ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

IMPLEMENTATION AND IMPACT OF INTELLIGENCE REPORT WRITING: TOWARDS AN INTERVENTION PROGRAM

Renbo Donasco Leyson
Author, Philippine College of Criminology

Article DOI: https://doi.org/10.36713/epra25259
DOI No: 10.36713/epra25259

ABSTRACT

This study investigated the implementation and impact of intelligence report writing among selected Philippine National Police (PNP) personnel, particularly in Police Regional Office 8 (PRO8), to propose an intervention program and enhance reporting practices. Intelligence reports are critical in ensuring timely, accurate, and ethical information for operational decision-making. However, challenges such as inaccuracies, malicious reporting, and security breaches compromise the integrity of intelligence outputs. Using a Sequential Explanatory Mixed Methods Design, the study quantitatively assessed the implementation level of the guiding principles – accuracy, clarity, completeness, and timeliness – among PNP personnel and confidential unit members, followed by qualitative data gathered from high-ranking officials to understand the impact and verification processes of intelligence reporting.

The study revealed that the guiding principles of intelligence writing – accuracy, clarity, completeness, and timeliness – are generally very much implemented across respondents, with high-ranking officials and Confidential Unit members showing strong adherence to professional standards. This indicates a high level of competence and organizational discipline in intelligence documentation. However, PNP personnel rated the implementation as moderate, suggesting areas for improvement in data verification, clarity of communication, and timeliness of report submission. The findings also showed that inaccuracies, security breaches, and malicious reporting have a very much effective impact on the overall efficiency of security operations. These issues can lead to poor decision-making, coordination problems, and loss of credibility. The study concludes that maintaining information accuracy, confidentiality, and authenticity is crucial for operational success and public trust. It recommends continuous training, strict supervision, improved verification mechanisms, and stronger security protocols to enhance the reliability and effectiveness of intelligence operations.

KEYWORDS: *Intelligence Report Writing, Implementation, PNP, Security Operations, Intervention Program*

I. INTRODUCTION

Effective policing in the 21st century increasingly relies on the accuracy, clarity, and timeliness of intelligence reports. These documents are foundational to operational planning, strategic decision-making, and the overall success of law enforcement agencies in preventing and combating crime (International Association of Chiefs of Police). This study provides an overview of the critical role of intelligence report writing within the Philippine National Police (PNP), with a specific focus on its implementation and impact in Police Regional Office 8 (PRO8). The core aim is to identify existing practices, discern challenges (Skipanes et al., 2025), and understand the consequences of intelligence reporting quality on security operations.

A significant gap exists in understanding the practical application of standardized intelligence report writing principles at the regional and local levels within the PNP, despite established national guidelines. While the importance of accurate intelligence is acknowledged (BlueForce Learning, 2025), there is a need to empirically assess how guiding principles—such as accuracy, clarity, completeness, and timeliness—are implemented by PNP personnel and to measure the actual impact of these reports on operational effectiveness and outcomes. This study addresses the need to bridge this gap by systematically evaluating current intelligence reporting mechanisms in PRO8. The findings will inform the development of a targeted intervention program designed to enhance the quality of intelligence reports, thereby improving the efficacy and accountability of police operations in the region.

Recent evaluations underline the importance of formal oversight mechanisms and transparent governance to sustain accountability in intelligence organizations. Government audits and semi-annual inspector general reports emphasize the need for clear oversight expectations, documented procedures, and tools that enhance accountability for intelligence activities (U.S. Government Accountability Office, 2021; U.S. Intelligence Community Inspector General, 2019–2020). These reviews show that institutionalizing oversight—through audits, inspectorates, and legislated reporting—helps deter misuse, improves internal controls, and sustains public confidence while balancing necessary secrecy.

In the Philippines, the Philippine National Police (PNP) officially champions intelligence-led policing as a primary strategy to address criminality and maintain peace and order (Philippine Information Agency [PIA], 2025). The organization periodically updates its operational procedures, including those related to intelligence, to align with contemporary policing demands and

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

emerging security challenges (PNP Anti-Kidnapping Group, 2021). However, a critical gap often lies in the translation of these national-level policies and guidelines into consistent, effective practices at the operational levels across the archipelago.

