

Cyber Resilience Readiness Assessment Using NIST Cybersecurity Framework 2.0 in Local Government

Aziev Hanif Bahtiar¹, Rahadian Bisma²

^{1,2}*Universitas Negeri Surabaya, Surabaya, Indonesia*

aziev.21035@mhs.unesa.ac.id, rahadianbisma@unesa.ac.id

ABSTRACT

The acceleration of public service digitalization through the Electronic-Based Government System (Sistem Pemerintahan Berbasis Elektronik, SPBE) requires comprehensive information security strengthening within local government agencies. This study measures the cyber resilience readiness level of the Communication and Informatics Office (Diskominfo) of Mojokerto City using the NIST Cybersecurity Framework (CSF) 2.0. A descriptive qualitative method with a case study approach was applied through in-depth interviews, field observations, and document analysis to map the organization's existing conditions onto the six core functions of NIST CSF 2.0: Govern, Identify, Protect, Detect, Respond, and Recover, comprising 22 categories and 106 subcategories. The measurement shows that the average cyber resilience readiness score of Diskominfo Mojokerto City is 2.10 on a 4.00 scale. This score places the agency at the Risk Informed level (Tier 2), indicating that the organization possesses risk awareness but has not yet implemented it consistently or through automation across all functions. Specifically, the Govern function achieved the highest score (2.47), supported by a solid administrative and legal foundation, whereas the Recover function was identified as the most critical vulnerability with the lowest score (1.67) due to the absence of a formal disaster recovery plan. Strategic recommendations to reach the Repeatable target profile (Tier 3) include the formulation of a Disaster Recovery Plan, formalization of vendor supply-chain security policies, and the implementation of centralized automated security monitoring technologies such as SIEM and threat intelligence. These findings provide an objective baseline to support the agency's transition from a reactive posture toward a mature and standardized cyber resilience program.

Keyword: NIST CSF 2.0, Cyber Resilience, SPBE, Local Government, Readiness Level, Information Security Governance.

Article Info:

Article history:

Received 04 13, 2026

Revised 05 14, 2026

Accepted 06 15, 2026

Corresponding Author

Aziev Hanif Bahtiar

Universitas Negeri Surabaya, Surabaya, Indonesia

aziev.21035@mhs.unesa.ac.id

1. INTRODUCTION

Digital transformation has become one of the main pillars in the modernization of government administration worldwide, including in Indonesia. Governments increasingly rely on digital platforms to improve the efficiency, transparency, and reach of public services while strengthening the participation of citizens and stakeholders in governance [1]. The implementation of electronic governance (e-governance) has transformed government administration by enabling more accessible, efficient, and transparent public service delivery through the support of information and communication technology infrastructure [2]. Through Presidential Regulation No. 95 of 2018 on the Electronic-Based Government System (SPBE), the Indonesian government encourages

agencies to leverage information assets and technology infrastructure for administration and public services [3][4]. However, this growing digitalization also widens the attack surface and introduces new exposure to cyber threats, which reinforces the importance of integrated information security to preserve data confidentiality and public trust in electronic government [2].

As technology advances, cyber threats are becoming more complex and target various sectors, with public administration being among the most vulnerable [5]. The National Cyber and Crypto Agency (BSSN) reported that during August 2025 the public administration sector was the most affected by cyberattacks, accounting for 52% of a total of 153 recorded cyber-incident indications. These indications were dominated by data breaches (139 cases), followed by doxing (12 cases) and ransomware (2 cases) [6]. Such figures signal significant and urgent vulnerabilities that government agencies must address, making cyber resilience a critical concern for safeguarding public services [7].

Cyber resilience is the ability of a system or organization to anticipate, withstand, and recover effectively from cyberattacks [7]. The concept focuses not only on prevention but also on maintaining operational continuity even while an incident is occurring. Effective measurement of cyber resilience is therefore essential so that organizations can analyze and strengthen their information technology infrastructure against continuously evolving threats. This need is also evident at the regional level.

