Design Information Security in Electronic-Based Government Systems Using NIST CSF 2.0, ISO/IEC 27001: 2022 and CIS Control

Dio Febrilian Tanjung[1]; Oky Dwi Nurhayati[2]; Adi Wibowo[3]
[1,2,3]Magister Information System, Postgraduate School
Diponegoro University Semarang, Indonesia

Abstract:- This study explores the application of three cybersecurity frameworks: NIST CSF 2.0, ISO/IEC 27001:2022, and CIS Control v8, resulting in the synthesis of 22 key components: Organizational context, Risk management processes, Assignment of security roles, Security policy implementation, Governance, monitoring, Third-party risk management, Inventory and management of assets, Risk identification and analysis, Continuous improvement, Access control, account management, Security awareness and training, Data protection, encryption, Configuration and maintenance management, Network and software security, Continuous monitoring, anomaly detection, Incident detection and analysis, Incident response planning, Incident analysis and prioritization, Incident response communication, and Incident mitigation. These syntheses serve as recommendations and information security controls applicable to government agencies. The frameworks provide guidance for developing information security measures, preparing necessary documents, and implementing technical steps to enhance information security.

Keywords:- *NIST CSF 2.0, ISO/IEC 27001:2022, CIS Control v8, Information Security, Cybersecurity Frameworks, Government Agencies.*

I. INTRODUCTION

Rapid advancements in information and communication technology necessitate that the government develop its state apparatus further by implementing an electronic-based government system (SPBE) or e-government. SPBE is a form of governance that utilizes information technology to deliver services to government institutions, state civil servants, businesses, communities, and other stakeholders. SPBE helps to foster and realize an open, participatory, innovative, and accountable government, enhance collaboration among government institutions to achieve shared objectives, improve the quality and accessibility of public services for the broader community, and reduce levels of collusion, corruption, and nepotism through the implementation of a supervision system [1]. The government's electronic system, which stores sensitive information from citizens and manages the country's operations, is a primary target for cybercriminals. In 2023, there were 403,990,813 instances of anomalous cyberattacks traffic in Indonesia, primarily targeting government administration systems. Cyber Threat Intelligence (CTI) monitoring identified 347 suspected cyber incidents, including data leakage, ransomware, website defacement, indications of potential DDoS attacks, and proactive monitoring of alleged cyber incidents. The search for cyber incidents aims to deepen the understanding of reported cyber occurrences published across forums and media on the Surface Web, Deep Web, and Dark Web, such as alleged data leaks and ransomware disclosures [2].

The potential threats mentioned above represent only a fraction of the issues in the cyber world. These threats continually evolve and demand organizations to adapt swiftly to prevent significant impacts that could disrupt their sustainability [3]. Risk management involves steps to mitigate and reduce risks to ensure smooth business operations [4]. Understanding, identifying, and evaluating every potential risk is fundamental to effective risk management [5]. Standardizing planning and implementing risk mitigation strategies in information technology applications serves as a foundational framework, enabling the measurement of each risk based on its severity [6]. Adopting a cybersecurity framework is crucial for safeguarding organizations against cyber threats. Such frameworks typically offer high-level guidelines rather than specific opinions [7].

The National Institute of Standards and Technology Cybersecurity Framework 2.0 (NIST CSF 2.0) is a framework designed to help organizations define and mitigate the risks of cyberattacks. The NIST CSF includes components such as technical controls, log analysis, and incident response. NIST CSF 2.0 represents an evolution from its predecessor, NIST CSF 1.1, with changes including restructuring core components into six categories and enhancing the detail and refinement of each category and subcategory [8]. ISO/IEC 27001:2022 is an international standard for information security management that serves as a guide for organizations in managing data security risks. ISO/IEC 27001:2022 provides guidelines for conducting risk analysis, implementing controls, and monitoring and evaluating organizational responsibilities in information management [9]. The Center for Internet Security (CIS) Controls V8 offers specific cybersecurity measures aimed at preventing common attacks on systems and networks. CIS Controls V8 aligns with globally recognized standards and represents best practices for protecting IT systems and data from cyberattacks [10]. The available security frameworks can serve as a guide for formulating measurable and targeted risk management strategies based on the organization's current conditions and capabilities [11]. This research focuses on risk management within government agency ABC, where government systems are frequent targets of threats. By leveraging NIST CSF 2.0, ISO/IEC 27001:2022, and CIS Controls V8, this study aims to identify security risks and systematically mitigate them within ABC government agencies.