Human source handling and immediate field-level corroboration remain core safeguards against misinformation. Modern HUMINT certification and training programs emphasize source vetting, placement review, and routine field–analyst feedback loops as best practice for improving source reliability and reducing single-source dependency. Practitioner training materials and national training catalogs highlight the role of standardized HUMINT tradecraft in strengthening analytic confidence and operational security (CISA, 2024).

Police Regional Office 8 (PRO8) is mandated to implement PNP policies and execute law enforcement operations within the Eastern Visayas region, guided by national operational procedures (PNP Anti-Kidnapping Group, 2021). While specific, publicly available research-based data pinpointing gaps exclusively within PRO8's intelligence report writing processes may be scarce, the challenges identified at the national level often permeate regional commands. The actual setting of this study, PRO8, presents an opportunity to investigate these potential gaps at a localized level.

The challenges in the place of study may include ensuring that all intelligence personnel consistently adhere to the principles of accuracy, clarity, completeness, and timeliness in their reports amidst varying operational demands and resource availability. The impact of intelligence report quality on sensitive cases within the region highlights the critical need for impeccable reporting. Based on available data regarding the general operational landscape and the PNP's commitment to target-driven operations (PIA, 2025), the effectiveness of PRO8 in combating local crime and security threats is directly influenced by the actionable intelligence its units produce. This study seeks to identify specific gaps in the implementation and impact of intelligence report writing within PRO8. By understanding these localized challenges—be they related to training, resource allocation, supervision, or systemic issues—the research can lay the groundwork for proposing contextually relevant system enhancements and interventions, directly addressing the needs of the personnel and the operational demands within Eastern Visayas.

specific local literature exclusively focused on the implementation and impact of intelligence report writing remains limited, existing Philippine sources from law enforcement training materials, academic publications, and public ethics frameworks collectively highlight the crucial role of accurate, timely, and ethical reporting in intelligence operations. Materials such as Lesson 14 – Intelligence Report Writing (n.d.), widely used in police training modules, emphasize clarity, conciseness, and factual accuracy to ensure intelligence outputs are actionable and support evidence-based decision-making. These reports are foundational to operational effectiveness, inter-agency coordination, and the enforcement of national security mandates.

The modernization of intelligence operations is not solely dependent on technology and leadership but also on the legal and policy framework that governs them. Outdated laws and unclear operational mandates can hinder cooperation, slow decision-making, and create legal ambiguities that impede effective intelligence work. Dela Cruz and Bautista (2022) argued that legislative reforms are essential for aligning intelligence protocols with contemporary security threats, particularly in the context of cyber operations and hybrid warfare. Similarly, Patel (2019) highlighted that clearly defined inter-agency responsibilities within national security policies minimize jurisdictional conflicts and improve accountability. A more recent study by Ocampo and Rivera (2023) emphasized that incorporating community engagement into official intelligence policy not only broadens the information base but also increases public trust in national security institutions.

In sum, the reviewed literature emphasizes that effective intelligence operations rest on three interdependent pillars: ethical and accurate reporting, strong leadership and organizational culture, and a responsive legal-policy framework. Local training materials and ethical mandates provide a foundation for accuracy, professionalism, and public accountability, while empirical studies affirm that trust, communication, and leadership directly influence operational efficiency and report quality. Furthermore, contemporary scholarship emphasizes that modernization efforts must include legislative reforms to eliminate procedural ambiguities, strengthen inter-agency cooperation, and integrate community participation. Collectively, these insights point to the necessity of a holistic approach, one that aligns ethical standards, organizational practices, and legal structures, to ensure that intelligence agencies can meet evolving security demands with integrity, precision, and public trust.

The review of both foreign and local literature reveals converging themes and contextual differences in the implementation and impact of intelligence report writing. Across international and Philippine sources, there is a shared understanding that intelligence reports serve as critical tools in decision-making processes, particularly in law enforcement, security, and policymaking contexts. Common principles emphasized include clarity, accuracy, timeliness, and ethical standards, which are vital to ensuring the reliability and utility of intelligence outputs.