As the Regional Data Steward (Walidata) and the main network infrastructure provider for all Regional Government Organizations, Diskominfo Mojokerto City holds a strategic role at the forefront of managing IT infrastructure, developing digital public services, and securing the data assets of the Mojokerto City Government [8][9]. A security failure at the Diskominfo level could trigger systemic risk capable of paralyzing the public services of an entire city simultaneously. Considering the high national trend of cyber threats in the government sector, it is imperative for the agency to proactively identify and measure its cyber resilience readiness.

Measuring cyber resilience readiness cannot be done subjectively; it requires a structured and globally recognized framework. One of the most widely adopted is the NIST Cybersecurity Framework (CSF), developed by the National Institute of Standards and Technology (NIST). NIST CSF was chosen in this study because it is flexible, adaptive, and risk-based; it does not prescribe rigid rules and can therefore be applied to diverse organizations, including government agencies that are still developing their cybersecurity programs [10]. Its latest version, CSF 2.0, offers a logical approach organized into six core functions: Govern, Identify, Protect, Detect, Respond, and Recover [11]. Using this framework, an organization can assess its current security posture, identify existing gaps, and formulate future improvement strategies.

Several prior studies have applied maturity- and risk-based frameworks in the Indonesian public sector, for example information-security risk management using NIST CSF and ISO/IEC 27001 at a statistics agency [12], maturity assessment combining NIST CSF and CMMI on an academic information system [13], and governance evaluation using the Information Security Index (Indeks KAMI) at a district communication office [14]. Nevertheless, most existing works apply the framework in academic or corporate settings and rarely address local-government agencies acting as regional data stewards. Unlike those studies, this research contributes an objective, framework-based measurement of cyber resilience readiness in a local government agency that has not previously conducted a formal assessment, and translates the resulting gaps into prioritized, implementable recommendations that serve as a foundation for structured strategic improvement.

2. METHODS

This study employed a descriptive qualitative research design with a case study approach to obtain an in-depth understanding of the actual cyber resilience conditions at Diskominfo Mojokerto City. The research instruments were derived from the NIST CSF 2.0 structure, which consists of 6 Functions, 22 Categories, and 106 Subcategories, and were arranged into two forms: an interview guide containing open-ended questions developed from the CSF Categories, and an audit worksheet detailing all 106 Subcategories used to map informant answers and physical evidence into readiness tiers. The complete structure of functions and categories used as the assessment basis is presented in Table 1.

Table 1. NIST CSF 2.0 Function and Category Structure Used in the Assessment

Function	Category	Code
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
Identify (ID)	Cybersecurity Supply Chain Risk Management	GV.SC
	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvements	ID.IM
	Identity Management, Authentication & Access Control	PR.AA
Protect (PR)	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
Detect (DE)	Technology Infrastructure Resilience	PR.IR
	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
	Incident Management	RS.MA
Respond (RS)	Incident Analysis	RS.AN
	Incident Response Reporting & Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

Informants were selected using purposive sampling based on competence, certification, and authority related to information security. They were grouped into strategic informants (Head of the Information Technology Division and Head of the Cryptography and Telecommunications Operations Section), who addressed the Govern and Recover functions, and technical informants (First-Level Computer Associate and First-Level Cryptographer), who addressed the Identify, Protect, Detect, and Respond functions. Data were collected through interviews, direct observation, and document study, and their validity was ensured through source triangulation and technique triangulation, cross-checking interview statements against observed practices and formal documents such as policies, standard operating procedures, activity logs, and incident reports.

Table 2. Readiness Level (Tier) Criteria and Indicators

Score	Readiness Level (Tier)	Indicator
1	Tier 1 (Partial)	Cybersecurity readiness at this level is still very weak and reactive.
2	Tier 2 (Risk Informed)	Risk awareness exists, but implementation is not uniform and is not yet fully supported by formal policy.
3	Tier 3 (Repeatable)	Cybersecurity readiness is mature and standardized. Security practices are formalized through binding official documents.
4	Tier 4 (Adaptive)	The organization proactively and continuously adapts its security practices based on threat intelligence and lessons from previous incidents.