Intelligent government refers to public administration services that leverage electronic and internet systems, along with principles of open government. It involves using ICTs to enhance the effectiveness, innovation, efficiency, transparency, accountability, and inclusivity of public administration [5].

II. LITERATUR REVIEW

➢ *Information Security*

Information is one of the most critical assets within an organization, and on a national scale encompassing business, defense, and security sectors, maintaining the availability, integrity, and reliability of information is paramount. Information security is especially crucial for organizations with strategic importance. The more information an organization manages, the greater the risk of information threats. Cybersecurity efforts focus on preventing, detecting, and mitigating the impact of losses and damage to the system [8].

The primary purpose of information security is to prevent or mitigate cyberattacks and reduce the risk of cyber threats. The application of standards brings benefits such as saving time, reducing costs, increasing profits, enhancing user awareness, minimizing risks, and ensuring business continuity. Additionally, adherence to standards facilitates organizational compliance with the best industry practices and procedures, and provides opportunities to benchmark security systems internationally [12].

➢ *Risk Management*

Risk management involves steps to overcome and reduce risks to the organization, ensuring that business processes can sustain effectively [1]. Understanding, identifying, and evaluating every potential risk are key components of risk management [2]. Every organization must plan comprehensively to prevent and reduce cyber risks. Cyber risk management is a sustainable approach that addresses risks and uncertainties in cyberspace to maximize the achievement of organizational goals [3].

➢ *Electronic-based Government System*

Electronic-Based Government System (SPBE) or e-Government refers to government administration that utilizes ICTs to provide services to government agencies, state civil servants, businesses, communities, and other stakeholders. SPBE offers opportunities to promote and achieve open, participatory, innovative, and accountable governance. It enhances collaboration between government agencies to achieve common goals, improves the quality and accessibility of public services for the broader community, and reduces abuses of authority such as collusion, corruption, and nepotism through the implementation of electronic-based community supervision and complaint systems [4].

➢ *NIST CSF 2.0*

The National Institute of Standards and Technology Cybersecurity Framework is a framework designed to help organizations define and mitigate the risk of cyberattacks. The NIST CSF components are particularly suitable for use by technology organizations due to their focus on technical controls, log analysis, and incident response [6]. NIST CSF 2.0 is an advancement of the previous framework, NIST CSF 1.1. In NIST CSF 2.0, there are changes such as restructuring core components into 6 categories and enhancing the detail and refinement of each category and subcategory [7].

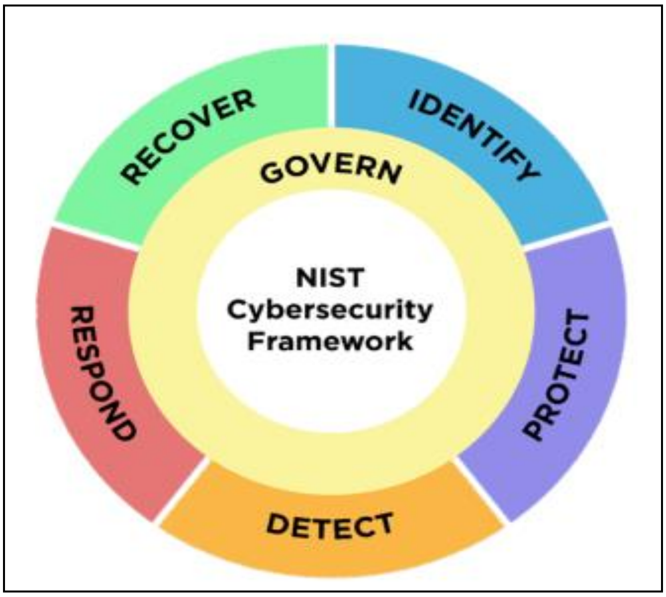

Fig 1 CSF 2.0 Core [7]

➢ *ISO/IEC 27001:2022*

ISO/IEC 27001:2022 is used to develop and manage the Information Security Management System (ISMS). ISO/IEC 27001:2022 ensures that the risk management process is carried out systematically and well-documented. The focus is on standards and Annex A requirements to identify relevant controls and integrate them into a broader management framework. The ISO/IEC 27001:2022 framework consists of 10 clauses and 93 appendices in Annex A. The preparation of information security frameworks in organizations can be seen in Table 1. [8].