Foreign literature provides extensive theoretical and empirical insights into the standards and best practices of intelligence report writing. Authors such as Ratcliffe (2007) and Zegart (2022) highlight frameworks like the BLUF (Bottom Line Up Front) and stress the importance of actionable, tailored content for decision-makers. Additionally, emerging challenges such as information overload, language barriers, and the integration of artificial intelligence are thoroughly explored in global contexts, reflecting the increasing complexity of intelligence work in the digital age.

Local literature, though more limited in volume and scope, echoes many of these concerns. Philippine sources, such as Lesson 14 – Intelligence Report Writing (n.d.), reiterate the importance of clear and concise reporting within law enforcement institutions.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

Ethical standards grounded in Republic Act No. 6713 (n.d.) reinforce the need for professionalism and accountability in intelligence work. Moreover, academic contributions like Estrellado and Miranda (2023) offer relevant discussions on the ethical use of technology in writing—an area increasingly relevant in intelligence contexts.

The implementation of intelligence report writing in foreign contexts is guided by established frameworks and methodologies. The intelligence cycle itself—planning, collection, processing, analysis, dissemination, and evaluation—provides the overarching structure, with reporting being a crucial dissemination and evaluation component. Standardized reporting structures, such as S.A.L.U.T.E. reports or specific CTI report formats, aim to promote clarity and consistency, though they vary by agency and purpose. Many intelligence communities adhere to formal analytic tradecraft standards, like the U.S. Intelligence Community Directive (ICD) 203 or the UK's Professional Development Framework, which mandate objectivity, timeliness, and rigorous analytical practices. A significant aspect of this tradecraft is the clear communication of uncertainty, using tools like the UK's PHIA Probability Yardstick and Analytical Confidence Ratings to convey the likelihood and reliability of assessments.

In the Philippines, the intelligence community comprises key agencies like the National Intelligence Coordinating Agency (NICA), Armed Forces of the Philippines (AFP) intelligence services, Philippine National Police (PNP) intelligence units, and the National Bureau of Investigation (NBI). NICA plays a central coordinating role, tasked with integrating government intelligence activities and preparing estimates for national policy. The National Intelligence Committee (NIC) advises NICA, particularly in preparing the National Intelligence Estimate (NIE). Administrative Orders, such as AO No. 68 (2003) and AO No. 7 (2017), have aimed to strengthen NICA's and the NIC's coordinating functions to create a more cohesive intelligence apparatus.

The implementation of intelligence reporting within the Philippine security sector follows specific agency guidelines. The PNP utilizes the Information Report (IR) as a basic format, emphasizing principles of Accuracy, Brevity, and Clarity/Completeness (the "ABC's of IR"), mirroring international standards. PNP report writing involves preparation, writing, and editing stages, with a focus on human source management and timely dissemination. The AFP, particularly through its Information Operations manual (PAM 3-06, 2022), underscores the necessity of accurate and timely intelligence for effective decision-making, integrating intelligence support throughout its Military Decision-Making Process. NICA, as the primary coordinating body, orchestrates intelligence fusion and provides regular threat assessments to inform national policy.

The impact of intelligence reports in the Philippines is evident in counter-terrorism and internal security operations conducted by the DND, AFP, and PNP. NICA's intelligence has reportedly contributed to neutralizing terrorists, and AMLC financial intelligence aids in disrupting terrorist financing. Within law enforcement, PNP intelligence reports (CRIMINT, INSINT, PUSINT) are vital for crime prevention and investigation. NICA's estimates are intended to inform national security policy formulation by the President and NSC. There's also a growing recognition of intelligence informing public communication strategies for peace and order.

Despite these impacts, Philippine intelligence reports have faced criticism. Concerns have been raised about the quality and alleged politicization of some NICA reports, particularly regarding "red-tagging," which can undermine credibility and have human rights implications. An overemphasis on internal security at the expense of external strategic intelligence has also been suggested. Challenges in the broader criminal justice system, such as evidence collection and witness intimidation, can affect the quality of information feeding into intelligence reports. Persistent resource limitations further hinder the capacity to produce high-quality, timely intelligence. Effective intelligence dissemination and inter-agency sharing, coordinated by bodies like NICA and the NIC, are crucial but face challenges, including potential inconsistencies in data formats and the inherent risks of sharing sensitive information that require robust security protocols.

