. The data collected from these interviews became the main data in the research conducted [4]. The questionnaire was used as a tool that was distributed to ten selected respondents who were in accordance with the main duties and functions relevant to each process in COBIT 2019. The interview and questionnaire mechanism are carried out simultaneously, where the questionnaire contains an interview form, so that each respondent can directly answer the questions submitted in the form, while filling out the questionnaire. This is done based on the mapping of the COBIT 2019 process with the NIST 800-30 Framework. Questionnaire questions can be seen in the table below:

TABLE I. QUESTIONNAIRE QUESTION

No	Process Name	Questione
1.	BAI.09.02 – Managing critical assest	How can agencies identify critical assests for services, and how can they maximize their reliability abd avaibility?
2.	BAI.02.03 – Managing risk needs	How to identify, document, prioritize, and mitigate functional, technical, and information processing risks associated with agency needs and proposed solutions?
3.	APO.13.02 – Estabilish and manage information security and privacy risk treatment	How does the agency maintain an information security plan that describes the process by which information security risks are managed and aligned with agency strategy?
4.	APO.12.06 – Responding to risk	How does the agency respond to risk that occur in a timely manner with effective measures to limit the magnitude of losses?
5.	DSS.05.01 – Protect against malicious software	How the agency implements and maintains preventive, detective, and corrective measures (especially up-to-date security patches and virus control) across work units to protect information systems and technology from malicious software (e.g., ransomware, malware, viruses, worms, spyware, spam).
6.	DSS.05.03 – Manage endpoint security	How does the agency ensure that end-point devices (such as laptops, desktops, servers, network devices, and software) are secured to or exceed security requirements for information processed, stored, or transmitted?
7.	MEA.01.04 – Analyze and report on performance	How does the agency periodically review and report performance against targets, using methods that provide a concise overview of IT performance and are appropriate to the monitoring system used?
8.	MEA.01.03 – Collect and process performance data and its appropriateness	How to collect and process data in a timely and accurate manner that aligns with the agency's approach?
9.	EDM.02.04 – Monitor value optimization	How does the agency monitor targets and key indicators to ensure the expected value and benefits of I&T investments and services are being achieved, as well as identify significant issues and corrective actions required?
10.	EDM.02.03 – Provide direction for value optimization	How does the agency drive value management principles and practices to realize optimal value realization from I&T-related investments across its economic lifecycle?

In security risk management on the website of the NTB Regional People's Representative Council (DPRD), the selection of 10 COBIT 2019 domains is the result of considerations that take into account the greatest impact on information security sustainability. These domains were chosen because they have direct relevance to critical information security issues in government agencies, such as identification and management of critical assets, protection of malicious software, and operational risk management. A focus on these domains allows for more specific mitigation measures in areas that have a significant impact on information system continuity and security. In addition, these domains also cover fundamental aspects of risk management that are synergistic with the NIST 800-30 framework, which supports COBIT 2019's goal of maintaining operational effectiveness and compliance with information security standards. By limiting the domains to 10 key areas, risk analysis can be conducted in more depth and focus on risk mitigation that is most relevant to the infrastructure and operations of the NTB DPRD website. This domain selection considers efficiency and implementability, as selecting too many domains can be challenging in terms of resource allocation and management prioritization. By selecting domains that have a direct impact, management can formulate concrete and focused actions to continuously improve information security governance.

E. Data Processing and Analysis

Data processing is an advanced stage in this research series which is carried out after the data collection process. At this stage, the data that has been collected is processed or analyzed in order to produce relevant information to answer research questions.