Table 1 Klausul ISO/IEC 27001:2022

Clause	Title	Description
1	Scope	Defining the boundaries and application of the ISMS
2	Normative References	Listing the documents essential for the implementation of the standard.
3	Terms and Definition	Providing definitions of terms used in the standard.
4	Context of the organization	4.1 Understanding the organization and its context 4.2 Understanding the needs and expectations of interested parties 4.3 Determining the scope of the ISMS 4.4 Information security management system
5	Leadership	5.1 Leadership and commitment 5.2 Information security policy 5.3 Roles, responsibilities, and authorities within the organization
6	Planning	6.1 Actions to address risks and opportunities 6.1.1 General 6.1.2 Information security risk assessment 6.1.3 Information security risk treatment 6.2 Information security objectives and planning to achieve them 6.3 Planning for changes
7	Supporting	7.1 Resources 7.2 Competence 7.3 Awareness 7.4 Communication 7.5 Documented information 7.5.1 General 7.5.2 Creation and update 7.5.3 Control of documented information
8	Operating	8.1 Operational planning and control 8.2 Risk assessment and risk treatment
9	Performance Evaluation	9.1 Monitoring, measurement, analysis, and evaluation 9.1.1 General 9.1.2 Evaluation of information security performance 9.2 Internal audit 9.3 Management review
10	Improvement	10.1 Nonconformity and corrective action 10.2 Continual improvement

- ➢ *CIS Control v8*

CIS Controls v8 serves as a specific technical guideline. Use CIS Controls v8 to provide detailed technical guidance that IT and security teams can use to protect systems and data. CIS Controls v8 is highly specific and actionable, helping in the effective and efficient implementation of technical measures, as shown in Table II. Based on Table II, the CIS Controls framework consists of 18 information security controls, ranging from asset management to data protection, access management, continuous vulnerability management, and incident response. Each control is designed to help government agency ABC identify, manage, and mitigate information security risks and risk management effectively, ensuring compliance with good security practices within the agency.

Table 2 CIS Control v8

No	Control	Description
1	*Inventory and Control of Enterprise Assets*	Activate and control all physical and virtual devices within the organization's IT environment to ensure that only authorized devices have access.
2	*Inventory and Control of Software Assets*	Identify and manage software running in the organization's IT environment to ensure that only authorized software can be installed and executed.
3	*Data Protection*	Protect sensitive data stored, processed, or transmitted to maintain confidentiality, integrity, and availability.
4	*Secure Configuration of Enterprise Assets and Software*	Ensure hardware and software are configured securely to reduce the risk of attacks.
5	*Account Management*	Manage user account and service lifecycles to ensure only legitimate accounts exist and are used.
6	*Access Control Management*	Control access to assets and data based on the principle of least privilege and need-to-know.
7	*Continuous Vulnerability*	Continuously identify, evaluate, and remediate vulnerabilities to maintain system

No	Control	Description
	Management	and data security.
8	*Audit Log Management*	Manage, analyze, and retain audit logs to detect and respond to security incidents.
9	*Email and Web Browser Protections*	Implement security controls to protect against threats sent via email and web browsers.
10	*Malware Defenses*	Implement measures to detect and remove malicious software to protect systems.
11	*Data Recovery*	Ensure proper data recovery and system restoration in case of data loss or system failure.
12	*Network Infrastructure Management*	Manage and secure network infrastructure to protect data in transit and prevent unauthorized access.
13	*Security Awareness and Skills Training*	Manage and secure network infrastructure to protect data in transit and prevent unauthorized access.
14	*Service Provider Management*	Ensure third-party service providers comply with organizational security policies and manage associated risks.
15	*Application Software Security*	Identify and address vulnerabilities in application software to prevent attacks.
16	*Incident Response Management*	Develop and maintain an incident response plan to detect, respond to, and recover from security incidents.
17	*Penetration Testing*	Conduct regular penetration testing to identify and remediate vulnerabilities before attackers can exploit them.
18	*Security Policies and Procedures*	Develop, document, and disseminate information security policies and procedures to ensure consistent security practices.

