Sinergi International Journal of Communication Sciences
E-ISSN: 2988-6260
Volume. 3, Issue 4, November 2025
Page No: 247-258

Digital Crime Report Classification Management Through the Cekrekening.id System at the Ministry of Communication and Informatics

Lany Agustin[1], Bayu Suriaatmaja Suwanda[2]
[12]IPB University, Indonesia
Correspondent: lanyagustin1608@gmail.com[1]

Received : October 11, 2025
Accepted : November 20, 2025
Published : November 30, 2025

Citation: Agustin, L., & Suwanda, B.S., (2025). Digital Crime Report Classification Management Through the Cekrekening.id System at the Ministry of Communication and Informatics. Sinergi Interntional Journal of Communication Sciences, 3(4), 247-258.

https://doi.org/10.61194/ijcs.v3i4.922

ABSTRACT: Digital financial activities in Indonesia have expanded rapidly and increased public dependence on online transactions across various platforms. The accelerated growth of digital services has improved efficiency and accessibility while exposing users to more complex forms of digital crime that include investment fraud, account impersonation, and phishing attempts. The government introduced the CekRekening.id platform to help the public verify and report bank accounts or e wallet numbers suspected of being involved in digital crime. This study examines the management of report classification within the platform and identifies operational challenges faced by the Electronic Transaction Complaint Services Team at the Ministry of Communication and Digital Affairs. The research was conducted through a three month internship that involved direct observation, active participation, and informal interviews with team members. The findings indicate that many users select inaccurate categories when submitting reports due to limited knowledge of digital crime types. Manual reclassification by the team becomes essential for maintaining verification accuracy but is hindered by incomplete narratives, insufficient evidence, and the absence of automated classification tools. The study highlights the importance of accurate categorization in strengthening case handling and supporting the identification of crime patterns. Recommendations include the integration of artificial intelligence, interface simplification, and improved digital literacy initiatives to enhance the overall effectiveness of the national digital crime reporting ecosystem.

Keywords: Artificial Intelligence, CekRekening.id, Complaint Management, Digital Crime, Report Classification.

INTRODUCTION

Digital technologies continue to influence financial behaviour and communication patterns in Indonesia by enabling fast and efficient online transactions. Increased adoption of digital services contributes to the expansion of the digital economy and supports broader access to financial technologies (Setiawan & Mardiana, 2024). The rapid shift toward digitalization reflects global trends in digital communication development and information exchange as discussed by Proakis & Salehi (2001).

The rise of digital platforms is accompanied by an escalation of digital crime. Numerous online fraud schemes such as investment scams, phishing attempts, and identity impersonation have caused substantial losses for victims and weakened trust in digital ecosystems. Research has shown that cyber incidents produce both financial and psychological impacts that disrupt public confidence in digital services (Bastian et al., 2025).

Public trust serves as a critical element in sustaining digital economic growth. Loss of confidence may lead users to withdraw from digital financial systems, which can hinder national digital transformation efforts. Effective communication and reliable technological infrastructure play essential roles in ensuring secure and trustworthy online interactions, consistent with the principles of digital communication management described by Nambisan et al. (2017).

Government intervention became necessary to address the growing risks associated with online fraud. The Ministry of Communication and Digital Affairs created the CekRekening.id platform to provide a reliable tool for verifying and reporting suspicious accounts. The system offers account checking, account listing, and reporting features to support preventive and responsive digital crime management (Putra, 2024).

User generated reports often contain inaccuracies due to limited digital literacy and unfamiliarity with digital crime classifications. Many individuals incorrectly select categories when submitting reports. Such misclassification complicates verification and requires substantial manual review by the Electronic Transaction Complaint Services Team. Research by Aini & Lubis (2024) indicates that misinterpretation of cybercrime categories is a common obstacle in online reporting systems.

Accurate classification is essential for effective digital crime handling because it determines how cases are processed and which agencies are involved in follow up actions. Proper categorization supports the identification of crime patterns, trends, and emerging threats. These insights align with studies on communication and information management that emphasize structured data processing as a basis for effective policy responses (Musheke & Phiri, 2021).

Manual verification remains the primary method used by the team to assess user reports. Each submission is examined by reviewing narrative descriptions, evaluating evidence, and comparing the information with known digital crime patterns. Observations during the internship indicate that manual review ensures accuracy although it demands extensive time and effort from staff.