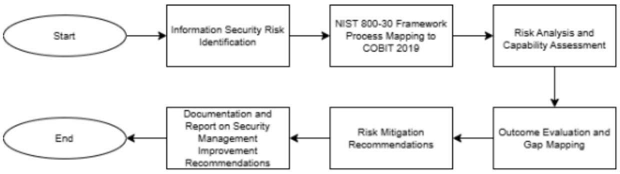
Start
Information Security Risk Identification
NIST 800-30 Framework Process Mapping to COBIT 2019
Risk Analysis and Capability Assessment
Outcome Evaluation and Gap Mapping
Risk Mitigation Recommendations
Documentation and Report on Security Management Improvement Recommendations
End

Figure 2. Data Processing and Analysis Process

The figure above illustrates the information security risk management process at DPRD NTB using the NIST 800-30 and COBIT 2019 frameworks. The process begins with the identification of information security risks to detect potential threats, followed by mapping the NIST 800-30 process to COBIT 2019 to ensure alignment between the two frameworks. Next, risk analysis and capability assessment were conducted using the Capability

Performance Management (CPM) method of COBIT 2019 to evaluate capability levels and identify gaps in risk management. After that, the evaluation results were used for gap mapping and determining areas that require improvement. Based on the mapping, risk mitigation recommendations were made which included increased security monitoring, policy updates and staff training. The process concludes with documentation and an improvement recommendation report containing corrective measures and suggestions for ongoing audits and training to ensure the effectiveness of security risk management. The results of data analysis can be presented in the form of graphs or diagrams, which illustrate the level of fulfillment of the implementation of the NIST 800-30 framework based on the processes contained in COBIT 2019.

Process capability assessment is carried out in stages, where each level must be fully achieved before proceeding to the next level. In the capability assessment based on COBIT 2019, the evaluation starts from level 2 because it is assumed that the agency has carried out the required activities at the previous level [11].

Processing of questionnaire data to determine the level of COBIT 2019 capability is carried out using the formula below, which aims to accurately evaluate the achievement of each activity. The results provide a comprehensive picture of the fulfillment of standards in the 2019 COBIT framework.

1) Calculation of the percentage of capability level 1 activities per objective

$$\text{Activity Percentage} = \frac{Activities\ Performed}{Total\ Activities} \times 100\%$$

2) Calculation of the percentage of output capability level 1 per objective

$$\text{Output percentage} = \frac{Defined\ Output}{Total\ Output} \times 100\%$$

3) Calculation of the percentage of process outcome level 1 per objective

$$\text{Outcome Process Percentage} = \frac{Activity\ Percentage + Outpu\ Percentage}{2} \times 100\%$$

4) Calculation of the percentage of capability attribute processes per level, level 2 to level 5

$$\text{Attribute Process Percentage} = \frac{Attribute\ Processes\ Executed}{Total\ Attribute\ Processes} \times 100\%$$

TABLE II. RATING LEVELS

Abberviation	Description	%Achieved
N	Not Achieved	0% - 15% achievement
P	Partially Achieved	>15% - 50% achievement
L	Largely Achieved	>50% - 85% achievement
F	Fully Achieved	>85% - 100% achievement

Based on the rating levels and capability levels used in the evaluation process, the mapping results are as follows:

TABLE III. CAPABILITY LEVEL PROCESS ASSESMENT MODEL

Capability level Process Assesment Model	1	2	3	4	5
Level 0 Incomplete					
Level 1 Performed	L/F	F	F	F	F
Level 2 Managed		L/F	F	F	F
Level 3 Estabilished			L/F	F	F
Level 4 Predictable				L/F	F
Level 5 Optimizing					L/F

The capability level can be considered achieved when a process is already in the Largely Achieved (L) category. If all processes have reached Fully Achieved (F) status, then the assessment can proceed to the next level.

The COBIT 2019 framework is used to ensure that the information security governance of the NTB Legislative Council's information system is optimized. Through mapping with NIST 800-30, some of the main domains that are prioritized in risk management include BAI, APO, DSS, EDM and MEA, with a focus on improving security controls and more effective risk mitigation. Improvements in these areas will strengthen risk management and ensure better protection against threats that can damage system integrity. Can be seen in the table below:

TABLE IV. COBIT FRAMEWORK PROCESS MAPPING

No	Domain	Description	Percentage COBIT Fulfilment (%)
1.	BAI.09.02	Managing critical assests	50%
2.	BAI.02.03	Managing risk needs	55%
3.	APO.13.02	Information security plan	70%
4.	APO.12.06	Responding to risk	50%
5.	DSS.05.01	Malicious software protection	85%
6.	DSS.05.03	End-point security	65%
7.	MEA.01.04	Performance reporting	40%
8.	MEA.01.03	Performance data collection	45%
9.	EDM.02.04	Performance score monitoring	60%
10.	EDM.02.03	Value Optimization Briefing	50%