III. RESEARCH METHODOLOGY

This research is conducted at government agency ABC, which focuses on the management of technology and information in a specific region. The study uses a qualitative approach, with data collected through interviews, observations, and documentation.

- *Comparative Analysis*

Identify the main components of each framework, such as functions, categories, and controls. Compare the structure of the three frameworks to find similarities and differences. This includes identifying areas where the frameworks overlap and differ.

Table 3 Comparison Framework

Models	Functions	Goals
NIST CSF 2.0	• *Govern* • *Identify* • *Protect* • *Detect* • *Respond* • *Recover*	Cybersecurity standards and risk management Check level implementation and deployment
ISO/IEC 27001:2022	• Organizational Context • Leadership • Planning • Support • Operation • Performance Evaluation • Improvement	Standards and procedures related to information security and control
CIS Controls v8	• Inventory and Control of Enterprise Assets • Inventory and Control of Software Assets • Data Protection • Secure Configuration of Enterprise Assets and Software • Account Management • Access Control Management • Continuous Vulnerability Management • Audit Log Management • Email and Web Browser Protections • Malware Defenses • Data Recovery • Network Infrastructure Management	Practice for improvement cybersecurity

Models	Functions	Goals
	• Security Awareness and Skills Training • Service Provider Management • Application Software Security • Incident Response Management • Penetration Testing • Security Policies and Procedures	

➢ *Mapping Component*

Create a map that connects the elements of each framework. For example, link the categories and subcategories of NIST CSF with the clauses of ISO/IEC 27001 and the controls of CIS. Use cross-referencing to see how the components of these frameworks can be integrated, matching similar controls and identifying areas where additional controls are needed. Based on the comparison in Table III, it can be observed that each framework has specific functions and objectives in information security. The main difference among the three frameworks is that more controls or functions are covered in ISO/IEC 27001:2022 and CIS Controls v8.

Table 4 Pemetaan Tata Kelola Manajemen Resiko

NIST CSF Subcategory	NIST CSF Subcategory	ISO 27001 Control	CIS Control	Synthesis
GV.OC	Organizational Context	Clause 4.1, 4.2		Organizational context
GV.RM	Risk Management Strategy	Clause 6.1.2, Clause 6.1.3	All Control	Risk management processes
GV.RR	Roles, Responsibilities, and Authorities	Clause 5.3	Control 5. Control 6	Assignment of security roles
GV.PO	Policy	Clause 5.2		Security policy implementation
GV.OV	Oversight	Clause 5, Clause 9		Governance, monitoring
GV.SC	Cybersecurity Supply Chain Risk Management	A 5.19, A 5.20, A 5.21, A 5.22	Control 15	Third-party risk management
ID.AM	Asset Management	A 5. 9, A 5.10, A 5.11, A 5.12, A 5.13, A 8.7	Control 1, Control 2	Inventory and management of assets
ID.RA	Risk Assessment	A 5.24, A 5.25, A 5.26, A 5.27, A 5.28, A 5.29, A 8.8	Control 3	Risk identification and analysis
ID.IM	Improvement	A 5.31, A 5.32, A 8.32	Control 18	Continuous improvement
PR.AA	Identity Management, Authentication, and Access Control	A. 5.14, A. 5.15, A. 5.16, A. 5.17, A. 5.18, A 7.2, A 7.3, A 7.4, A 8.1, A 8.2, A 8.3, A 8.4, A 8.5	Control 5, 6	Access control, account management
PR.AT	Awareness and Training	A 5. 36, A 6.1, A 6.2, A 6.3, A 6.4, A 6.5,	Control 14	Security awareness and training
PR.DS	Data Security	A 8.6, A. 8. 10, A. 8. 11, A. 8. 12, A. 8. 13, A. 8. 14, A 8.15, A 8.16	Control 3	Data protection, encryption
PR.PS	Platform Security	A 7.1, A 7.2, A 7.3, A 7.4, A 7.5, A 7.6, A 7.7, A 7.8, A 7.9, A 7.10, A 7.11, A 7.12, A 7.13, A 7.14	Control 4, 11	Configuration and maintenance management
PR.IR	Technology Infrastructure Resilience	A 8.19, A 8.20, A 8.21, A 8.22, A 8.23, A 8.24, A 8.25, A 8.26, A 8.27, 8.28, A 8.29, A 8.30, A 8.31	Control 9, 10, 12, 16	Network and software security
DE.CM	Continuous Monitoring	A 5.6, A 5.7, A 5.22, A 5.35, A 6.8, A 8.34	Control 7, 8, 13	Continuous monitoring, anomaly detection
DE.AE	Adverse Event Analysis	A5.6, A 5.7, A 5.22, A 5.35, A 6.8, A 8.34	Control 7, 8	Incident detection and analysis
RS.MA	Incident Management	A 5.26	Control 17	Incident response planning
RS.AN	Incident Analysis	A 5.28	Control 17	Incident analysis and prioritization
RS.CO	Incident Response Reporting and	A 5.29	Control 17	Incident response communication