A synthesis of foreign and local literature on intelligence report writing reveals strong commonalities in core principles: clarity, accuracy, timeliness, relevance, and actionability are universally emphasized as essential for reports to effectively inform decision-making across diverse sectors. The overarching objective, both internationally and in the Philippines, is to provide intelligence that supports tactical, operational, and strategic choices. This shared understanding forms the bedrock of intelligence reporting practices globally.

Despite technological advancements, core challenges in intelligence reporting remain fundamentally human. Ensuring analytical rigor, mitigating cognitive biases, understanding audience needs, and effectively communicating complex information and uncertainty depend heavily on the skill, judgment, and integrity of human analysts. Technology is a tool, not a panacea; the "human touch" is crucial for interpreting context, ensuring strategic relevance, and upholding ethical standards. Issues like politicization are human and organizational, requiring solutions beyond technology. Furthermore, the "last mile" problem—effective dissemination to the right people at the right time and evaluating report impact—remains a critical juncture. Neglecting strategic dissemination and systematic feedback can prevent the full value of intelligence from being realized, underscoring the need for robust mechanisms to close this loop in the intelligence cycle.

Significance of the Study

Intelligence Report Writers and Analysts. This study would improve skills in intelligence report writing, leading to clearer, more concise, accurate, and impactful reports. They will benefit from identified best practices, common pitfalls, and the specific areas for improvement highlighted by the study. The intervention

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

program will provide structured guidance to enhance their capabilities.

Intelligence Unit/Department Heads/Supervisors. This study would enhanced ability to evaluate the quality of intelligence reports, identify areas for improvement within their teams, and implement effective oversight.

Decision-Makers and End-users of Intelligence Reports. The study would give access to higher quality, more reliable, and more actionable intelligence reports. This will lead to better-informed decisions, improved strategic planning, and more effective operational outcomes. When intelligence reports are well-written, clear, and comprehensive (as a result of improved writing skills among analysts), decision-makers can quickly grasp critical information, assess threats, identify opportunities, and formulate appropriate responses with greater confidence.

Training and Development Departments/institutions. The study would give Evidence-based insights to design, update, and improve existing intelligence report writing training programs. The study's findings might provide empirical data to justify the need for specific training modules and validate the effectiveness of certain pedagogical approaches.

PRO Intelligence Unit. This study would enhanced organizational effectiveness, improved intelligence-driven operations, reduced risks, and potentially increased competitive advantage. Then intelligence reports are consistently of high quality, the entire organization benefits from a robust information flow. This leads to more coordinated efforts, proactive problem-solving, and better resource allocation, ultimately contributing to the successful achievement of its mission and objectives.

Future Researchers. This study would contribute to the existing body of knowledge on intelligence studies, technical communication, and organizational development. The methodology and findings could serve as a springboard for further research in related areas.

Statement of the Problem

This study sought to evaluate the level of implementation of key reporting principles, determine their impact on security operations, and explore measures for improving the verification and accountability mechanisms within the system. Specifically, the researcher aimed to answer the following:

1. What is the level of implementation of the respondents of the guiding principles in Intelligence Report Writing in terms of:
   1.1. Accuracy,
   1.2. Clarity,
   1.3. Completeness, and
   1.4. Timeliness?
2. Is there a significant difference in the level of implementation of the guiding principles in Intelligence Report Writing between the three groups of respondents?
3. What are the impacts of the following on the effectiveness of security operations:
   3.1. Inaccuracies,
   3.2. Security breaches, and
   3.3. Malicious reporting?
4. What are the measures for verifying intelligence reports by independent reviews?
5. What measures or actions should be taken when a report is verified as maliciously fabricated against individuals or events? Based on the results, what system enhancement may be proposed?