Data analysis was conducted descriptively to construct the NIST CSF Profiles. The researcher assigned a readiness tier to each Subcategory according to a scoring rubric on a scale of 1 to 4, whose indicators are summarized in Table 2. Because the average of the Subcategory scores yields decimal values, a class interval of 0.75 was computed to classify the average scores into readiness tiers, as presented in Table 3. Based on regulatory compliance needs under SPBE and the agency's strategic role as Data Steward, Tier 3 (Repeatable) was set as the target profile for all functions. A gap analysis was then performed to measure the difference between the target and current profiles, identifying the functions with the largest gaps as improvement priorities. Finally, strategic recommendations were formulated by referring to the Implementation Examples in the NIST CSF 2.0 Reference Tool [15], adjusted to the resources and capabilities of the agency.

Table 3. Average Score Ranges for Readiness Levels (Tiers)

Average Score Range	Readiness Level (Tier)
1.00 - 1.74	Tier 1 (Partial)
1.75 - 2.49	Tier 2 (Risk Informed)
2.50 - 3.24	Tier 3 (Repeatable)
3.25 - 4.00	Tier 4 (Adaptive)

3. RESULTS AND DISCUSSION

This section presents the results of the cyber resilience readiness measurement at Diskominfo Mojokerto City using NIST CSF 2.0, organized into the general profile of the object, the current readiness profile and gap analysis, function-level discussion with detailed recommendations, and a priority summary.

3.1 Overview of the Research Object

Diskominfo Mojokerto City serves as the backbone of SPBE implementation, responsible for managing the data center, maintaining the intra-government network connecting all Regional Government Organizations, and developing public-service and administrative applications. Its high operational dependence on digital infrastructure is matched by escalating cyber threats; historical incidents, such as web defacement affecting the Heroes' Cemetery site and the Environmental Agency profile, confirm that cyber threats are a daily operational risk. To manage these threats, the agency operates a Computer Security Incident Response Team (CSIRT). Nevertheless, robust cyber resilience requires a comprehensive approach that extends beyond reactive response to strategic governance, asset protection, and disaster recovery planning.

3.2 Current Readiness Profile and Gap Analysis

Table 4. Recapitulation of NIST CSF 2.0 Cyber Resilience Readiness Scores per Function

Function	Current Profile	Target Profile	Gap
Govern	2.47	3.00	0.53
Identify	1.97	3.00	1.03
Protect	2.18	3.00	0.82
Detect	2.02	3.00	0.98
Respond	2.28	3.00	0.72
Recover	1.67	3.00	1.33
Overall Average	2.10	3.00	0.90

After all Subcategories were assessed and aggregated at the Category and Function levels, the overall cyber resilience readiness score of Diskominfo Mojokerto City reached 2.10 on a 4.00 scale, placing the agency at the Risk Informed level (Tier 2). This indicates that the organization already possesses risk awareness but has not yet implemented it uniformly or through automation.

The recapitulation of scores per function, together with the target profile and gap, is presented in Table 4 and visualized in Figure 1.

