Indonesian Interdisciplinary Journal of Sharia Economics (IIJSE) Vol. 7. No. 1 (2024)
e-ISSN: 2621-606X Page: 1331-1353

DEVELOPMENT OF AN INTEGRATED IT RISK MANAGEMENT FRAMEWORK FOR ELECTRONIC-BASED GOVERNMENT SYSTEMS: A CASE STUDY OF THE XYZ MINISTRY

Irfan Erfian Nurdin [1]
Bina Nusantara University, Jakarta Pusat, Indonesia
irfan.nurdin@binus.ac.id

Benfano Soewito [2]
Bina Nusantara University, Jakarta Pusat, Indonesia

Abstract

This study establishes a robust IT risk management and governance framework for The XYZ Ministry. The design combines ISO 31000 and NIST SP 800-30 methodologies, tailored for electronic-based government systems and alignment with regulatory mandates. The research emphasizes improved IT risk management, incident response, and disaster recovery, targeting optimal electronic-based government operations. Adapting this model offers solutions for central and local government entities. Using ISO 31000 and NIST SP 800-30 revision 1, a risk priority matrix was produced, showcasing the relationship between assets and threats, and identifying varying risk levels. Specifically, the most significant risk at The XYZ Ministry was outdated policies. This risk is due to the slow adaptation to central government regulations and current IT standards. This highlights the need for the ministry to incorporate risk management outcomes into its IT governance, essential for risk mitigation and strategic alignment with government directives.

Keywords: IT Risk Management, Electronic Government System, SPBE index

INTRODUCTION

The use of Information Technology (IT) has become essential for both government and private organizations in enhancing the effectiveness and efficiency of business performance (Marchiori *et al.* 2023). However, the planning, implementation, and operational maintenance of IT in an organization requires significant investments in terms of finances, time, and other resources (Fikri 2019). IT has evolved from being a mere operational tool to a decision-making tool that contributes to the organization's survival and goal achievement. Nevertheless, the use of IT also comes with potential risks that organizations need to address (Settembre-Blundo et al. 2021).

The XYZ Ministry is a governmental institution entrusted with the crucial task of national development planning, thereby actively contributing to the efficient governance of the nation under the leadership of the President. To effectively discharge its responsibilities, the ministry has adopted state-of-the-art Information Technology (IT) systems to optimize its services internally and externally, in strict compliance with the Electronic-Based Government Systems (SPBE) guidelines. Consequently, the management of the IT infrastructure must be dedicated to upholding the pillars of confidentiality, availability, and security (Lee, Neeley, and Stewart 2021).

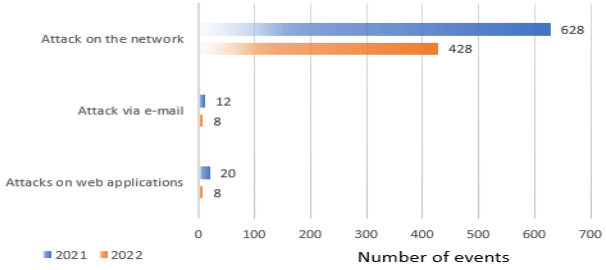

Figure 1
Stat of cyber-attack at The XYZ Ministry (Kementerian PAN RB 2022)

However, The XYZ Ministry has encountered IT security incidents in recent years, such as SQL injection attacks in 2021 an phishing email attacks in 2022. These incidents disrupted online services temporarily and highlighted the need for improved security measures and risk management practices. Furthermore, the ministry faces challenges in implementing the SPBE due to the lack of internal policies on IT risk management and IT audit aspects (Kementerian PAN RB 2022)

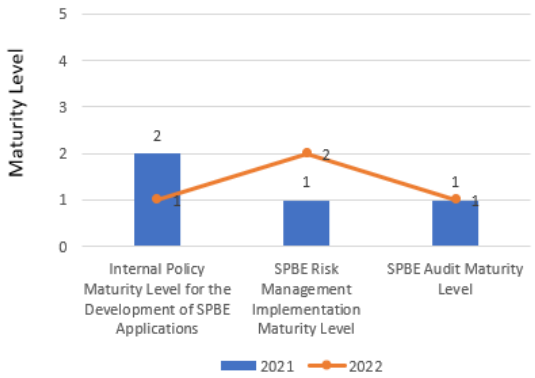

Figure 2
SPBE Index of The XYZ Ministry (Kementerian PAN RB 2022)

In response to these challenges, The XYZ Ministry requires appropriate IT risk management and governance to mitigate the potential risks and enhance its SPBE index. The ministry seeks guidance and reference materials that are easy to understand and implement to prevent and reduce similar risks. Although there is already a guideline for IT risk management in the government sector, as outlined in the Minister of State Apparatus Empowerment and Bureaucratic Reform Regulation No. 5 of 2020, its implementation across all government agencies remains limited due to its general nature. Private sectors often rely on other references, such as COBIT (Control Objective for Information Technology and Related Technology), ISO (International Standard Organization) 31000, and NIST (National Institute of Standards and Technology) Special Publication (SP) 800-30, to develop IT risk management guidelines.