II. METHODOLOGY

This study employed a Sequential Explanatory Mixed Methods Design, integrating quantitative and qualitative approaches to gain a comprehensive understanding of intelligence report writing practices within the Philippine National Police (PNP). The first phase utilized a quantitative survey to assess the level of implementation of the guiding principles—accuracy, clarity, completeness, and timeliness—among PNP personnel and members of the Confidential Unit. Statistical analyses such as descriptive statistics and the Mann–Whitney U test were used to determine differences between groups. The second phase involved qualitative interviews and focus group discussions with high-ranking officials to explore the causes and impacts of inaccuracies, security breaches, and malicious reporting, as well as the measures taken to verify intelligence reports.

The study population consisted of 22 participants purposively selected based on their expertise and involvement in intelligence operations. Participants included PNP personnel, Confidential Unit members, and high-ranking officials, ensuring that the data collected reflected both operational and managerial perspectives. The research was conducted within selected PNP intelligence units where issues of report accuracy, confidentiality, and integrity are highly relevant. Data collection tools included a validated survey questionnaire and interview guides derived from official PNP intelligence manuals and related literature. Quantitative data were analyzed using SPSS, while qualitative data underwent thematic analysis following Braun and Clarke's framework.

Ethical standards were strictly observed throughout the study, with participants providing informed consent and assurances of confidentiality. Findings from both phases were integrated to develop an evidence-based intervention program aimed at improving intelligence report writing practices, ensuring accountability, and minimizing risks of misinformation or malicious reporting. The results are intended for dissemination through academic presentations, journal publications, and formal reports to the PNP and related agencies to guide future policy formulation and operational enhancement in intelligence documentation and reporting systems.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

III. RESULTS AND DISCUSSION

This chapter presents the findings of the study based on the data gathered through the chosen research instruments. The results are systematically organized and analyzed according to the specific objectives of the study. Tables, figures, and descriptive analyses are provided to illustrate the responses of the participants and highlight significant patterns or trends. The discussion interprets these results in relation to the research questions, existing literature, and theoretical framework, thereby providing deeper insights into the implications of the study.

In The Level of implementation of the respondents on the guiding principles in Intelligence writing in terms of Accuracy, reveals that the guiding principles in intelligence writing in terms of accuracy are generally very much implemented (VMI) by both the PNP and the Confidential Unit, with the overall median rated at 4. Among the indicators, the highest level of implementation is seen in ensuring that intelligence reports are based on verified and credible sources. This item received a consistent rating of "Very Much Implemented," highlighting the respondents' strong adherence to credibility and source validation as the foundation of intelligence work. Likewise, the indicators on presenting details that accurately reflect the situation, avoiding exaggeration or understatement, updating reports with the most current information, ensuring precision and specificity, and maintaining objectivity by avoiding bias or unfounded assumptions were all rated at the highest level. These results suggest that respondents place great emphasis on accuracy, credibility, and objectivity, which are consistent with the standards outlined in the PNP Intelligence Doctrine and international best practices in intelligence reporting.

On the other hand, some items received only a rating of "Implemented (I)", pointing to areas that need improvement. These include ensuring the overall accuracy of report writing, cross-checking all data before submission, reviewing reports to eliminate misleading or conflicting details, and including only relevant and factually correct information. The lower ratings in these indicators imply that while reports are generally reliable, lapses in cross-checking, thorough review, and filtering out irrelevant information may still occur, possibly due to operational constraints, time pressure, or uneven training across units. These results are corroborated by recent assessments of the Philippine law enforcement sector, which identified gaps in validation and review mechanisms as recurring challenges in intelligence operations (PNP Annual Report, 2023; DILG Memorandum Circular 2021-125).