The mapping of the fulfillment of the COBIT 2019 framework in managing information security risks at the NTB DPRD reveals critical compliance levels across various domains, highlighting urgent needs for improvement. In the EDM domain, subprocesses EDM.02.04 and EDM.02.03 show 60% and 50% compliance, respectively, suggesting that enhanced performance monitoring and optimization will reduce IT inefficiencies. Similarly, in the BAI domain, subprocesses BAI.09.02 and BAI.02.03 demonstrate 50% and 55% compliance, indicating a need for better protection of critical assets and risk management. The DSS domain's focus on endpoint security and malware protection requires immediate attention to mitigate potential service disruptions, while the APO domain highlights the necessity for stronger information security planning to bolster asset protection. The MEA domain, with its lowest results in reporting and data collection, underscores the urgency for improvements to ensure accurate performance data for informed decision-making. Failure to address these areas may lead to operational inefficiencies and unpreparedness against threats, adversely affecting the sustainability and reliability of public services; therefore, prioritizing these improvements is essential for strengthening risk management and enhancing operational effectiveness in accordance with COBIT 2019 standards.

F. Recomendation

Recommendations describe and set priorities for actions that need to be taken. This stage is the final result of the *capability* level assessment and the level of capability that the institution wants to achieve. The results of this Recommendation set the priority steps that must be taken immediately by the NTB DPRD to strengthen information security risk management. Based on the results of the assessment with the NIST 800-30 and COBIT 2019 frameworks, the proposed mitigation measures are focused on closing gaps in the management of identified security risks and controls. The analysis highlighted key threats such as DDoS, XSS and malware, which require rapid response and more intensive protection. By strengthening protection against these threats, NTB Council can mitigate significant impacts that could potentially disrupt services and data security.

In addition, increased monitoring and maintenance of digital assets should be a priority to ensure continuity of system protection. This recommendation also serves as a reference in establishing more solid risk governance, in line with the agency's expected capabilities. Stricter implementation of security controls and increased cyber awareness among staff will strengthen overall system resilience, enabling faster and more appropriate responses to evolving threats. Effective implementation of these recommendations will not only ensure better data security, but also support the smooth operation and achievement of the NTB Legislative Council's strategic objectives, as well as reduce potential losses due to future cyberattacks.

IV. Result

This research was conducted following the flow in Chapter III. The approach used in this research aims to integrate the NIST 800-30 information security framework and IT governance through COBIT 2019 based on questionnaire data and interviews that have been conducted previously to the agency, with the following steps:

A. Identification of Information Security Risks on the NTB DPRD Website

In this research, the risk identification process is carried out based on the NIST 800-30 framework, which serves to identify potential threats and vulnerabilities in the information system of the West Nusa Tenggara Regional House of Representatives (DPRD NTB) website. This process involves a thorough analysis of factors that can affect information security, including technical and operational aspects. The assessment took into account the reliance on third-party network infrastructure, which may carry additional risks, as well as the physical condition of the data center which may not be adequate to support optimal security. In addition, interviews with DPRD NTB IT technicians revealed that there are current technical constraints that could potentially disrupt website security, such as frequent Distributed Denial of Service attacks caused by a lack of routine system maintenance, required software updates, and constrained servers located at third parties. With this approach, risk identification aims to provide a clear picture of the challenges faced and a solid basis for the development of appropriate mitigation strategies. For risk identification can be seen in the table below:

TABLE V. IDENTIFICATION OF INFORMATION SECURITY RISKS ON THE NTB DPRD WEBSITE

No	Type of threat	Risk Level	Impact	Frequen	Current Avaibility of Control
1.	Deface	Medium	Danage ti wesute appeaance, danage to reputation	Rare (occurs 1-3 times a year)	Medium
2.	Malware	Low	Data loss, theft of sensitive information	Medium (detected 1-2 times a year)	Medium
3.	SQL Injection	Low	Illegal access to databases, data theft	Very rare (occurs 0-1 times a year)	High
4.	Cross-Site Scripting (XSS)	High	Web interface manipulation, theft of user information	Frequent (occurs several times a year)	High
5.	Distributed Denial of Service (DDoS)	High	Interrupted access to website, significant downtime	Frequent (occurs several times a year)	Medium
6.	IDOR (Insecure Direct Object Reference)	Medium	Immediate access to sensitive data, alteration or deletion of data	Medium (occurs 1-3 times a year)	Medium
7.	Human Error	Medium	Downtime, security misconfiguraton	Medium (occurs 1-3 times a year)	Medium

Based on the results of risk identification on the NTB DPRD website, it shows the specific threats that often occur and the impact they can have, so that it can guide the prioritization of security measures that must be taken. In the context of this research, this risk analysis provides a clearer understanding of vulnerable areas and the need for improved controls on high-risk threats, such as DDoS and XSS. These two threats not only disrupt service availability but also have the potential to lower public trust if user data is exposed.

The importance of this result lies in identifying the urgent need to improve protection at critical points, for example by strengthening firewalls against DDoS attacks and implementing input sanitization to prevent XSS. In addition, medium-risk threats such as deface and malware still need attention to prevent them from developing into higher risks. The impact on information system security is a reduction in the likelihood of security incidents that could disrupt website operations or cause data loss. By understanding this risk profile, NTB Legislative Council can more effectively design a proactive security strategy that focuses on prevention, maintaining the integrity and availability of their information systems.

B. NIST 800-30 Framework Process Mapping

In an effort to improve information security governance, it is important to conduct a mapping between the NIST 800-30 and COBIT 2019 subcategories. This mapping aims to identify and evaluate the level of risk management capability that exists within the agency. By referring to the NIST 800-30 framework, agencies can understand the vulnerabilities they may face and the mitigation measures that need to be implemented. On the other hand, COBIT 2019 provides guidance related to good IT governance and management, so this mapping serves as an effective tool to evaluate performance and identify areas of improvement needed.

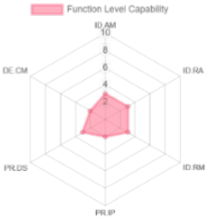

Figure 3. Capability Level in Each Function of the NIST Information Security Framework at the NTB Regional Representative Council

Based on the capability diagram above, the capability level of the information security framework function in this agency is mostly at level 3, especially in the *Asset Management* (ID.AM) and *Risk Assessment* (ID.RA) functions, which shows that the risk management process is quite good and structured. However, there are several functions that are still at level 2, such as *Information Protection* (PR.IP) and *Continuous Monitoring* (DE.CM). This indicates that despite mitigation efforts, capabilities in these areas are still not fully mature. For this reason, agencies need to strengthen incident management and cybersecurity monitoring to achieve higher capabilities.

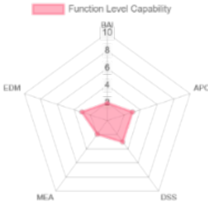

Figure 4. Capability Level of Information Security Function Based on COBIT 2019 at the NTB Regional Representative Council

This figure shows the capability level of various functions in the COBIT 2019 framework at an agency. Of the five domains evaluated, it can be seen that all functions, including APO (Align, Plan, Organize), DSS (Deliver, Service, and Support), MEA (Monitor, Evaluate, and Assess), BAI (Build, Acquire, and Implement), and EDM (Evaluate, Direct, and Monitor), are at level 3 capability level. This indicates that processes within the agency have been managed and regulated, although they still require improvement to achieve a more mature capability. This evaluation provides an overview of the areas that need to be strengthened so that agencies can improve information technology governance more optimally.