Previous studies have proposed various methods for managing IT risks, such as implementing the Project Management Body of Knowledge (PMBOK) and ISO 31000 (Iin 2017), and combining ISO 27005 and NIST SP 800-30 revision 1 in profit organizations (Fikri 2019). Building upon previous research, this study aims to analyze and determine IT governance risks at The XYZ Ministry using a combination of ISO 31000 and NIST SP 800-30 frameworks, considering the guidelines of the Minister of State Apparatus Empowerment and Bureaucratic Reform Regulation No. 5 of 2020. Additionally, the study aims to develop an appropriate incident response plan for the ministry.

The research objectives include obtaining a list of IT governance risks as a guide for implementing risk management in The XYZ Ministry and providing recommendations for

an effective incident response plan. The study aims to contribute to the field of knowledge by developing a risk management model that combines ISO 31000 and NIST SP 800-30 frameworks, aligned with the requirements of the Minister of State Apparatus Empowerment and Bureaucratic Reform Regulation No. 5 of 2020, applicable to central and local government institutions.

The scope of this research is delimited exclusively to The XYZ Ministry and does not encompass other governmental entities. This study bears significant implications as it assists the ministry in enhancing its IT risk management practices, mitigating potential risks, and augmenting the efficacy and efficiency of its services in the digital age. Through the assimilation of globally acknowledged frameworks and guidelines, the ministry can fortify its IT governance and guarantee the uninterrupted functionality of its operations when confronted with IT-related challenges.

REVIEW OF LITERATURE

Risk Management

Research on the implementation of risk management standards in e-government has been conducted, focusing on various aspects such as IT project risk management, software lifecycle, information security, cloud computing, and e-government risk management maturity level. The standards commonly used in these implementations include ISO 31000-series, ISO 27000-series, NIST SP 800-301, and COBIT (Abied et al. 2022).

Several studies have shown that the implementation of ISO 31000 standards can help in IT project risk management and enhance software lifecycle effectiveness. Meanwhile, ISO 27000-series is utilized in information security risk management, particularly in the context of cloud computing. COBIT is also applied in e-government governance to measure maturity level and improve accountability and transparency (Agung 2019).

In the assessment of information security risks, a combination of standards such as ISO 27005 and NIST SP 800-301 is widely applied. Research also indicates the need for an appropriate and accurate taxonomy or risk assessment method to address challenges in the information security risk assessment process (Akkiyat et al. 2019).

Incorporating risk management standards into organizations is perceived as a highly adaptable approach, as it can be customized to align with the specific conditions and

requirements of the organization. The utilization of Design Science Research Methodology (DSRM) frequently plays a pivotal role in the risk assessment process, facilitating the development of inventive models or methodologies, as noted by Barafort et al. in 2018 (Settembre-Blundo et al. 2021).

This approach not only allows organizations to tailor their risk management practices to their unique operational landscape but also empowers them to adapt to evolving challenges in a dynamic business environment. As a result, this flexible framework contributes significantly to enhancing overall risk management effectiveness and resilience(Allioui and Mourdi 2023).

Overall, risk management plays a crucial role in organizations by systematically assessing, managing, and addressing risks. Risk management standards such as ISO 31000-series, ISO 27000-series, NIST SP 800-301, and COBIT can be used as references in the risk assessment process, with the integration of other standards and modifications based on organizational needs.

ISO 31000

One study by Hurin in titled *"Manajemen Risiko Teknologi Informasi Pada proyek Perusahaan XYZ Melalui Kombinasi COBIT, PMBOK, and ISO 31000"* (2017) explored the implementation of ISO 31000 alongside COBIT and PMBOK as a combined risk management approach for IT projects at Company XYZ. The research found that the integration of ISO 31000 guidelines helped address various issues in the IT unit, such as incomplete design specifications, multiple design revisions, unreadable design files, and errors in material requirement calculations (Gordon *et al.* 2020). The study concluded that the overall survey conducted after the research was beneficial to the company, as the detailed risk management guidelines obtained from ISO 31000 were easily understood by stakeholders, aiding in mitigating IT risks (Gordon et al. 2020).

Additionally, Fazlida's study titled "Information Security: Risk, Governance, and Implementation Setback" (2015) highlighted the importance of integrating ISO 27001, which is based on ISO 31000 principles, into information security governance (Brunner *et al.* 2020). The research emphasized that ISO 31000 provides a valuable foundation for risk management in information security and, when integrated with ISO 27001, can enhance the implementation of information security governance within an organization. It suggested that

attention from top management, clear communication of information security measures, stakeholder involvement in policy formulation, and the recognition of the added value of implementing information security governance are essential for successful integration (Brunner *et al.* 2020).

NIST Cybersecurity Framework

In a comparative study by N. Alhojailan, M. Alghamdi, and M. Alghamdi titled "Risk Management for Small and Medium-Sized Enterprises: A Comparative Study of ISO/IEC 27001 and NIST Cybersecurity Framework" (2021), the researchers analyzed the benefits and limitations of both frameworks for risk management in small and medium-sized enterprises. The study highlighted the importance of the NIST Cybersecurity Framework in addressing the unique vulnerabilities faced by SMEs due to limited resources and lack of cybersecurity awareness. The research concluded that the NIST framework offers practical guidance to enhance cybersecurity measures and protect against cyber threats in SMEs.