NIST CSF Subcategory	NIST CSF Subcategory	ISO 27001 Control	CIS Control	Synthesis
	Communication			
RS.MI	Incident Mitigation	A 5.27	Control 17	Incident mitigation
RC.RP	Incident Recovery Plan Execution	A 5.30	Control 17	Business continuity planning
RC.CO	Incident Recovery Communication	A 5.26	Control 17	Recovery communication

In Table 4, it can be seen that ISO 27001:2022 and CIS Controls v8 can be used as technical guidelines for actions related to information security and risk management. The synthesis results from combining the three frameworks into one. The technical guidelines of ISO 27001:2022 provide recommended clauses and security control references (A), which serve as benchmarks for government agency ABC in information security and risk management. Each framework emphasizes different aspects of risk management and information security. NIST CSF focuses on organizational context, risk management, and incident management; ISO/IEC 27001:2022 focuses on asset management, risk assessment, and performance improvement; and CIS Controls v8 emphasizes asset inventory management, access management, and data protection.

- *Gap Analysis*

Identify gaps between the existing controls and those needed based on the mapping. This helps determine areas requiring further attention. Assess the risks associated with these gaps and set priorities for corrective actions.

- *Risk Management Recommendation*

Develop an action plan that includes steps for implementing the controls identified in the mapping and gap analysis. The action plan should cover responsibilities, required resources, and a timeline.

IV. RESEARCH FINDINGS

Based on the results of the GAP analysis interviews, several areas have been identified for improvement in the implementation of information security and risk management at government agency ABC. The key findings include the need to more clearly define the organizational context concerning external parties, strengthen the risk management process with more detailed technical steps and proactive risk prevention, and improve documentation and the creation of derivative rules for security policies, asset management, and risk management. Additionally, there is a need for a more structured approach to third-party risk management, more comprehensive data protection, and the development of a more detailed business continuity plan. By addressing these areas, the organization can enhance the overall effectiveness and security of its information-system.

Table 5 Analysis GAP

No	Sintesis	GAP
1	Organizational context	Already defined but lacks definitions related to external parties and is still limited to internal parties.
2	Risk management processes	Already defined but still lacks technical steps governing how risks are handled based on risk levels, and there are also no prevention processes to reduce risks.
3	Assignment of security roles	Already established but not yet defined in the case of technical transfers of authority
4	Security policy implementation	The regulations are already in place, but the technical derivatives of these regulations have not been specified yet.
5	Governance, monitoring	Already in place but not yet documented.
6	Third-party risk management	Not established yet.
7	Inventory and management of assets	Already existing and well-documented but needs more comprehensive data collection.
8	Risk identification and analysis	Not established yet
9	Continuous improvement	Not established yet.
10	Access control, account management	Already executed but lacks documentation, standards, and derivative rules.
11	Security awareness and training	Already done, needs improvement
12	Data protection, encryption	Some actions were taken, but they were not documented and implemented comprehensively.
13	Configuration and maintenance management	It has been done, but there is no documentation and no subsidiary regulations governing it.
14	Network and software security	It has been done, but there is no documentation, standards, or subsidiary regulations in place.
15	Continuous monitoring, anomaly detection	It has been done, but there is no documentation, standards, or subsidiary regulations in place.