This mapping between NIST 800-30 and COBIT 2019 in this study shows that both frameworks are effective in managing information security risks on the NTB DPRD website with a complementary approach. COBIT 2019 provides a structured governance framework, supporting oversight and policy adjustments through consistent asset management and risk response processes, thus helping to maintain system integrity. NIST 800-30 reinforces the technical aspects with detailed guidance for the identification and mitigation of specific threats, such as DDoS and XSS attacks, enabling a more proactive response. The effectiveness of both is seen in the ability to combine risk management at the technical and governance levels, which makes institutions better prepared to face complex digital threats with a comprehensive and targeted approach.

TABLE VI. MAPPING NIST 800-30 SUBCATEGORIES TO COBIT 2019 PROCESSES

NIST	Aspects	Subcategories based on NIST	Cobit 2019
ID.AM-1	Critical Asset Management	Physical devices and systems within the agency were inventoried	BAI09.01
ID.RA-1	General Risk Management	Asset vulnerabilities are identified and documented	DSS.05.01
ID.RA-2	Response to Cyber Threats	Threat and vulnerability information is received from forums and informationsharing sources	APO12.06
ID.RM-2	General Risk Management	Agency risk tolerance is defined and clearly stated	APO13.02
PR.IP-5	Information and Technology Protection	Policies and regulations regarding the physical operating environment for agency assets are met	BAI02.03
PR.IP-12	General Risk Management	Vulnerability management plan developed and implemented.	DSS.05.01
PR.IP-9	Response to Information Security Risks	Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed.	APO12.06
PR.DS-2	Information and Technology Protection	Data in transit is protected.	DSS.05.03
PR.IP-8	Information and Technology Protection	The effectiveness of protection technologies is shared with the right parties.	MEA01.04
DE.CM-1	Risk Monitoring	Networks are monitored to detect potential cybersecurity events	MEA01.03

Can be seen in the table above is a presentation of the mapping between the subcategories of NIST 800-30 and the processes in COBIT 2019, which aim to improve information security governance in agencies. Each description reflects an important aspect of risk management, while references to COBIT 2019 indicate the integration of these measures in the IT management framework. For example, ID.AM-1 (Asset Management) emphasizes the inventory of physical devices, while ID.RA-1 (Risk Assessment) focuses on the identification and documentation of asset vulnerabilities. ID.RM-2 (Risk Management) emphasizes the importance of setting clear risk tolerances. In addition, PR.IP-5 (Information Protection) deals with the fulfillment of policies that protect assets, and PR.IP-12 (Vulnerability Management) indicates the need for an effective vulnerability management plan. PR.IP-9 (Incident Response) highlights the importance of incident response plans, while PR.DS-2 (Data Protection) ensures the protection of data in transit. Finally, DE.CM-1 (Continuous Monitoring) covers network monitoring practices to detect potential threats.

The mapping of NIST 800-30 subcategories to COBIT 2019 processes in this study shows that the two frameworks complement each other in strengthening information security at the NTB DPRD. For example, the ID.AM-1 (Asset Management) and ID.RA-1 (Risk Assessment) subcategories of NIST 800-30 that focus on asset inventory and vulnerability identification are implemented through the BAI09.01 and DSS.05.01 processes in COBIT 2019, showing the importance of good asset management as a basis for risk mitigation, in line with Supristiowadi and Kurniati's findings. In addition, continuous monitoring DE.CM-1 in NIST 800-30, represented by MEA01.03 in COBIT 2019, enhances threat detection through proactive monitoring, as indicated by Tjahjono on the importance of early detection. These results are consistent with literature stating that a combination of governance such as COBIT and technical guidance such as NIST strengthens risk controls; Vatresia emphasizes that COBIT directs security strategy, while NIST strengthens operational controls. Thus, this mapping helps NTB Regional Council design a structured mitigation strategy and enables a holistic evaluation of risk management, according to information security best practices in the public sector to maintain public trust and service sustainability.

The COBIT 2019 framework is used to ensure that information security governance in the NTB DPRD information system runs optimally. Through mapping with NIST 800-30, some of the main domains that are prioritized in risk management include BAI, APO, DSS, EDM and MEA, with a focus on improving security controls and more effective risk mitigation. Improvements in these areas will strengthen risk management and ensure better protection against threats that can undermine system integrity.