Furthermore, another study by A. Dominguez, L. García-Sánchez, and M. Martin, titled "Integrating the ISO/IEC 27001 and NIST Cybersecurity Framework for Effective IT Risk Management" (2022), emphasized the benefits of integrating the ISO/IEC 27001 and NIST Cybersecurity Framework for IT risk management. The researchers suggested that the combination of both frameworks provides a comprehensive approach to risk management, leveraging the risk assessment capabilities of ISO/IEC 27001 and the specific cybersecurity controls provided by the NIST framework. The study highlighted the advantages of this integration, including improved risk assessment, stronger security controls, and better alignment between IT operations and business objectives.

These related works demonstrate the utilization and benefits of ISO 31000 and the NIST Cybersecurity Framework in various contexts, providing insights into their effectiveness and the value they bring to organizations in managing IT risks and enhancing information security practices.

RESEARCH METHOD

In this study, the authors will assess risks and propose enhancements to ICT services at The XYZ Ministry. The research process is divided into seven steps, which include conducting a literature review, comparing and selecting framework combinations, collecting

data, analyzing and formulating risk management recommendations based on the chosen frameworks, analyzing and creating an incident response plan, and finally evaluating the outcomes and providing suggestions:

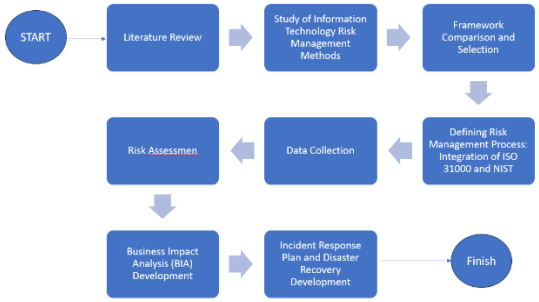

Figure 3
Research Metodology

Literature Review

Literature review is the process of collecting information by referring to previously documented sources such as theories and methods that will be needed in this research. The literature review aims to delve into all the information related to this research.

Study of Information Technology Risk Management Methods

This study will be conducted by gathering information on the risk management process in each framework to be used. It will also study the NIST 800-34 Contingency Planning Guide for Federal Information Systems, which will be used to recommend the development of an incident response plan and disaster recovery plan.

Framework Comparison and Selection

This stage involves analyzing several framework methods mentioned earlier, namely ISO 31000 and NIST SP 800-30, while considering the Minister of Administrative and Bureaucratic Reform Regulation No. 5 of 2020 on Guidelines for Electronic Government System Risk Management. According to a previous study titled "Towards a New Approach for Combining IT Frameworks," the study combined several methods by comparing the processes of each framework. The comparison aims to find the best method for each information technology risk management process to be conducted.

Defining Risk Management Process: Integration of ISO 31000 and NIST

By integrating ISO 31000 and NIST, organizations can benefit from a comprehensive risk management process that encompasses a broad range of risks, with a specific focus on IT and cybersecurity. This integration enhances the organization's ability to identify, analyze,

evaluate, treat, and monitor risks, leading to a more robust and effective risk management approach.

Data Collection

This stage involves the collection of information and data in the field through the creation of a list of information technology issues related to the operationalization and security of applications in The XYZ Ministry. This information will be obtained through document analysis and interviews with the central data and information staff. In addition to interviews, a survey will be conducted on the IT services used to gain a clearer understanding of the features and process flows of those services.

Risk Assessment

Organizations can conduct a robust risk assessment that covers a wide range of risks, including IT and cybersecurity. This integration ensures a comprehensive and tailored approach to identify, analyze, evaluate, treat, and monitor risks, resulting in effective risk management practices.

Business Impact Analysis (BIA) Development

Business Impact Analysis (BIA) is the process of evaluating the potential impact of failures in business operations and helping determine priorities and recovery focus in case of a disaster. In this stage, the author will develop the BIA based on the chosen risk management framework.

Incident Response Plan and Disaster Recovery Development

An Incident Response Plan (IRP) is a document that outlines how an organization will respond to and address incidents or events that threaten information security. The IRP includes actions to be taken in emergency situations such as information security incidents, pandemics, natural disasters, etc. The goal of an IRP is to ensure that the organization has clear and coordinated procedures for addressing incidents and minimizing damage.

Disaster Recovery (DR) is the process of ensuring that a business can resume operations after a disaster or incident that threatens the business. DR involves identifying risks and the process of recovering systems and data so that the business can operate normally after a disaster. DR also ensures that critical data and applications can be restored and protected within a reasonable time frame. The objective of DR is to ensure that the business

can operate efficiently and effectively as soon as possible after a disaster, thereby reducing business losses as much as possible.

In this stage, the author will meticulously craft the Information Risk Policy (IRP) and Disaster Recovery (DR) plan, ensuring their seamless alignment with the designated framework. This meticulous process will also consider the precise business prerequisites of The XYZ Ministry. To demonstrate the real-world application of this strategic undertaking, an in-depth case study involving the XYZ Ministry in Jakarta. This case study will offer invaluable insights into the practical implementation of these policies, underscoring their relevance within the operational landscape of The XYZ Ministry.

Evaluation

This research will be evaluated through a gap analysis using the Guidelines of the Minister of PANRB Number 6 of 2023 on the Monitoring and Evaluation Procedures of SPBE and the Implementation of IT Audits by Internal Auditors.

Recommendations

In this stage, the author will compile several recommendations and suggestions discovered during the research process.

RESULTS AND DISCUSSION

Combination of ISO 31000 and NIST

The risk management process will utilize the ISO 31000 standard, as this standard has been adopted to align with the governance system based on electronic government in Indonesia. Subsequently, to specifically identify the capabilities of information technology, particularly in the realm of information security, we will combine it with the guidelines provided by the National Institute of Standards and Technology (NIST), as illustrated in Figure 4.