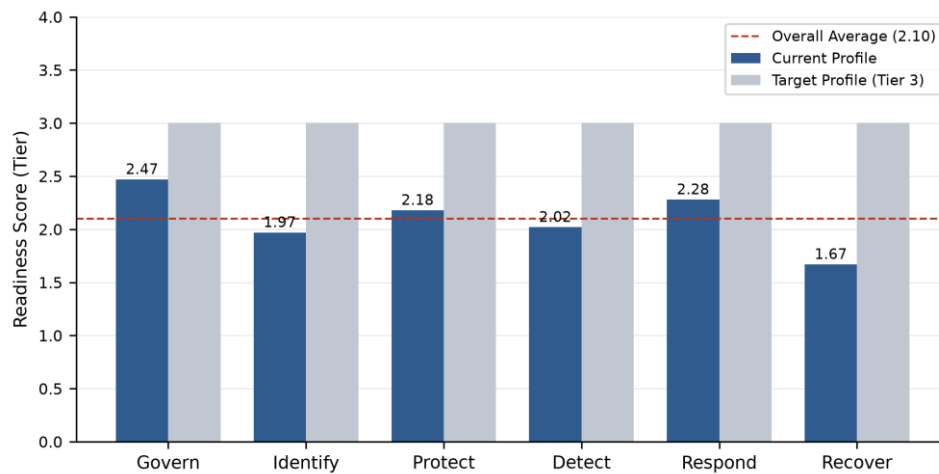


Figure 1. Cyber Resilience Readiness Profile of Diskominfo Mojokerto City

To provide a more granular view, Table 5 presents the readiness scores at the category level for all 22 categories. This breakdown reveals the specific strengths and weaknesses within each function. Strong categories such as Oversight (GV.OV, 3.00), Awareness and Training (PR.AT, 3.00), and Incident Response Reporting and Communication (RS.CO, 3.00) already reach the target, whereas Incident Recovery Plan Execution (RC.RP, 1.33), Incident Analysis (RS.AN, 1.50), and Cybersecurity Supply Chain Risk Management (GV.SC, 1.60) remain at the Partial level and constitute the most urgent improvement priorities.

Table 5. Category-Level Cyber Resilience Readiness Scores

Function	Category	Score	Tier
Govern	Organizational Context (GV.OC)	2.60	Tier 3
	Risk Management Strategy (GV.RM)	2.86	Tier 3
	Roles, Responsibilities & Authorities (GV.RR)	2.75	Tier 3
	Policy (GV.PO)	2.00	Tier 2
	Oversight (GV.OV)	3.00	Tier 3
Identify	Cybersecurity Supply Chain Risk Mgmt (GV.SC)	1.60	Tier 1
	Asset Management (ID.AM)	2.00	Tier 2
	Risk Assessment (ID.RA)	1.90	Tier 2
	Improvements (ID.IM)	2.00	Tier 2
Protect	Identity Mgmt, Authentication & Access (PR.AA)	2.00	Tier 2
	Awareness and Training (PR.AT)	3.00	Tier 3
	Data Security (PR.DS)	2.00	Tier 2
	Platform Security (PR.PS)	1.67	Tier 1
Detect	Technology Infrastructure Resilience (PR.IR)	2.25	Tier 2
	Continuous Monitoring (DE.CM)	2.20	Tier 2
	Adverse Event Analysis (DE.AE)	1.83	Tier 2
Respond	Incident Management (RS.MA)	2.60	Tier 3
	Incident Analysis (RS.AN)	1.50	Tier 1
	Incident Response Reporting & Comm. (RS.CO)	3.00	Tier 3
	Incident Mitigation (RS.MI)	2.00	Tier 2
Recover	Incident Recovery Plan Execution (RC.RP)	1.33	Tier 1
	Incident Recovery Communication (RC.CO)	2.00	Tier 2

3.3 Function-Level Discussion and Detailed Recommendations

This subsection discusses the findings of each function and presents detailed recommendations derived from the NIST CSF 2.0 Implementation Examples. Each table lists the affected subcategory, the key issue identified during assessment, and the corresponding recommended action.

3.3.1 Govern

The Govern function is the strongest (2.47), underpinned by a solid legal and administrative foundation and strong oversight (GV.OV, 3.00). However, Cybersecurity Supply Chain Risk Management (GV.SC, 1.60) is the main weakness, reflecting weak governance over external vendors, as detailed in Table 6.