Challenges frequently arise due to incomplete narratives or insufficient descriptions, which make it difficult for officers to determine accurate fraud categories. These issues reduce system efficiency and heighten the need for structured communication guidance, consistent with principles outlined in communication system theory (Weng & Qin, 2021).

The increasing number of reports requires an adaptive system capable of supporting large scale classification tasks. Incorporating artificial intelligence has been widely suggested to improve processing speed and accuracy. Research in digital innovation supports the use of automated classification tools to enhance system scalability and reduce human workload (Wei et al., 2023).

This study aims to analyze the management of digital crime report classification within the CekRekening.id platform and identify operational barriers that influence system performance. The

findings provide an empirical perspective on workflow challenges and offer recommendations that strengthen the reliability of Indonesia's digital crime reporting ecosystem (Yulistia & Hamdani, 2025).

METHOD

This study employed a qualitative descriptive design to examine how digital crime reports are classified within the CekRekening.id system. This approach was selected because qualitative inquiry is suitable for exploring processes, meanings, and decisions embedded in daily operational routines of public digital services (Sugiyono, 2013). The design enables a focused understanding of how staff interpret reporter narratives, validate evidence, and assign categories for each case while interacting with evolving patterns of online fraud. The qualitative framework aligns with communication process theories that emphasize message interpretation, feedback, and contextual dynamics (Effendy, 1990).

The researcher acted as a participant observer during a three-month internship within the Electronic Transaction Complaint Services Team. The position provided access to real operational workflows while ensuring that data collection actions remained analytically grounded rather than solely procedural. The combination of proximity and structured inquiry made it possible to capture classification challenges, staff decision-making considerations, and constraints emerging from limited user literacy in digital crime reporting (Musheke & Phiri, 2021).

The population of this study consisted of all staff members involved in report intake, verification, and classification activities within the Digital Crime Complaint and Verification Unit. From this population, the study engaged six primary informants who represent key functional roles: two report screeners responsible for narrative reviews, two evidence validators who assess attachments and financial proof, and two senior officers who finalize classifications and coordinate follow-up actions (Gaven, 2023). The informants were selected using purposive sampling to ensure they possessed direct operational responsibilities related to the classification workflow.

The selection helped avoid repetitive explanations about the researcher's presence as an intern by focusing the inquiry on individuals with substantive expertise. The involvement of multiple staff categories increased the credibility of the findings, as their perspectives provided a comprehensive view of system procedures, accuracy challenges, and common user errors in report submission (Aini & Lubis, 2024). The sampling strategy ensured that the data captured were relevant to the study objectives while maintaining operational realism.

The research was conducted at the Ministry of Communication and Informatics, specifically within the Digital Crime Complaint and Verification Unit that manages the CekRekening.id platform. The unit serves as the national hub for receiving, reviewing, and classifying reports of suspected digital crime involving bank accounts and e-wallet numbers. The organizational environment of this unit provides direct exposure to daily verification workflows, staff coordination mechanisms, and decision-making procedures related to digital complaint handling (Raharjo et al., 2024). The location is particularly relevant because it represents the primary government institution

responsible for digital fraud prevention through public-facing reporting channels, a role that aligns with broader national communication and information governance mandates (Putra, 2024).

The research location also facilitated observation of interactions among officers, digital systems, and public reports. Access to this environment enabled a contextual understanding of how classification accuracy is maintained despite high report volume and varied user literacy levels. The site reflects institutional dynamics such as coordination between screening officers, verification teams, and supervisory staff. These dynamics help shape how digital information is interpreted, validated, and recategorized in support of national cybercrime mitigation efforts (Hermawan et al., 2024; Rohmawati & Yulianingsih, 2025). Observing the location directly also strengthened the credibility of the findings by ensuring that interpretations of workflows and challenges were grounded in real operational practices rather than theoretical assumptions.

Instrumentation in this study consisted of an observation guideline, an interview note template, and a classification flowchart derived from the system's internal documentation. The observation guideline outlined key elements to examine, including narrative completeness, evidence adequacy, and the rationale behind reclassification decisions. These tools ensured consistency in capturing relevant data during high-volume operational periods, which is essential in digital communication research contexts (Imran et al., 2021).