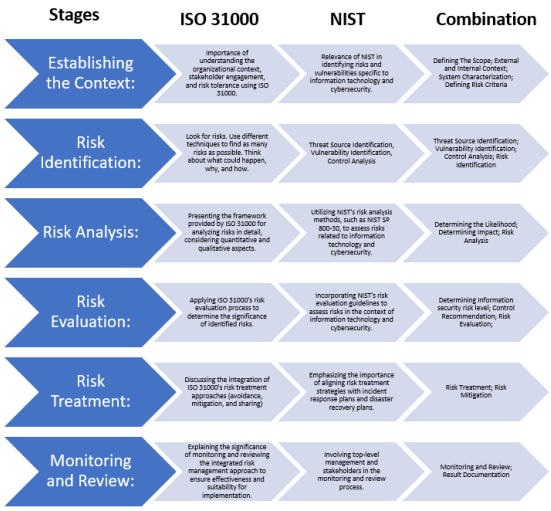

Figure 4
Integration of ISO 31000 and NIST

Establishing the Context:

Discuss the importance of understanding the organizational context, stakeholder engagement, and risk tolerance using ISO 31000. Highlight the relevance of NIST in identifying risks and vulnerabilities specific to information technology and cybersecurity.

The assessment scale for the likelihood level employs 5 levels, as described in Table 1.

Table 1
Assessment scale – Likelihood Level

Likelihood Level	Description	Percentage Likelihood of Occurrence in One Year	Number of Times Likely to Occur in One Year	Value
Almost Never Occurs	A threat or event that is insignificant and has little or no impact on operations, assets, or individuals.	X <= 5%	X < 2 Kali	1
Rarely Occurs	A threat or event that can cause minimal disruption to operations, assets, or individuals.	5% < X <= 10%	2 <= X <= 5 Kali	2

Sometimes Occurs	A threat or event that can cause significant disruption to operations, assets, or individuals.	10% < X <= 20%	6 <= X <= 9 Kali	3
Often Occurs	A threat or event that can cause severe disruption to operations, assets, or individuals.	20% < X <= 50%	10 <= X <= 12 Kali	4
Almost Certainly Occurs	A threat or event that can cause extremely severe or damaging disruption to operations, assets, or individuals.	X > 50%	X > 12 Kali	5

The assessment scale for the impact level utilizes 7 parameters, namely the risk impact on Financial, Reputation, Performance, Organizational Services, Operational and ICT Assets, Law and Regulation, and Human Resources. The mapping results of the impact level based on its impact area can be seen in Table 2.

Table 2
Assessment Scale – Impact Level

Impact Area	Impact Level				
	1	2	3	4	5
	Insignificant	Less Significant	Quite Significant	Significant	Very Significant
Financial (1)	Financial Decrease < 20%	Financial Decrease 20% to < 40%	Financial Decrease 40% to < 60%	Financial Decrease 60% to < 80%	Financial Decrease > 80%
Reputation (2)	Reputation Decrease < 20%	Reputation Decrease 20% to < 40%	Reputation Decrease 40% to < 60%	Reputation Decrease 60% to < 80%	Reputation Decrease > 80%
…..(…)					
Human Resources (7)	Human Resources Decrease < 20%	Human Resources Decrease 20% to < 40%	Human Resources Decrease 40% to < 60%	Human Resources Decrease 60% to < 80%	Human Resources Decrease > 80%

From the likelihood level and impact level described, we have created a 5x5 risk analysis matrix as shown in Figure 5. It begins with a risk level value of 1, indicating a very low risk level, represented by the color blue, and progresses to a risk level value of 25, indicative of a high risk level, represented by the color red.

Risk Analysis Matrix 5x5			Impact Level				
			1	2	3	4	5
			Insignificant	Less Significant	Quite Significant	Significant	Very Significant
Likelihood Level	5	Almost Certainly Occurs	9	15	18	23	25
	4	Often Occurs	6	12	16	19	24
	3	Sometimes Occurs	4	10	14	17	22
	2	Rarely Occurs	2	7	11	13	21
	1	Almost Never Occurs	1	3	5	8	20

Figure 5
Risk Analysis Matrix

Risk Identification:

Explain how ISO 31000's risk categorization and NIST's risk analysis techniques can be combined to identify risks across various domains, including technology, operations, and compliance.

The identified assets during the asset inventory are 11 assets with the following details:

Table 3
List of Assets

Code	Assets	Description
M1	Data Center	Data Center: A physical facility that stores all hardware and data, typically including servers, storage systems, and cooling systems.
M2	Government Intranet	Government Intranet: This encompasses infrastructure that supports internal data communication among government entities.
M3	Government Service Linkage System	Government Service Linkage System: A system that enables various government entities to share information and communicate with each other and the public.
M4	Data and Information	Data and Information: Includes all types of data and information managed by ministries or agencies, including personal and business data.
M…	….	
M11	Web Application	Web Application: An application created by The XYZ Ministry as part of SPBE (E-Planning and Budgeting System) services.