16	Incident detection and analysis	Conducted without accompanying documentation, standards, or derivative rules to regulate
17	Incident response planning	Conducted without accompanying documentation, standards, or derivative rules to regulate
18	Incident analysis and prioritization	Conducted without accompanying documentation, standards, or derivative rules to regulate
19	Incident response communication	Conducted without accompanying documentation, standards, or derivative rules to regulate
20	Incident mitigation	Conducted without accompanying documentation, standards, or derivative rules to regulate
21	Governance, monitoring	It has not been done yet
22	Third-party risk management	It has been done, but there are no standards or subsidiary regulations governing it.

Based on the findings in Table V, the GAP analysis identifies several areas that need attention in information security and risk management. The GAP analysis presented in the table highlights a series of challenges in implementing information security and risk management at government agency ABC. Organizational context (point 1), although defined, lacks development to cover external aspects important for understanding the influence of the external environment on information security. Risk management (points 2 and 8), despite existing processes, requires more detailed technical steps and structured prevention processes to reduce potential threats. Security role management (point 3) needs clearer definitions related to authority transfer, which is essential to ensure consistency and continuity in information security implementation. Security policy (point 4) requires further development in technical documents and guidelines to ensure consistent understanding and effective implementation across all parts of government agency ABC. Governance and monitoring (point 5) need improvement with better documentation to ensure that information security processes are systematically monitored and evaluated. Third-party risk management (point 6) is an area that still needs development, given the importance of managing risks arising from external parties. Asset inventory management (point 7), risk identification (point 8), continuous improvement (point 9), access control and account management (point 10), and security awareness and training (point 11) all require more documentation, standards, and regulated procedures to ensure consistent and effective information security practices. All these aspects must be supported by effective communication in planning and responding to security incidents (points 17-20), as well as more detailed business continuity planning (point 21) and recovery communication (point 22) to ensure a quick and coordinated response in case of emergencies or security crises. By identifying and closing these gaps, government agency ABC can enhance its resilience against information security threats and strengthen the protection of its assets and data comprehensively. Through the GAP analysis table, recommendations can be provided on areas for improvement, enhancing information security and risk management at government agency ABC. Based on field findings from interviews, observations, and documentation, and the synthesis results of the NIST CSF 2.0, ISO/IEC 27001:2022, and CIS Controls frameworks, we identified twenty-two recommendations for the government agency in this study. The synthesis for Organizational Context recommends emphasizing internal and external aspects of the organization to define clear boundaries. The Risk Management Processes synthesis recommends that risk management include not only policies but also an assessment of existing risks and an explanation of handling procedures. The Assignment of Security Role synthesis recommends additional rules regarding authority transfer if the appointed employee is transferred or retired. The Security Policy Implementation synthesis recommends practical steps or guidelines for security implementation for users. The Oversight Governance synthesis recommends creating rules and mapping negligence that could impact the continuity of government systems. The Third-Party Risk Management synthesis recommends policies, risk analysis, and risk recommendations related to using third parties. The Inventory and Management of Assets synthesis recommends a more comprehensive asset list. The Risk Identification and Analysis synthesis recommends identifying and analyzing risks based on threats and impacts on IT assets. The Continuous Improvement synthesis recommends a measurable and pre-prepared development plan. The Access Control and Account Management synthesis recommends documenting access for account use, server facilities, and other devices, ensuring they are well-regulated with time limits and agreements to bind user responsibility. The Security Awareness and Training synthesis recommends enhancing cyber security literacy, which evolves rapidly. The Data Protection and Encryption synthesis recommends comprehensive encryption of critical data so that, in case of a database leak, decryption is still required to read the data. The Configuration and Maintenance Management synthesis recommends documenting technical settings and maintenance to facilitate and speed up repair time in case of disruptions/incidents. The Network and Software Security synthesis recommends documenting secured networks and applications, such as device updates, network, or system scans, suggesting layered security rather than relying on a single security measure. The Continuous Monitoring and Anomaly Detection synthesis recommends documenting every monitoring and anomaly detection result to facilitate further analysis. The Incident Detection and Analysis synthesis recommends documenting and analyzing each detected incident to provide material for future improvements. The Incident Response Planning synthesis recommends documenting every incident response plan to facilitate quick steps in case of similar incidents. The Incident Analysis and Prioritization synthesis recommends analyzing each collected incident and prioritizing repairs based on severity. The Incident Response Communication synthesis recommends maintaining good communication between affected parties and the repair team during incidents to provide certainty for affected users, with a dedicated channel for incident reporting. The Incident Mitigation synthesis recommends that well-documented incidents require mitigation steps to avoid recurrence. The Business Continuity Planning synthesis recommends designing or creating policies for future information security development to ensure continuous updates, and the Recovery Communication synthesis recommends further communication about the recovery process when an incident has been resolved.