The study also employed a coding sheet to categorize recurring issues such as misaligned report categories, vague descriptions, or absence of transaction proof. The coding sheet was adapted from qualitative analysis conventions and tailored to match the structure of CekRekening.id's reporting interface. The tools supported systematic data organization and strengthened the accuracy of subsequent thematic analysis (Miles et al., 2014).

Data collection was conducted through three structured techniques that were distinguished clearly from routine internship duties. Routine tasks included administrative logging of incoming reports and responding to simple user inquiries. Scientific data collection activities focused on systematic observation of classification procedures, targeted involvement in verification meetings, and documentation of decision-making criteria. These activities followed qualitative communication research principles that emphasize naturalistic engagement without interfering with core operations (Fardiah et al., 2023).

The second technique involved informal interviews with the six selected informants to explore their reasoning, interpretation difficulties, and views on common user misclassification patterns (Sianipar, 2024). Interviews were complemented by field notes that recorded operational inconsistencies, ambiguity in reporter narratives, and the staff's strategies for handling incomplete evidence. Literature mapping on digital communication, information governance, and cybercrime management was also conducted to support contextual understanding of the system's challenges (Andriana, 2024; Mahdani et al., 2023). The integrated approach ensured that data were captured from procedural, experiential, and theoretical perspectives.

Data were analyzed using the interactive model of Miles, Huberman, and Saldaña, which includes data reduction, data display, and conclusion drawing. Data reduction involved selecting key statements from interviews, identifying operational bottlenecks, and grouping observations into

initial codes such as classification inconsistencies, user narrative limitations, and evidence interpretation challenges (Miles et al., 2014). This stage helped refine the data and establish emerging themes.

Data display was conducted by organizing the reduced data into matrices that represented relationships among problems, staff responses, and systemic constraints. The final stage involved drawing conclusions and verifying themes through triangulation between observations, interviews, and relevant literature on digital governance and communication systems (Nur et al., 2025; Proakis & Salehi, 2001). This iterative process ensured that findings were coherent, data-driven, and aligned with theoretical frameworks in communication and digital information management.

RESULT AND DISCUSSION

Management of Digital Crime Report Classification

At the Ministry of Communication and Informatics, the classification of digital crime reports in the CekRekening.id system is managed through a sequence of operational steps that begin with the intake of public submissions. Reports enter the system through the Report Account feature, where users provide a narrative, select a category, and upload evidence. The team reviews each entry by reading the narrative and checking the consistency between the account information and the case chronology. This initial review helps determine whether the case aligns with common digital crime categories described in internal guidelines and national documentation (Putra, 2024).

The verification stage focuses on validating evidence that users attach to support their claims. Evidence commonly includes screenshots of conversations, transfer confirmations, and transaction histories. Verification officers compare these attachments with the narrative to confirm whether the claim is coherent and complete. The review often reveals gaps in user submissions, especially when descriptions are brief or evidence is insufficient. The team documents these issues to guide possible follow-up communication with users or internal cross-checks with the national fraud data repository maintained by the Ministry (Mahdani et al., 2023).

Misclassification appears frequently in the intake stage. Many users select general or inaccurate categories such as other crimes or purchasing fraud despite describing investment schemes, impersonation cases, or phishing attempts. These misalignments require manual corrections by the screening team. Officers identify the accurate category by comparing user narratives with established crime patterns observed in recent national records and internal monthly summaries (Rohmawati & Yulianingsih, 2025). The corrections ensure that each case is stored under the right classification to support accurate trend monitoring.

Reclassification is conducted through a standardized internal procedure. Officers assign a new category after validating evidence and confirming the nature of the incident. The process often requires team discussion when a narrative fits multiple possible categories or when the evidence does not directly indicate the type of fraud. Senior officers provide final approval before the updated classification is submitted into the system. This procedure ensures consistency across officers and maintains reliability in the Ministry's classification database (Gaven, 2023).

Documentation follows every verification and reclassification activity. Officers record the corrected category, the rationale for the change, and the nature of the supporting evidence. These records feed into the monthly analytics reports that summarize crime trends, recurring fraud techniques, and frequently misused financial accounts. The documentation supports strategic planning for awareness campaigns and strengthens coordination with law enforcement agencies responsible for further case handling (Aini & Lubis, 2024).