The identified Threat Events during the threat analysis are 32 threats with the following details:

Table 4
Threat Events

Assets	Threat Event	Threat Source	Relevance
Data Center (M1)	Data Breach (T1)	External Intruder	Confirmed
Data Center	Cooling System Failure	Device Failure	Anticipated
Web Application	Information Disclosure	External Intruder	Possible
M….	T….		
Web Application (M11)	Web Defacement (T32)	External Intruder	Possible

Identification of Existing Control:

Data Encryption, Temperature and Humidity Monitoring, Disaster Recovery Plan, DDoS Protection, Data Encryption in Transit, Security Awareness Training, Logging and Activity Monitoring, Redundant Systems and Failover, Access Control, Data Backup and Recovery, Data Usage Policies, Policy Training, Access Control to Policy Documents, Regular Policy Review and Updates, Hardware Maintenance and Replacement, Physical Security, Configuration Management, Antivirus and Anti-malware, Update and Patch Management, Multi-factor Authentication, Certificate and PKI Management, Security Review, SLA with Service Providers, Personnel Changes Management, Input Filtering, Output Encoding, CSRF Token, Proper Session Management, Appropriate Access Control, Patch and Version Management, Firewall, Security Awareness Training, Compliance Review, Asset Tracking, Pre-deployment Testing, Updates and Patching, Intrusion Detection, Account Management, Activity Monitoring, Access Review, Prepared Statements, Content Security Policy, SameSite Cookie Attribute, SSL/TLS, Rate Limiting, Minimal Response Errors, WAF (Web Application Firewall).

The identified vulnerabilities for those assets are 27 vulnerabilities with the following details:

Table 5
Identification of vulnerabilities

Infrastructure of IT	Existing Control	Vulnerability	Vulnerability Severity
Data Center (M1)	Data Encryption, Access Control	Weak Access Control System (V1)	High
Data Center (M1)	Temperature and Humidity Monitoring	Lack of Device Maintenance	Medium
Data Center (M2)	Disaster Recovery Plan	Physical Location Vulnerability	Low
M…	……..		
Web Application (M11)	Patch and Version Management, WAF (Web Application Firewall)	Improper Web Security Configuration (V27)	High

Risk Analysis:

Present the framework provided by ISO 31000 for analyzing risks in detail, considering the quantitative and qualitative aspects.

Risk Appetite			Impact Level				
			1	2	3	4	5
			Insignificant	Less Significant	Quite Significant	Significant	Very Significant
Likelihood Level	5	Almost Certainly Occurs	Accept	Mitigation	Mitigation	Mitigation	Mitigation
	4	Often Occurs	Accept	Mitigation	Mitigation	Mitigation	Mitigation
	3	Sometimes Occurs	Accept	Accept	Mitigation	Mitigation	Mitigation
	2	Rarely Occurs	Accept	Accept	Mitigation	Mitigation	Mitigation
	1	Almost Never Occurs	Accept	Accept	Accept	Accept	Mitigation

Figure 6
Risk Appetite

Illustrate how NIST's risk analysis methods, such as the NIST SP 800-30, can be utilized to assess risks specifically related to information technology and cybersecurity. Here are the results of the risk level calculation based on the 32 identified threats:

Table 6
Risk Analysis

Assets	Threat Event	Threat Source	Likelihood Level	Impact Level	Risk Level
Policies and Procedures (M5)	Outdated policies	Management	Almost Certainly Occurs	Insignificant	25

Government Service Connector System	Data theft	External intruder	Often Occurs	Very Significant	20
Policies and Procedures	Poor compliance	Employee	Almost Certainly Occurs	Less Significant	20
Web Application	SQL Injection	External intruder	Often Occurs	Very Significant	20
Web Application	Web Defacement	External Intruder	Often Occurs	Very Significant	20
…….					
Cloud Services	Cloud service failure	Cloud service provider	Almost Never Occurs	Quite Significant	3

Risk Evaluation:

Describe how ISO 31000's risk evaluation process can be applied to determine the significance of identified risks. Explain how NIST's risk evaluation guidelines can be incorporated to assess risks in the context of information technology and cybersecurity.

Risk determination is the initial stage before risk prioritizing. The risk priority matrix is classified based on the NIST SP 800-30 revision 1 and is a matrix of the relationship between assets and threats. From the matrix, we obtained result examples as follows: 1 very high (top priority), 4 high (priority), 7 moderate (second priority), 14 low (last priority), and 6 very low (no priority) risk scenarios. Figure 7 explains the priority of these risks.

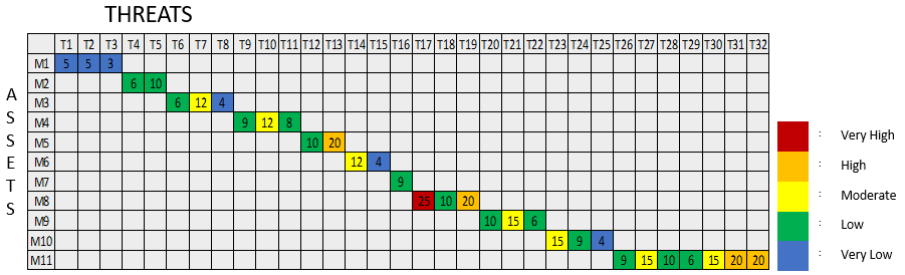

Figure 7
Risk Evaluation

Risk Treatment:

Discuss the integration of ISO 31000's risk treatment approaches, such as avoidance, mitigation, and sharing, with NIST's control self-assessment techniques and recommendations.