Table 6. Findings and Recommendations for the Govern Function

Code	Key Issue Identified	Recommendation
GV.OC-02	Stakeholder needs and expectations are not yet formally documented.	Identify relevant internal and external stakeholders and formally document their cybersecurity expectations.
GV.OC-05	Visibility of dependent third-party services is only partial.	Create an inventory of dependencies on external resources and their relationships to functional assets.
GV.RM-07	Opportunities (positive risks) are not explored in a structured way.	Define and communicate guidance to identify opportunities within cybersecurity risk discussions.
GV.RR-03	Limited personnel capacity affects the speed of security operations.	Provide adequate human, process, and technical resources to support the cybersecurity strategy.
GV.PO-02	Existing mayoral-regulation policy is not periodically reviewed.	Set a timeline to review changes in the risk environment and recommend policy updates.
GV.SC-04	No risk-level mapping for each external service provider.	Develop supplier criticality criteria based on data sensitivity and level of access.
GV.SC-05	Third-party contracts omit technical cybersecurity obligations.	Embed all required cybersecurity and supply-chain requirements into contract language.
GV.SC-06	No procedure to verify vendor security posture before engagement.	Assess technology suitability, security capability, and risk-management practices of prospective suppliers.
GV.SC-07	The agency lacks audit capacity to evaluate third-party performance.	Monitor critical suppliers to ensure they meet security obligations through inspection and other methods.
GV.SC-08	Third parties are not involved in joint incident response.	Document the roles and responsibilities of the agency and its suppliers in incident response.
GV.SC-09	Device procurement is not verified for provenance.	Ensure software patches and updates originate only from legitimate vendors.
GV.SC-10	Authorization gap when vendor engagement ends.	Immediately disable supplier access to resources once no longer needed.

3.3.2 Identify

The Identify function scored 1.97, constrained by reliance on manual asset inventory, the absence of external threat-intelligence integration, and the lack of an independent program audit, as summarized in Table 7.

Table 7. Findings and Recommendations for the Identify Function

Code	Key Issue Identified	Recommendation
ID.AM-02	Software license/version records rely on manual spreadsheets.	Continuously monitor platforms to detect changes in software and service inventory automatically.
ID.AM-03	Internal/external network data flows have no baseline.	Maintain a baseline of communications and data flows across wired and wireless networks.
ID.AM-04	Third-party services are not specifically inventoried.	Inventory all external services used, including cloud-hosted applications.
ID.AM-07	Sensitive-data classification/labeling is not standardized.	Maintain a list of data types with defined importance to ease labeling and handling.
ID.AM-08	Device lifecycle and data destruction on retirement not standardized.	Securely sanitize data storage when hardware is retired, decommissioned, or reused.
ID.RA-01	Vulnerability and misconfiguration checks are manual.	Use automated vulnerability-management technology to identify unpatched software.
ID.RA-02	No intake of regional/global cyber threat alerts.	Configure security devices to securely receive threat-intelligence feeds and review alerts.
ID.RA-03	Threat-actor profiles and methods are not mapped.	Use threat intelligence to maintain awareness of threat actors and their TTPs.
ID.RA-07	Architecture/configuration changes are not risk-reviewed.	Implement formal documentation, review, testing, and approval of proposed changes.
ID.RA-08	No channel to receive vulnerability reports from the public.	Assign responsibility to process and respond to externally reported vulnerability disclosures.
ID.RA-09	Product authenticity/security not assessed before procurement.	Assess authenticity and security of critical tech products before acquisition.
ID.RA-10	Cyber risk of critical vendors not evaluated before contract.	Conduct supplier risk assessment against compliance and cybersecurity requirements.
ID.IM-01	Program effectiveness never independently audited.	Invest in independent audits of the cybersecurity program to find improvement areas.
ID.IM-02	Cyber Drill results not documented into improvements.	Identify improvements for future incident response from exercise evaluations.
ID.IM-03	SOPs not periodically reviewed against field dynamics.	Review policies, processes, and procedures annually considering lessons learned.
ID.IM-04	Agency lacks a BCP and Disaster Recovery Plan (DRP).	Establish operational contingency plans, including incident response and disaster recovery.

3.3.3 Protect

The Protect function scored 2.18. While awareness and training are strong (PR.AT, 3.00), defensive architecture is weakened by the absence of comprehensive encryption, non-standardized authentication, and fully manual configuration and patching (PR.PS, 1.67), as detailed in Table 8.