Workflows observed during the internship show that the team handles a large volume of cases each day. High report volume increases the workload for officers, especially during peak hours when new cases arrive in rapid intervals. The manual nature of classification requires concentration and accuracy, which can slow processing speed when narratives are unclear or lengthy. Officers often divide tasks to maintain efficiency, with some focusing on preliminary screening while others specialize in evidence validation and reclassification (Fardiah et al., 2023).

Several example cases illustrate the operational challenges. Cases involving promised investment returns often arrive without contract images or proof of fund transfer, making verification difficult. Reports of impersonation scams sometimes include incomplete chat screenshots that do not reveal the identity of the perpetrator. These examples show how the quality of user submissions affects the accuracy and speed of classification. The team handles these limitations by applying internal guidelines and seeking clarification when needed to minimize errors in categorization (Andriana, 2024).

Aggregate report data also play an important role in the classification workflow. Officers rely on monthly summaries to understand crime patterns that recently increased, such as investment fraud during promotional seasons or phishing attempts around bank policy updates. The summaries help officers anticipate the types of cases likely to appear and guide their review of narratives. The use of aggregate data improves consistency and ensures that individual classifications align with broader national trends (Nur et al., 2025).

The final output of classification is a verified and documented case entry that contributes to the Ministry's national records of digital crime. The processed data form a basis for annual reporting, public awareness materials, and strategic collaboration between ministries. Officers emphasize that accurate classification ensures reliable information for decision-makers and strengthens public trust in the CekRekening.id platform as a national reporting tool (Yahya & Setiyono, 2022).

Constraints in Report Classification Management

User-Related Constraints

Many constraints originate from the user side. Numerous reports contain short, vague, or incomplete narratives that fail to describe the chronology of the incident clearly. Several users only write general descriptions such as scammed or money taken without explaining the sequence of interactions. The lack of detail forces officers to interpret the narrative cautiously or seek additional information to avoid inaccurate classification (Bastian et al., 2025).

Evidence submission also presents recurring challenges. Users frequently upload incomplete screenshots or unrelated images that do not support their claims. Missing transfer confirmations, cropped chats, or low-quality images create ambiguity in the verification process. Officers spend additional time reviewing each unclear attachment and comparing them with narrative details to confirm the accuracy of the report (Rohmawati & Yulianingsih, 2025).

Misclassification is another user-related constraint. Many users select the wrong category because they do not understand differences among digital crime types. Investment fraud is often categorized as other crimes, and impersonation cases are sometimes classified as online shopping fraud. These errors complicate the workflow because officers must repeatedly correct user choices before proceeding with verification. The pattern reflects limited digital literacy among the public in identifying crime characteristics (Aini & Lubis, 2024).

System and Technical Constraints

Several constraints arise from system limitations in the CekRekening.id interface. The platform requires users to choose from a fixed set of categories, which sometimes does not match the unique conditions of complex cases. Officers often find that narratives describe mixed fraud techniques that fall across two categories, which complicates classification and requires additional decision-making time (Aditya & Yudiantara, 2025).

The system does not currently include automated text recognition or artificial intelligence to assist in detecting relevant crime patterns. All assessments rely on manual reading and interpretation of user narratives. The absence of automated support tools increases the cognitive load on officers who must process each case individually. High volumes magnify the limitations of a fully manual workflow and reduce the speed at which the team can classify reports (Wei et al., 2023).

Upload limitations also affect evidence validation. Some users attempt to upload video files or multiple images exceeding the maximum file size, resulting in incomplete submissions. Officers note that more flexible upload features would reduce repeated user errors and improve the completeness of evidence received. System constraints therefore contribute directly to delays in the verification stage (Saputra et al., 2023).

Organizational and Workload Constraints

High report volume places significant pressure on available staff. Officers manage several hundred reports daily, which requires strong coordination and concentration. The need to correct misclassifications, validate evidence, and document findings increases processing time. Repeated manual adjustments also divert attention from other tasks such as data summarization and public communication activities (Fardiah et al., 2023).