Table 7
Risk Treatment Plan

Threat Event	Action Plan	Technologies Implemented	Output	Responsible Party	Implementation Schedule
Outdated Policies	Review and update policies periodically	Policy Management Software	Up-to-date policy documents	Policy Team	Q1 2023
Data Theft	Implement strong encryption and access controls	Encryption Algorithms, Firewall, VPN	Enhanced data security	Security Team	Q2 2023
Poor Compliance	Regularly audit and ensure adherence to laws	Compliance Management Systems	Compliance reports	Compliance Team	Continuous
SQL Injection	Implement prepared statements, input validation	Input Validation Tools, Web Application Firewalls	Secured database interactions	Development Team	Q2 2023
Web Defacement	Monitor, respond, and restore altered web content	Intrusion Detection Systems (IDS), Content Management Systems (CMS)	Maintained web appearance	Web Management Team	Q2 2023

From the 32 threats identified, we prioritize handling those risks that have been identified as having a high and very high-risk level, as detailed in Table 7. Emphasize the importance of aligning risk treatment strategies with incident response plans and disaster recovery plans.

Monitoring and Review:

Explain the significance of monitoring and reviewing the integrated risk management approach to ensure its effectiveness and suitability for implementation. Discuss the involvement of top-level management and stakeholders in the monitoring and review process.

Business Impact Analysis and Plan Development

Business Impact Analysis (BIA)

Explain the purpose and steps involved in conducting a BIA according to NIST guidelines. Emphasize the identification of critical processes, assessment of outage impacts, estimation of downtime, and resource requirements for recovery.

Here are the results of the business impact analysis from the 117 applications at Bappenas. We selected 11 key applications based on their criticality and significant impact on the operational processes at Bappenas. The selected applications are as follows:

Table 7
BIA

Application	Application Description	RTO	RPO	Recovery Priority
Ministry of National Development Planning/Bappenas Website (A1)	The XYZ Ministry Main Website provides information about the Ministry's programs, activities, performance, and other related details. It also offers email access for employees and serves as a platform for the public to get updates on government programs.	4 hours	1 hour	Hot
Planning Collaboration and Budget Performance Information Application (KRISNA)	The Budget Planning Information System manages budget planning for the Ministry/Institution. It includes preparing strategic plans, National Medium-Term Development Plans (RPJMN), Government Work Plans, National Development Planning Meeting (Musrenbangnas) Online,	8 hours	4 hours	Hot

	Physical Special Allocation Fund (DAK Fisik) Proposal, People's Representative Council (DPR) Aspirations Proposal, and Budget Tagging.			
Electronic Monitoring and Evaluation (e-Monev PP 39)	Implementation Performance Reporting Application: Used for reporting the realization and achievement of the current year's work plan of the Ministry/Institution.	1 day	4 hours	Hot
A…	……..			
RPJPN (National Medium-Term Development Plan) Website (A10)	RPJPN 2045 Website: Developed as a communication and information dissemination medium to the public regarding the entire range of activities related to the long-term development through the RPJPN.	1 day	4 hours	Cold

To address the risks identified in the Business Impact Analysis (BIA) for applications at The XYZ Ministry, a dedicated internal team is essential. This team, specializing in handling incidents and potential disasters, would be responsible for safeguarding the electronic governance system. By understanding the priorities set in the BIA, utilizing advanced technologies, and coordinating with various stakeholders, this team would ensure the resilience and continuity of the ministry's critical functions. Regular training, clear communication, and alignment with national policies would further enhance their effectiveness in protecting the ministry's electronic governance against potential threats.

Incident Response Plan (IRP) and Disaster Recovery Plan (DRP):

Describe the development of IRP and DRP based on the identified risks and critical processes. Discuss the activation procedures, notification processes, recovery priorities, and reconstitution phase as recommended by NIST SP 800-34.

Figure 8
Incident Response Teams

In an electronic governance system, the flawless operation of technology and information protection holds the utmost significance. Within The XYZ Ministry, as illustrated in Figure 8, the Incident Response Team assumes a pivotal and indispensable role in preserving the integrity, accessibility, and confidentiality of government services delivered through electronic means.

The Incident Response Manager would be in charge of aligning incident response strategies with governmental objectives, ensuring that any incidents are handled swiftly to minimize disruption to public services. The Lead Investigator would work closely with other governmental bodies, ensuring that the investigations are in line with national security interests and that intelligence is shared appropriately. Security Analysts would be tasked with protecting sensitive governmental data, focusing on the unique threats that governmental bodies might face. IT Support would ensure that all electronic systems in the governance are functioning optimally, preserving the continuity of services. The Communications Coordinator would be responsible for communicating with various governmental agencies, the public, and possibly international bodies, depending on the nature of the incident. The Legal Advisor would ensure that all actions are in accordance with national and international laws, including those specifically related to electronic governance, data protection, and cybersecurity.