TABLE VII. NIST 800-30 SUBCATEGORY GAP ASSESSMENT

NIST subcategory	COBIT	Capability (NIST)	Capability (COBIT)
ID.AM-1	BAI09.01	3	3
ID.RA-1	DSS.05.01	3	4
ID.RA-2	APO12.06	3	3
ID.RM-2	APO13.02	3	3
PR.IP-5	BAI02.03	3	2
PR.IP-12	DSS.05.01	2	3
PR.IP-9	APO12.06	3	3
PR.DS-2	DSS.05.03	3	3
PR.IP-8	MEA01.04	2	2
DE.CM-1	MEA01.03	2	3

The table above evaluates the gap between NIST 800-30 subcategories and COBIT 2019 processes in the NTB Legislative Council, highlighting areas that require improvement to achieve capability parity between the two frameworks. Most subcategories, such as ID.AM-1 (Asset Management) and ID.RA-1 (Risk Identification), are at level 3, signifying a good structure. However, some areas such as PR.IP-5 (Physical Information Protection) at level 2 in COBIT indicate the need for strengthening physical security, while PR.IP-12 (Vulnerability Management) at level 2 in NIST confirms the need for improvement in vulnerability management. These results are consistent with the literature, such as Supristiowadi's research highlighting the importance of asset management for risk mitigation, Tjahjono supporting continuous monitoring as the key to early detection of cyber threats, and Vatresia showing that the combination of NIST and COBIT supports comprehensive risk management in the public sector. Overall, the literature corroborates the finding that improvements in the identified areas can strengthen risk management in the NTB Regional House of Representatives.

C. Risk Analysis

Based on the risk analysis with NIST 800-30 and COBIT 2019, the main threats on the NTB DPRD website are DDoS and XSS attacks with high risks that occur frequently and have a significant impact on service availability and potential data theft. In the NIST framework, domain ID.RA-1 (Risk Assessment) highlights the importance of early detection and mitigation, while ID.AM-1 (Asset Management) emphasizes asset inventory and maintenance to reduce security gaps. In terms of COBIT 2019, DSS05 (Protection against malicious software) and BAI09 (Management of critical assets) point to the need for improved response to high-risk threats. Deficiencies in MEA01 (Monitoring and Evaluation) in terms of monitoring frequency slow down early detection of threats, indicating that improving the frequency and quality of monitoring and risk reporting will strengthen detection and response capabilities to cyber threats.

These results suggest that the combination of the NIST and COBIT frameworks helps create a holistic approach to managing information security risks, with NIST focusing on technical controls and threat detection, and COBIT supporting more strategic oversight and governance. potentially, the NTB Regional Council needs to improve monitoring and reporting of risks on a regular basis to evaluate the effectiveness of controls and identify areas that require immediate improvement. The research also revealed that improving risk management capabilities, including reviewing procedures and training staff, will strengthen agencies' ability to deal with evolving cyber threats. By implementing more comprehensive and proactive mitigation strategies, the NTB Regional House of Representatives can protect its information assets and maintain public confidence in the security of their services.

D. Recomendation

Based on the results of the analysis, the following recommendations are designed to assist the NTB Legislative Council in addressing the risks identified, strengthening existing security controls, and increasing the resilience of information systems against possible threats. Implementation of these recommendations is expected to improve the effectiveness of risk management, ensure better data protection, and support the achievement of overall agency goals:

TABLE IX. INFORMATION SECURITY RECOMENDATIONS ON THE NTB DPRD WEBSITE

No	NIST Subcategory	COBIT Subcategory	Gap	Recomendation
1.	ID.AM-1	BAI09.01	0	No additional action is required as the process meets the standard. Focus on maintaining a regular inventory of devices.
2.	ID.RA-1	DSS.05.01	-1	Improve the process of identifying and documenting asset vulnerabilities by developing a more efficient reporting system. Conduct regular vulnerability audits to update potential threats.
3.	ID.RA-2	APO12.06	0	Process is adequate. Continue to engage in information-sharing forums on threats and vulnerabilities, and improve access to relevant sources of information.
4.	ID.RM-2	APO13.02	0	No gap. Maintain established risk tolerance and conduct periodic review of risk management policies.
5.	PR.IP-5	BAI02.03	-1	The implementation of physical and operational safeguards needs to be strengthened by regularly updating physical security policies, as well as monitoring access to critical facilities
6.	PR.IP-12	DSS.05.01	-1	The vulnerability management plan needs to be updated and documented in more detail. Ensure training for staff on vulnerability management.
7.	PR.IP-9	APO12.06	0	The incident response and recovery process is well managed, but regular simulations and trials are needed to test the effectiveness of the plan.
8.	PR.DS-2	DSS.05.03	0	There is no gap. Data protection processes in transit are adequate, but could be improved with stronger data encryption and additional security technologies.
9.	PR.IP-8	MEA01.04	0	Maintain the effectiveness of protection technologies and continue to share information on protection measures with interested parties.
10.	DE.CM-1	MEA01.03	-1	Increase the frequency and scope of network monitoring with more advanced monitoring technology and training for cybersecurity teams to detect potential threats quickly.

The table above shows the information security recommendations for the NTB DPRD website based on the evaluation of the gap between the NIST 800-30 subcategories and the COBIT 2019 process. This gap indicates differences in capability levels, such as in subcategory ID.RA-1 (DSS.05.01) which has a gap of -1, where the NIST capability is worth 3 while COBIT is worth 4. This means that improvements are needed in the process of identifying and documenting asset vulnerabilities to achieve higher capability standards. This recommendation guides the NTB Legislative Council in prioritizing improvements, for example, updating the physical security policy in subcategory PR.IP-5. This evaluation shows that COBIT 2019 supports overall governance, while NIST 800-30 focuses on technical security, so the combination of the two results in more effective and integrated risk mitigation.

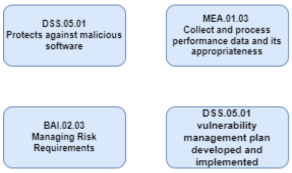
DSS.05.01
Protects against malicious software
MEA.01.03
Collect and process performance data and its appropriateness
BAI.02.03
Managing Risk Requirements
DSS.05.01
vulnerability management plan developed and implemented

Figure 4. COBIT 2019 Recommendations that Must be Improved

Based on the figure shown, there are four subprocesses within the COBIT 2019 framework that are recommended for improvement at DPRD NTB. These include DSS.05.01, which focuses on protecting against malicious software and developing a robust vulnerability management plan; BAI.02.03, related to managing risk requirements to identify, evaluate, and address potential security risks proactively; and MEA.01.03, which emphasizes the importance of enhancing data collection and performance processing for informed decision-making. Improving these subprocesses is critical, as they serve as the backbone for effective risk governance and operational resilience. By prioritizing these areas, DPRD NTB can significantly reduce its vulnerability to cyber threats, ensure compliance with security standards, and foster a culture of continuous improvement in information security management. Such enhancements will ultimately lead to better resource allocation and a more strategic approach to managing and mitigating risks, enabling DPRD NTB to safeguard its information assets and maintain public trust.

V. Conclusion

The results of this study indicate that the information security risk management capability of the NTB DPRD website still has significant weaknesses, especially against critical threats such as cross-site scripting (XSS) and Distributed Denial of Service (DDoS). Mapping using COBIT 2019 and NIST 800-30 identified gaps in several important areas, including malicious software protection (DSS.05.01), risk requirements management (BAI.02.03), and vulnerability management (DSS.05.01), indicating the need for improvement in these areas. The study recommends the adoption of more effective security technologies, increased training and security awareness for staff, and periodic strengthening of audit and risk management processes. For future research, it is recommended to focus on measuring the effectiveness of implemented controls as well as exploring new technologies such as artificial intelligence (AI) in cyber threat mitigation. With these measures, the NTB Legislative Council is expected to strengthen its defenses against existing threats and improve the resilience of its information systems in accordance with technological developments.