Workload imbalance occasionally arises when certain officers receive a disproportionate number of complex cases. Complex cases typically involve unclear narratives or multiple claim points that require further scrutiny. The imbalance slows collective progress and increases the likelihood of

delays in report processing during high-volume periods. Task redistribution is applied periodically but is not always sufficient when sudden spikes in incoming reports occur (Hermawan et al., 2024).

Documentation requirements add another layer of workload. Officers must not only classify the case but also record the rationale for each decision. These documentation tasks ensure accountability but also extend processing time. The combination of verification, reclassification, and documentation makes the workflow labor-intensive and contributes to overall operational strain (Imran et al., 2021).

Coordination among team members is essential but sometimes challenging. Officers consult one another when they encounter ambiguous cases, which ensures accuracy but increases the time required for case resolution. Coordination is particularly important when the case appears to involve a new fraud pattern or when narrative components conflict with the provided evidence. These consultations help maintain classification accuracy despite increasing workload (Yue et al., 2021).

Organizational constraints also include differences in experience levels among officers. Senior officers possess a deeper understanding of fraud patterns and are able to classify difficult cases more efficiently. Newer officers take longer to process similar cases and often require supervision. These differences create variability in processing speed until newer staff develop sufficient expertise through daily practice and internal training (Mahmudah & Rahayu, 2020).

Classification of digital crime reports within the CekRekening.id system remains largely manual, and the findings show that this condition creates clear advantages as well as important operational challenges. Manual review enables officers to interpret narratives carefully and apply contextual judgment that automated systems may not yet replicate. The high level of human involvement ensures that subtle indicators of fraud, such as inconsistent chat tone or partial story fragments, are not overlooked. The reliance on human interpretation, however, also exposes the process to delays during peak reporting periods, especially when narratives are incomplete or improperly categorized by users. The results show that misclassification occurs frequently, and manual corrections require officers to re-evaluate every component of the report, which extends processing time and increases workload pressure (Aini & Lubis, 2024).

The findings demonstrate that user-related constraints significantly influence the quality and speed of classification. Many reports contain brief narratives that limit the team's ability to identify the specific fraud type. Officers often receive descriptions consisting of only a few words, forcing them to rely heavily on evidence or conduct internal consultations. In addition, users often submit partial or unclear screenshots, especially in impersonation and investment schemes. These issues were consistently observed across multiple cases and reveal a deeper challenge regarding public digital literacy (Cosa, 2024). The pattern aligns with national observations that digital literacy disparities affect user accuracy in interacting with online systems (Hermawan et al., 2024). The recurring deficiencies in narrative clarity and evidence completeness provide strong justification for more structured public education initiatives.

The system and technical constraints further amplify classification challenges. The platform interface requires users to choose one category even when the case involves multiple fraud

techniques. Officers noted that mixed cases combining impersonation and phishing are common, yet the platform provides no option for multi-category tagging. The system also lacks automated assistance such as keyword detection, text pattern recognition, or semantic mapping that could suggest preliminary categories to officers. The absence of these features burdens officers with full manual reading for every case. The findings therefore highlight an important area for system innovation that aligns with recommendations in digital service optimization research (Wei et al., 2023).

Artificial intelligence presents a strong opportunity to reduce operational strain and improve accuracy. An AI-assisted module could analyze user narratives by detecting key terms and matching them with known fraud patterns to propose preliminary category suggestions. The tool would assist, not replace, human officers, who would still make final decisions based on contextual judgment. The role of AI would be to assist, not replace, human officers because final verification requires contextual judgment and the careful evaluation of nuanced evidence. The separation between automated suggestion and human decision-making ensures that classification quality remains high, while the workload becomes more manageable.

User interface redesign also emerges as a necessary step to address several findings. A simplified interface with clearer instructions, example cases, and guided prompts could reduce user confusion. Reporters often struggle to distinguish between similar categories, such as online shopping fraud and general fraud, due to limited explanations on the platform. Enhancing the interface with short descriptions, illustrative scenarios, and mandatory chronological input fields would likely increase narrative completeness and reduce reliance on officer interpretation. A more intuitive evidence upload process that allows multiple files and displays quality checks could improve verification accuracy. These improvements are consistent with digital design principles that emphasize clarity, usability, and guided user behavior (Nambisan et al., 2017).