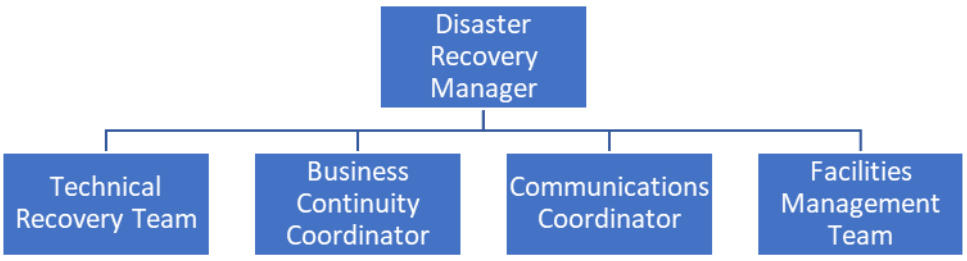

Figure 9
Disaster Response Teams

The Disaster Recovery Manager in this context ensures that the recovery strategies align with the government's commitment to providing uninterrupted e-services to its citizens. The Technical Recovery Team, as depicted in Figure 8, is tasked with restoring critical e-government infrastructure, like servers hosting governmental websites and databases containing essential public records. The Business Continuity Coordinator ensures that essential electronic services, such as online tax filing, license renewals, and public service applications, remain accessible even during disruptions. The Communications Coordinator ensures transparent and consistent communication with citizens, media, and other governmental bodies, maintaining trust and clarity in government interactions. The Facilities Management Team manages physical infrastructure related to e-government, such as data centers and network hubs.

CONCLUSION

In the analysis, the type of asset is identified based on asset categories according to the Presidential Regulation Number 95 of 2018 concerning Electronic-Based Government Systems. The information business process has risk scenarios that need to be assessed. The assessment can be done based on the information owner's perception or the technical aspect of the system.

The mapping of NIST SP 800-30 revision 1 to ISO 31000 focuses on the assessment of information security risks. The mapping-based analysis results in a comprehensive risk assessment following the ISO 31000 standard. Understanding is obtained from the details of threat sources based on adversaries and non-adversaries in the threat identification stage. The combination of techniques mentioned above can be applied to applications as a tool to simplify the information security risk management process for information owners. The semi-quantitative technique in NIST SP 800-30 revision 1 also plays a role in supporting risk analysis in ISO 31000. This process can be developed in applications up to the risk handling stage by providing control recommendations.

The risk management was structured with reference to the ISO 31000 and NIST SP 800-30 frameworks to formulate an accurate risk management guide in the form of a Business Impact Analysis (BIA) for the ministry. The preparation of the BIA was complemented with appropriate incident response plans and disaster recovery documents to enable the

organization to mitigate financial or non-financial damages and provide response options if the identified risks materialize.

This study thus underscores the critical importance of adopting a comprehensive and integrated approach to risk management within the sphere of e-government. By leveraging internationally recognized frameworks and tailoring them to the specific needs and regulations of the Indonesian government, this research contributes valuable insights and tools that can enhance the resilience, security, and efficiency of electronic governance systems. The findings offer a foundation upon which future studies may build, further refining and expanding the methodologies and practices essential for the robust and responsible management of technological risks in the governmental sector.

REFERENCES

Abied, O., O. Ibrahim, and S. N.-I. Mat Kamal. (2022). "Adoption of cloud computing in E-government: A systematic literature review." *Pertanika Journal of Science & Technology*. https://doi.org/10.47836/pjst.30.1.36

Agung, Muhammad Zakuan. (2019). "Perancangan Disaster Recovery Plan Sistem Informasi Akademik dengan Pendekatan Kerangka Kerja NIST 800-34." *JTERA (Jurnal Teknologi Rekayasa).* https://doi.org/10.31544/jtera.v4.i2.2019.157-166

Akkiyat, Ikram, and Nissrine Souissi. (2019). "Modelling Risk Management Process According to ISO." *International Journal of Recent Technology and Engineering (IJRTE) Volume 8 No 2:* https://doi.org/10.35940/ijrte.B3751.078219.

Allioui, Hanane, and Youssef Mourdi. (2023). “Unleashing the Potential of AI: Investigating Cutting-Edge Technologies That Are Transforming Businesses.” *International Journal of Computer Engineering and Data Science (IJCEDS)* 3(2), 1–12.

Barafort, Béatrix, Antoni Lluís Mesquida, and Antònia Mas. (2018). "Integrated Risk Management Process Assessment Model for IT Organizations Based on ISO 31000 in an ISO Multi-Standards Context." *Computer Standards and Interfaces 60* https://doi.org/10.1016/j.csi.2018.04.010

Brunner, Michael, Clemens Sauerwein, and Michael Felde. (2020). "Risk Management Practices in Information Security: Exploring the Status Quo in the DACH Region." *Computers and Security* https://doi.org/10.1016/j.cose.2020.101776

Fazlida, M.R., and Jamaliah Said. (2015). "Information Security: Risk, Governance and Implementation." *Procedia Economics and Finance 28 (April)* https://doi.org/10.1016/s2212-5671(15)01106-5

Fazlidaa, M.R., and Jamaliah Said. (2015). "Information Security: Risk, Governance and Implementation Setback." *Procedia Economics and Finance* https://doi.org/10.1016/S2212-5671(15)01106-5

Fikri, Muhamad Al. (2019). "Risk assessment using NIST SP 800-30 revision 1 and ISO 27005 combination technique in profit-based organization: Case study of ZZZ information system application in ABC agency." *Procedia Computer Science* (Elsevier).

Gordon, Lawrence A. , Martin P. Loeb, and Lei Zhou. (2020). "Integrating cost–benefit analysis into the NIST Cybersecurity Framework via the Gordon–Loeb Model." *Journal of Cybersecurity* DOI: 10.1093/cybsec/tyaa005.