Table 8. Findings and Recommendations for the Protect Function

Code	Key Issue Identified	Recommendation
PR.AA-01	Credential management lacks strict access-lifecycle tracking.	Initiate access-request processes for staff/contractors and track and review fulfillment.
PR.AA-02	Shared administrator accounts weaken identity verification.	Issue distinct, unique credentials per individual to prevent credential sharing.
PR.AA-03	Multi-factor authentication is not mandatory for system access.	Require multi-factor authentication to validate users.
PR.AA-04	User identity assertions are not protected in a standard way.	Protect identity assertions conveyed via single sign-on systems.
PR.AA-05	Access privileges are not auto-reviewed/revoked on role change.	Periodically review logical access privileges and promptly revoke on role change.
PR.DS-01	Data at rest is unencrypted, protected only by network boundaries.	Use encryption, digital signatures, and hashing to protect stored-data confidentiality and integrity.
PR.DS-02	Data-in-transit is not fully protected by strong encryption.	Use encryption and cryptographic techniques to protect communications.
PR.DS-10	Data in use is vulnerable to interception within the platform.	Protect data in use from access by other users or processes on the same platform.
PR.DS-11	Backup restoration testing is not routinely standardized.	Test backups and restoration procedures for all data sources at least annually.
PR.PS-01	OS/network configuration is manual, without centralization.	Establish, test, and maintain hardened configuration baselines.
PR.PS-02	Patching depends heavily on manual admin execution.	Perform routine and emergency patching within defined timeframes.
PR.PS-03	Hardware replacement not evaluated by risk profile.	Plan hardware maintenance support and end-of-life management.
PR.PS-04	Security logs are scattered across local servers.	Configure services to securely share logs with monitoring infrastructure.
PR.PS-05	No endpoint protection against unauthorized software.	Allow exclusively approved software installation on platforms.
PR.PS-06	Security not integrated into in-house app development.	Secure all in-house-developed software to minimize vulnerabilities.
PR.IR-01	Network segmentation is insufficient against lateral movement.	Logically segment the network by trust boundaries to limit lateral movement.
PR.IR-03	Infrastructure lacks redundancy if the main server fails.	Use high-availability components such as backup storage and power.
PR.IR-04	Availability is vulnerable to overload with no auto-scaling.	Forecast future workload and scale resources automatically.

3.3.4 Detect

The Detect function scored 2.02. Detection remains basic due to the absence of centralized log aggregation, which forces reactive manual correlation, and there is limited visibility into the vendor ecosystem, as summarized in Table 9.

Table 9. Findings and Recommendations for the Detect Function

Code	Key Issue Identified	Recommendation
DE.CM-03	Internal anomaly monitoring cannot detect insider threats.	Use behavior analytics to detect anomalous user activity and mitigate insider threats.
DE.CM-06	No technical mechanism to monitor third-party operations.	Monitor administrative and maintenance activity of external providers.
DE.CM-09	Monitoring focuses on uptime, not runtime execution.	Monitor software configuration for deviations from the security baseline, and monitor hardware.
DE.AE-02	Anomaly-notification review is purely manual.	Use SIEM or other tools to monitor suspicious log activity.
DE.AE-03	Scattered logs hinder anomaly correlation by the CSIRT.	Use event-correlation technology (SIEM) to consolidate information from multiple sources.
DE.AE-04	Operational impact estimation is done manually.	Use SIEM or detection tools to estimate impact and scope of damage.
DE.AE-06	Crisis-status delegation lacks ticket automation.	Configure security software to automatically create and assign incident tickets.
DE.AE-07	Investigation is not integrated with the threat landscape.	Provide threat-intelligence feeds securely to technology, processes, and personnel.
DE.AE-08	No standard metrics for declaring incidents.	Apply incident criteria to known/assumed suspicious-activity characteristics.

3.3.5 Respond

The Respond function is relatively strong at 2.28, supported by a solid SOP and CSIRT (RS.CO, 3.00). However, technical execution still relies heavily on manual analysis and lacks digital-forensic readiness (RS.AN, 1.50), as detailed in Table 10.