References

[1] Y. Suherman, M. Informatika, and A. Jayanusa, “JURNAL RESTI (Rekayasa Sistem dan Teknologi I nformasi) Sistem Informasi Kearsipan Tata Kelola Surat Pada Kantor Inspeksi BRI Kota Padang”,

[2] E. Surya Negara, J. Jenderal Ahmad Yani No, K. I. Seberang Ulu, K. Palembang, and S. Selatan, “Manajemen Risiko Divisi Sistem Informasi Pada Universitas Bina Insan Menggunakan Framework Cobit 5 Risk Management Information Systems Division at Bina Insan University Using the Cobit 5 Framework,” *Cogito Smart Journal* |, vol. 8, no. 2.

[3] I Nyoman Rai Widartha Kesuma, Hermadi Irman, and Nurhadryani Yani, “EVALUASI TATA KELOLA TEKNOLOGI INFORMASI DI DINAS PERTANIAN GIANYAR MENGGUNAKAN COBIT 2019,” *Jurnal Teknologi Informasi dan Ilmu Komputer*, vol. 10, pp. 513–522, 2023.

[4] R. Putra, “Manajemen Risiko Keamanan Informasi: Studi Kasus Pusat Data Dinas XYZ,” *The Indonesian Journal of Computer Science*, vol. 13, no. 4, Jul. 2024, doi: 10.33022/ijcs.v13i4.4129.

[5] B. A. Nugraha, A. R. Perdanakusuma, and A. Rachmadi, “Analisa Manajemen Risiko pada Sistem Informasi Tata Naskah Dinas Elektronik dengan Kerangka Kerja NIST 800-30 pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur,” 2020. [Online]. Available: http://j-ptiik.ub.ac.id

[6] A. Muchsinul, H. M. Jamil, A. Rachmadi, and A. R. Perdanakusuma, “Evaluasi Manajemen dan Tatakelola Teknologi Informasi pada Dinas Kominfo Kota Malang dengan menggunakan Framework Cobit 2019,” 2021. [Online]. Available: http://j-ptiik.ub.ac.id

[7] D. Trihapningsari, A. R. Dewi, L. Y. Banowosari, and P. Korespondensi, “PENGUKURAN KAPABILITAS TATA KELOLA TI SISTEM INFORMASI TIRAS DAN TRANSAKSI BAHAN AJAR UNIVERSITAS TERBUKA MENGGUNAKAN COBIT 5 IT GOVERNANCE CAPABILITY MEASUREMENT USING COBIT 5 FRAMEWORK (CASE STUDY: INFORMATION SYSTEM OF TIRAS AND TEACHING MATERIALS TRANSACTIONS IN UNIVERSITAS TERBUKA)”, doi: 10.25126/jtiik.202184648.

[8] A. Vatresia, P. Nicholas, P. Tambunan, and A. Erlansari, “AUDIT SISTEM INFORMASI PADA SISTEM MANAJAMEN LAYANAN SATU ATAP (SIMANTAP) MENGGUNAKAN KERANGKA COBIT 5.0 (STUDI KASUS: BANK INDONESIA PROVINSI BENGKULU)”, doi: 10.25126/jtiik.202295792.

[9] B. Tjahjono, M. Ardiansyah, ; Gerry Firmansyah, and H. Akbar, “RISK MANAGEMENT OF INFORMATION SYSTEM IN DISKOMINFO STATISTIC AND ENCODING USING NIST SP 800-30id 4 (*) Corresponding Author (Responsible for the Quality of Paper Content),” vol. 9, no. 1, 2023, doi: 10.33480/jitk.v9i1.4080.

[10] U. Literatur Sistematis, A. Kurniati, L. Edi Nugroho, M. Nur Rizal, M. Jalan Grafika, and K. Ugm, “Manajemen Risiko Teknologi Informasi pada e-Government: Information Technology Risk Management on e-Government: Systematic Literature Review.”

[11] R. Ayunda Sari, “Evaluation of IT Risk Management in DISKOMINFO of Magelang Regency using COBIT Framework 2019 Objectve EDM03 & APO12,” *Jurnal Informatika dan Teknologi Informasi*, vol. 20, no. 3, pp. 442–456, 2023, doi: 10.31515/telematika.v20i3.11867.