V. CONCLUSION

This research found that the implementation of the three frameworks NIST CSF 2.0, ISO/IEC 27001:2022, and CIS Controls v8 resulted in 22 synthesized elements: organizational context, risk management processes, assignment of security roles, security policy implementation, governance and monitoring, third-party risk management, inventory and management of assets, risk identification and analysis, continuous improvement, access control and account management, security awareness and training, data protection and encryption, configuration and maintenance management, network and software security, continuous monitoring and anomaly detection, incident detection and analysis, incident response planning, incident analysis and prioritization, incident response communication, incident mitigation, governance and monitoring, and third-party risk management. From these 22 synthesized elements, recommendations and information security controls can be provided to government agency ABC. This framework can serve as a reference for developing steps in information security, preparing necessary documents, and implementing technical measures to enhance information security.

REFERENCES

[1]. D. . Tanjung, O. A, and A. . Widodo, “Analisis Manajemen Risiko Startup Pada Masa Pandemi Covid-19 Startup Risk Management Analysis During Covid-19 Pandemic Using,” J. Teknol. Inf. dan Ilmu Komput., vol. 8, no. 3, pp. 635–642, 2021, doi: 10.25126/jtiik.202184914.

[2]. H. M. Astuti, F. A. Muqtadiroh, E. W. T. Darmaningrat, and C. U. Putri, “Risks Assessment of Information Technology Processes Based on COBIT 5 Framework: A Case Study of ITS Service Desk,” Procedia Comput. Sci., vol. 124, pp. 569–576, 2017, doi: 10.1016/j.procs.2017.12.191.

[3]. A. Amiruddin, H. G. Afiansyah, and H. A. Nugroho, “Cyber-Risk Management Planning Using NIST CSF v1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8,” Proc. - 3rd Int. Conf. Informatics, Multimedia, Cyber, Inf. Syst. ICIMCIS 2021, pp. 19–24, 2021, doi: 10.1109/ICIMCIS53775.2021.9699337.

[4]. Pemerintah Pusat, “Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik,” Menteri Huk. Dan Hak Asasi Mns. Republik Indones., p. 110, 2018.

[5]. P. A. W. Putro, D. I. Sensuse, and W. S. S. Wibowo, “Framework for critical information infrastructure protection in smart government: a case study in Indonesia,” Inf. Comput. Secur., vol. 32, no. 1, pp. 112–129, 2024, doi: 10.1108/ICS-03-2023-0031.

[6]. D. Sulistyowati, F. Handayani, and Y. Suryanto, “Comparative analysis and design of cybersecurity maturity assessment methodology using nist csf, cobit, iso/iec 27002 and pci dss,” Int. J. Informatics Vis., vol. 4, no. 4, pp. 225–230, 2020, doi: 10.30630/joiv.4.4.482.

[7]. NIST, “NIST Cybersecurity Framework (CSF) Version 2.0.” National Institute of Standards and Technology, 2024. [Online]. Available: https://www.nist.gov/cyberframework

[8]. ISO and IEC, “ISO/IEC 27001:2022 - Sistem Manajemen Keamanan Informasi - Persyaratan,” ISO/IEC 27001:2022, vol. 2022. International Organization for Standardization (ISO), Jenewa, Swiss, 2022. doi: 10.2307/j.ctv30qq13d.