HM, Jogiyanto, Willy Abdillah, dan Sigit Suyantoro. (2011). *Sistem tatakelola teknologi informasi.* Yogyakarta: Andi, 2011.

Iin, Hurin. 2017. *Manajemen Risiko Teknologi Informasi Padaproyek Perusahaan Xyz Melalui Kombinasi Cobit, Pmbok, Dan Iso 31000.* Surabaya: Institut Teknologi Sepuluh Nopember.

Joshi, Anant, Laury Bollen, Harold Hassink, and Steven. (2018). "Explaining IT Governance Disclosure through the Constructs of IT Governance Maturity and IT Strategic Role." *Information and Management Vol 55* https://doi.org/10.1016/j.im.2017.09.003

Kasidi. (2010). *Risk management.* Bogor: Ghalia Indonesia.

Kasma, Vira Septiyana, Sarwono Sutikno, and Kridanto Surendro. (2019). "Design of e-Government Security Governance System Using COBIT 2019 : (Trial Implementation in Badan XYZ)." *International Conference on ICT for Smart Society (ICISS).* https://doi.org/10.1109/ICISS48059.2019.8969808

Kementerian PAN RB. 2022. *Reviu Hasil Penilaian Evaluasi SPBE Tahun 2022 Kementerian PPN/Bappenas.* Jakarta: Kementerian PAN RB.

Khairiyah, I., Lubis, F., & Nasution, M. L. (2023). Analysis of the Influence of External Factors of Sharia Bank on Non-Performing Financing (NPF) of Indonesian Sharia Commercial Banks. *Indonesian Interdisciplinary Journal of Sharia Economics (IIJSE)*, *6*(3), 1838-1851. https://doi.org/10.31538/iijse.v6i3.3899

Kusumastuti, R., Mulyati, H., & Suprayitno, G. (2021). Disclosure Integration of Lean Six Sigma Principles in Sustainable Supply Chain in Poultry Industry. *Indonesian Interdisciplinary Journal of Sharia Economics (IIJSE)*, *4*(1), 300-312. https://doi.org/10.31538/iijse.v4i1.1706

Lee, Mordecai, Grant Neeley, and Kendra Stewart. (2021). *The Practice of Government Public Relations*. Routledge.

Marchiori, Danilo Magno , Ricardo Gouveia Rodrigues, Emerson Wagner Mainardes, and Silvio Popadiuk. (2023). "Smith, J. A., & Jones, M. B. (2019). The role of information technology in optimizing organizational performance in the public and private

sectors. Journal of Business and Technology, 45(3), 152-168." *Revista de Administração Pública 57(2).* http://dx.doi.org/10.1590/0034-761220220221x

Masso, Jhon Eder, Francisco J. Pino, J. Pardo, F. García, and M. Piattini. 2020. "Risk management in the software life cycle: A systematic literature review." *Computer Standards & Interfaces*. https://doi.org/10.1016/j.csi.2020.103431

Olechowski, A., J. Oehmen, W. Seering, and M. Ben-Daya. (2016). "The professionalization of risk management: What role can the ISO 31000 risk management principles play?" *International Journal of Project Management* 34(8), 1568–1578. https://doi.org/10.1016/j.ijproman.2016.08.002

Oliveira, De, Fernando Augusto, and Silva Marins. (2017). "The ISO 31000 Standard in Supply Chain Risk." *Journal of Cleaner Production* https://doi.org/10.1016/j.jclepro.2017.03.054

Settembre-Blundo, Davide, Rocío González-Sánchez, Sonia Medina-Salgado, and Fernando E García-Muiña. (2021). "Flexibility and Resilience in Corporate Decision Making: A New Sustainability-Based Risk Management System in Uncertain Times." *Global Journal of Flexible Systems Management* 22(Suppl 2): 107–32.

Shakibazad, Mohammad, and Ali Jabbar Rashidi. (2020). "New Method for Assets Sensitivity Calculation and Technical Risks Assessment in the Information Systems." *IET Information Security 14* https://doi.org/10.1049/iet-ifs.2018.5390

Shameli-Sendi, Alireza , Rouzbeh Aghababaei-Barzegar, and Mohamed Cheriet. 2015. "Taxonomy of Information Security Risk Assessment (ISRA)." *Computers & Security 57.* https://doi.org/10.1016/j.cose.2015.11.001

Stoneburner, Gary, Goguen, Alice, Feringa, and Alexi. (2002). "Risk Management Guide for Information Technology Systems." *National Institute of Standards and Technology.*

Tanuwijaya, H., and R. Sarno. (2010). "Comparation of CobiT Maturity Model and Structural Equation Model for Measuring the Alignment between University." *IJCSNS International Journal of Computer Science and Network Security.*

Toha, M., Ulfa, E., & Yanti Sandra Dewi, N. (2021). Analysis of The Implementation of Sharia Strategy Management at BMT Maslahah. Majapahit Journal of Islamic Finance and Management, 1(1), 29-40. https://doi.org/10.31538/mjifm.v1i1.3

Webb, J., and D. Hume. (2018). "Campus IoT Collaboration and Governance using the NIST Cybersecurity Framework." *Conference Paper*. https://doi.org/10.1049/cp.2018.0025

Wolingpirayat, J. (2007). "E-payment Strategies of Bank Card Innovation." *Journal of Internet Banking And Commerce.*