Table 10. Findings and Recommendations for the Respond Function

Code	Key Issue Identified	Recommendation
RS.MA-01	Field execution depends heavily on external authority.	Proactively initiate additional cybersecurity plans as needed (e.g., business continuity).
RS.MA-05	Recovery initiation lacks standard technical criteria.	Apply recovery criteria to known/assumed incident characteristics.
RS.AN-03	Root-cause analysis relies on manual local-log reading.	Analyze incidents deeply to find underlying systemic root causes.
RS.AN-06	Investigations lack chain-of-custody integrity.	Require responders to log every action and keep records tamper-evident.
RS.AN-07	Log trails lack cryptographic integrity mechanisms.	Collect, maintain, and preserve integrity of all incident data and metadata.
RS.AN-08	Incident impact scale is estimated manually.	Run automated tools on target systems to search for indicators of compromise.
RS.MI-01	Network isolation (containment) is done manually.	Use security technology and network features to perform containment.
RS.MI-02	Eradication is done one by one after containment.	Configure security technology and infrastructure to execute eradication actions.

3.3.6 Recover

The Recover function is the most critical vulnerability (1.67). The absence of a formal Disaster Recovery Plan, backup restoration without integrity verification, the lack of post-incident evaluation, and reliance on informal communication make recovery reactive and dependent on individual capacity, as detailed in Table 11.

Table 11. Findings and Recommendations for the Recover Function

Code	Key Issue Identified	Recommendation
RC.RP-01	Absence of a formal DRP makes recovery purely reactive.	Ensure all recovery-responsible individuals know the recovery plan and required authorizations.
RC.RP-02	Restoration priorities are set situationally.	Select recovery actions based on criteria defined in the incident-response plan.
RC.RP-03	Backups are restored without malware verification.	Check restoration assets for indicators of compromise and integrity issues before use.
RC.RP-04	Post-incident evaluation not used to update SOPs.	Monitor recovered-system performance to verify adequacy of restoration.
RC.RP-05	No metrics to verify asset cleanliness before go-live.	Verify correctness and adequacy of restoration before reactivating systems.
RC.RP-06	No formal criteria to declare recovery complete.	Produce an after-action report documenting the incident, actions, and lessons learned.
RC.CO-03	Restoration updates to leadership use informal channels.	Periodically update senior leadership on recovery status and progress.
RC.CO-04	Public announcements lack pre-approved message drafts.	Communicate restoration steps and measures to prevent recurrence.

3.4 Summary of Priority Recommendations

Synthesizing the function-level findings, Table 12 summarizes the highest-priority recommendation for each function to guide the transition from a reactive, manual posture toward automated and formalized cyber resilience.

Table 12. Summary of Strategic Recommendations per Function

Function	Priority Recommendation
Govern	Formalize vendor supply-chain security policies and embed strict cybersecurity requirements into external contracts.
Identify	Implement lifecycle-based asset management and integrate external threat intelligence to strengthen risk visibility.
Protect	Enforce comprehensive data encryption, adopt multi-factor authentication (MFA), and establish centralized patch management.
Detect	Deploy centralized log aggregation and event-correlation technology (SIEM) to accelerate anomaly detection.
Respond	Establish digital-forensic chain-of-custody procedures and automated containment/eradication tooling.
Recover	Formulate and regularly test a formal Disaster Recovery Plan (DRP), apply backup-integrity verification, and prepare a crisis-communication matrix.

CONCLUSION

This study measured the cyber resilience readiness of Diskominfo Mojokerto City using the NIST Cybersecurity Framework 2.0. The overall readiness score reached 2.10 on a 4.00 scale, placing the agency at the Risk Informed level (Tier 2) and in transition toward the ideal Repeatable target (Tier 3). Functionally, the agency is strongest in Govern (2.47), owing to a solid administrative and legal foundation, while its most critical vulnerability lies in Recover (1.67), caused by the absence of a formal Disaster Recovery Plan that renders post-incident recovery reactive and dependent on subjective personnel capacity.