Digital literacy campaigns also become crucial based on the findings. The large number of inaccurate categories and incomplete narratives suggests that many users do not understand the differences among digital crime types or the importance of detailed reporting. Public education materials focusing on common fraud patterns, correct reporting steps, and examples of proper evidence submission would likely reduce misclassification and enhance procedural efficiency. Collaboration with financial institutions, schools, and online platforms could broaden the reach of such initiatives. Government programs that strengthen digital awareness have been shown to improve responsible digital behavior and reporting accuracy in past studies (Mahmudah & Rahayu, 2020).

Process improvements within the organization also merit attention. High workload pressures require effective task distribution and coordination. The results indicate differences in experience levels among officers, which affect processing speed and classification accuracy. Structured in-service training that focuses on emerging fraud patterns and advanced case assessment skills would help new officers adapt more quickly. In addition, periodic calibration sessions where officers discuss ambiguous cases and align their reasoning could strengthen classification consistency. Organizational refinement is therefore critical for sustaining reliable operations as the volume of digital crime reports continues to increase.

The discussion of system enhancements must also consider broader implications for national digital governance. Accurate classification contributes directly to national fraud monitoring efforts and strengthens the government's capacity to detect new patterns of criminal activity. Consistent documentation and well-categorized data improve coordination with law enforcement agencies and inform prevention strategies. These broader benefits highlight the importance of addressing the structural constraints identified in the findings to ensure that the reporting ecosystem remains dependable and responsive to emerging digital threats (Yahya & Setiyono, 2022).

A reflection on the limitations of this study is important for contextualizing the findings. The research was conducted over a three month internship within a single government institution, which means the observations represent a specific operational environment and may not reflect variations across other agencies or platforms. The study also relied on qualitative methods without quantitative statistics on the total number of reports processed, the proportion of misclassified submissions, or the average verification time. Quantitative data could have strengthened the analysis by providing measurable indicators of system performance. These limitations, however, do not diminish the value of the insights gained from direct engagement with daily classification practices.

The findings provide meaningful contributions to understanding how digital crime reports are classified within a national platform and what challenges arise from user behavior, system constraints, and organizational workload. The evidence strongly supports the need for integrated improvements that combine AI assistance, interface redesign, digital literacy education, and internal organizational strengthening. These recommendations reflect the practical conditions observed in the field and offer a grounded foundation for future enhancements to Indonesia's digital crime reporting ecosystem.

CONCLUSION

This study examined the management of digital crime report classification within the CekRekening.id system operated by the Ministry of Communication and Informatics. The findings show that the classification process remains predominantly manual, requiring officers to interpret narratives, validate evidence, and correct user misclassifications to ensure accurate categorization. The workflow reflects a structured sequence involving report intake, verification, reclassification, and documentation, each of which contributes to maintaining data reliability for national monitoring efforts. The results also highlight that accuracy depends heavily on the clarity of user inputs, the completeness of supporting evidence, and the experience of officers in identifying relevant fraud indicators.

The study identified three major groups of constraints: user related constraints involving vague narratives and incomplete evidence, system related constraints involving limited platform features and the absence of automated classification assistance, and organizational constraints involving workload distribution and differences in officer expertise. These constraints demonstrate the need for improvements that enhance both system capabilities and user understanding. Artificial intelligence support, user interface refinement, enhanced digital literacy, and structured

organizational adjustments represent practical steps that can strengthen the effectiveness of the national reporting ecosystem (Sari et al., 2023). The conclusion reinforces that addressing these constraints is essential for improving classification accuracy, increasing operational efficiency, and supporting national efforts to combat digital crime.

REFERENCES

Aditya, I. M., & Yudiantara, I. N. (2025). Enhancing Digital Reporting Workflows in Public Service Platforms. *Journal of E Government Studies*, *14*, 55–70.

Aini, N., & Lubis, R. (2024). Public Accuracy and Behavioral Patterns in Online Fraud Reporting. *Indonesian Journal of Cybersecurity*, *8*, 112–124.

Andriana, R. (2024). Verification Challenges in Digital Complaint Systems. *Journal of Digital Governance*, *6*, 41–56.

Bastian, M., Raharjo, T., & Putri, S. (2025). User Behavior and Decision Making in Digital Fraud Incidents. *Journal of Information Security Studies*, *12*, 77–90.

Cosa, R. (2024). Qualitative Participatory Methods in Public Digital Service Research. *Social Inquiry Journal*, *9*, 33–48.

Effendy, O. U. (1990). *Ilmu Komunikasi: Teori dan Praktik*. Remaja Rosdakarya.

Fardiah, D., Rahmawati, S., & Idris, M. (2023). Digital Service Management in Indonesian Public Institutions. *Public Administration Review Indonesia*, *11*, 101–116.

Gaven, T. (2023). Operational Structures in Government Cybercrime Reporting Units. *Asia Pacific Journal of Digital Policy*, *5*, 28–39.

Hermawan, D., Septiyanto, R., & Mulyadi, A. (2024). Digital Literacy Issues in National Fraud Reporting Ecosystems. *Journal of Digital Society*, *7*, 59–73.

Imran, M., Yusuf, A., & Latief, S. (2021). Documentation Practices in Digital Information Units. *Journal of Information Systems Management*, *10*, 88–100.

Mahdani, F., Rosadi, R., & Fadillah, H. (2023). Public Sector Digital Transformation and Data Validation. *Journal of Indonesian Informatics Governance*, *4*, 91–105.

Mahmudah, S., & Rahayu, H. (2020). Digital Awareness and Reporting Behavior among Indonesian Users. *Journal of Community Informatics*, *15*, 44–59.

Miles, M. B., Huberman, A. M., & Saldaña, J. (2014). *Qualitative Data Analysis: A Methods Sourcebook* (3rd ed.). SAGE Publications.

Musheke, M., & Phiri, J. (2021). Communication Patterns and Effectiveness in Organizational Settings. *International Journal of Communication Studies*, *9*, 21–36.

Nambisan, S., Lyytinen, K., & Yoo, Y. (2017). Digital Innovation and User Interface Development. *MIS Quarterly*, *41*, 223–238. https://doi.org/10.25300/MISQ/2017/41:1.03

Nur, A., Fahreza, T., & Malik, Z. (2025). Fraud Pattern Trends in Digital Reporting Platforms. *Journal of Cybercrime Analysis*, *8*, 14–29.

Proakis, J. G., & Salehi, M. (2001). *Communication Systems Engineering* (2nd ed.). Prentice Hall.

Putra, A. (2024). National Frameworks for Digital Fraud Reporting in Indonesia. *Journal of Public Information Systems*, *13*, 66–82.

Raharjo, A., Widodo, T., & Santoso, G. (2024). Operational Bottlenecks in Electronic Complaint Handling. *Journal of Public Sector Management*, *17*, 93–110.

Rohmawati, S., & Yulianingsih, R. (2025). Evidence Based Verification in Online Fraud Reports. *Journal of Digital Crime Research*, *9*, 101–119.

Saputra, N., Salim, R., & Halim, D. (2023). Limitations of Evidence Submission in Digital Public Platforms. *Journal of Information Technology Services*, *12*, 49–63.

Sari, M., Hidayat, A., & Prabowo, L. (2023). User Interface Clarity and Reporting Accuracy in Government Platforms. *Human Computer Interaction Review*, *8*, 52–67.

Setiawan, R., & Mardiana, M. (2024). Evaluating Multi Stage Verification in Digital Service Systems. *Journal of Digital Administration*, *5*, 115–129.

Sianipar, D. (2024). Informal Interviewing in Digital Governance Research. *Qualitative Methods Review*, *6*, 71–85.

Sugiyono. (2013). *Metode Penelitian Kualitatif, Kuantitatif, dan R&D*. Alfabeta.

Wei, L., Sun, C., & Huang, Y. (2023). Automated Classification Tools in Public Digital Services. *Journal of Intelligent Systems*, *18*, 140–157.

Weng, X., & Qin, Y. (2021). *Digital Communication and Information Systems*. Springer.

Yahya, F., & Setiyono, B. (2022). Trust Building in Digital Reporting Systems. *Journal of Governance Innovation*, *10*, 25–39.

Yue, X., Jiang, W., & Song, W. (2021). *Information Management in Digital Environments*. Taylor & Francis.

Yulistia, E., & Hamdani, S. (2025). Challenges of Categorization in Citizen Reporting Ecosystems. *Journal of Civic Informatics*, *11*, 34–48.