The proposed strategic recommendations focus on shifting from a reactive, manual approach toward technical automation and the formalization of third-party policies. Priorities include developing and testing a Disaster Recovery Plan, applying backup-integrity verification, and

preparing a public crisis communication matrix, followed by embedding cybersecurity requirements into vendor contracts, implementing multi-factor authentication, and adopting event-correlation technologies such as SIEM and threat intelligence. Theoretically, this study demonstrates the applicability of NIST CSF 2.0 for assessing cyber resilience in local government; practically, it offers the agency an objective reference for strengthening its security posture. Future research may compare or integrate these results with other standards, such as ISO/IEC 27001 or the Information Security Index (Indeks KAMI) of BSSN, to obtain a more comprehensive governance-compliance perspective.

ACKNOWLEDGEMENTS

The authors sincerely thank the Communication and Informatics Office (Diskominfo) of Mojokerto City for granting research permission and providing objective data and access, as well as the management and technical staff for their cooperation during the interviews and observations.

REFERENCES

- [1] E. H. Ramadhani, I. K. A. Enriko, and E. L. I. P. Sari, "Kajian Strategik Manajemen Keamanan Siber terhadap Proyek Telematika di Indonesia: Studi Kasus Kebocoran Pusat Data Nasional," in *Jurnal Indonesia: Manajemen Informatika dan Komunikasi (JIMIK)*, vol. 6, no. 1, 2025.
- [2] P. Singh, S. Sirpal, and O. Pal, "Cyber resilience in e-governance: A review of strategies, challenges, and directions," in *Internet of Things (The Netherlands)*, vol. 33, Elsevier B.V., 2025.
- [3] Peraturan Presiden Republik Indonesia, *Sistem Pemerintahan Berbasis Elektronik*, 2018.
- [4] M. Alfi, N. P. Yundari, and A. Tsaqif, "Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia," *Jurnal Kajian Strategik Ketahanan Nasional*, vol. 6, no. 2, 2023.
- [5] S. T. Hossain, T. Yigitcanlar, K. Nguyen, and Y. Xu, "Cybersecurity in local governments: A systematic review and framework of key challenges," in *Urban Governance*, vol. 5, no. 1, Elsevier B.V., 2025.
- [6] Badan Siber dan Sandi Negara, "Laporan Bulanan Publik Hasil Monitoring Keamanan Siber Agustus 2025," 2025.
- [7] S. M. Alhidaifi, M. R. Asghar, and I. S. Ansari, "Cyber resilience quantification: A probabilistic estimation model for IT infrastructure," *Reliability Engineering and System Safety*, vol. 265, 2026.
- [8] Pemerintah Kota Mojokerto, "Peraturan Daerah Kota Mojokerto Nomor 5 Tahun 2020 tentang Perubahan Kedua Atas Peraturan Daerah Nomor 8 Tahun 2016 tentang Pembentukan Perangkat Daerah," 2020.
- [9] Pemerintah Kota Mojokerto, "Peraturan Wali Kota Mojokerto Nomor 78 Tahun 2022 tentang Kedudukan, Susunan Organisasi, Tugas, dan Fungsi, serta Tata Kerja Dinas Komunikasi dan Informatika Kota Mojokerto," 2022.
- [10] R. Rahman, A. Ananta, and B. Surianti, "Analisis Perbandingan Framework Keamanan Jaringan (NIST CSF, CIS Controls, ISO 27001)," 2025.
- [11] National Institute of Standards and Technology, "The NIST Cybersecurity Framework (CSF) 2.0," 2024.

- [12] T. S. Putri, N. Mutiah, and D. Prawira, "Analisis Manajemen Risiko Keamanan Informasi Menggunakan NIST Cybersecurity Framework dan ISO/IEC 27001:2013 (Studi Kasus: Badan Pusat Statistik Kalimantan Barat)," 2022.
- [13] D. Amanda, N. Mutiah, and S. Rahmayudha, "Analisis Tingkat Kematangan Keamanan Informasi Menggunakan NIST Cybersecurity Framework dan CMMI," 2023.
- [14] M. Yunella, A. D. Herlambang, and W. H. N. Putra, "Evaluasi Tata Kelola Keamanan Informasi pada Dinas Komunikasi dan Informatika Kota Malang Menggunakan Indeks KAMI," 2020.
- [15] National Institute of Standards and Technology, "NIST CSF 2.0 Reference Tool," 2024.