Table 3. Test of Significant Relationship on the Level of Implementation of Accuracy in Intelligence Writing (Based on Median Values)

Groups Compared	*Median (High R Per)*	*Median (PNP Personnel)*	*Median (Confidential Unit)*	*χ^2 / H-value*	*p-value*	*Decision*	*Interpretation*
High R Per vs. PNP Personnel	*4*	*3*	*4*	*6.21*	*0.013*	*Significant*	*PNP Personnel rated accuracy lower compared to High R Per.*
High R Per vs. Confidential Unit	*4*	*4*	*4*	*1.07*	*0.301*	*Not Significant*	*Both groups show strong implementation of accuracy.*
PNP Personnel vs. Confidential Unit	*4*	*3*	*4*	*5.89*	*0.016*	*Significant*	*Confidential Unit rated accuracy higher than PNP Personnel.*
Overall (All Groups)	***4***	***3***	***4***	***7.45***	***0.006***	***Significant***	

The results in Table 3 demonstrate notable differences among the three groups regarding the implementation of accuracy in intelligence writing. When comparing High-Rank Personnel (High R Per) with PNP Personnel, a statistically significant difference ($\chi^2 = 6.21$, $p = 0.013$) was found, with PNP Personnel rating accuracy lower (Median = 3) compared to High R Per (Median = 4). This suggests that while higher-ranking officials perceive accuracy as highly implemented, field-level personnel encounter greater challenges in maintaining consistent precision in intelligence reports. Conversely, no significant difference ($\chi^2 = 1.07$, $p = 0.301$) was observed between High R Per and the Confidential Unit, both reflecting strong accuracy practices (Median = 4). However, a significant difference ($\chi^2 = 5.89$, $p = 0.016$) emerged between PNP Personnel and the Confidential Unit, where the latter rated accuracy higher. Taken together, the overall test across all groups ($\chi^2 = 7.45$, $p = 0.006$) confirmed a statistically significant relationship, highlighting discrepancies in perceptions and practices of accuracy among different organizational roles.

This implies that the significant gaps identified in this study carry important implications for intelligence and security operations. First, the lower accuracy ratings from PNP Personnel highlight the need for targeted capacity-building programs, particularly training in intelligence writing and fact validation at the operational level. Second, the findings suggest that organizational leadership should allocate more resources—such as access to technology, data verification tools, and structured report review

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

mechanisms—to frontline officers to help reduce discrepancies. Third, policy reforms should institutionalize standardized accuracy protocols across all units, ensuring that intelligence reports meet the same quality benchmarks regardless of origin. Finally, the results emphasize the importance of fostering accountability and continuous quality assurance in intelligence reporting, as inaccuracies at the operational level may undermine higher-level planning and decision-making.

The findings mirror the PNP Annual Report (2021), which highlighted reporting discrepancies between field operatives and specialized units due to workload, technological limitations, and training gaps. Similarly, UNODC (2021) stressed that accuracy in intelligence products varies across policing levels, with specialized units having access to more resources and advanced protocols. Estrella & Santos (2022) found that confidential or specialized units often maintain stricter reporting standards, while general PNP personnel face systemic constraints. Internationally, Carter & Carter (2020) observed that organizational hierarchies in police intelligence practices often produce uneven reporting standards, leading to inconsistencies in intelligence reliability.

Table 4. Level of implementation of the respondents on the guiding principles in Intelligence writing in terms of Clarity

Items	High R Per		PNP Per		Confidential Unit		Over all Mdn	
	Mdn	**DI**	**Mdn**	**DI**	**Mdn**	**DI**	**Mdn**	**SD**
1. Implement clear and straightforward language in their reports to avoid confusion.	4	VMI	3	I	4	VMI	4	VMI
2. Ensure that technical terms and abbreviations are fully explained for the reader's understanding.	4	VMI	3	I	3	I	3	I
3. Organize reports in a logical and easy-to-follow sequence to maintain coherence.	4	VMI	4	I	4	VMI	4	VMI
4. Use concise sentences and paragraphs to improve the clarity of presentation.	4	VMI	4	I	4	VMI	4	VMI
5. Highlight key points so that the reader can easily grasp the main ideas.	4	VMI	3	I	4	VMI	4	VMI
6. Avoid vague or ambiguous statements that may cause misinterpretation.	4	VMI	4	I	4	VMI	4	VMI
7. Apply formatting techniques, such as headings and bullet points, to make reports easier to understand.	4	VMI	3	I	4	VMI	4	VMI
8. Review their reports to check if the information is presented clearly to the intended audience.	4	VMI	4	I	4	VMI	4	VMI
9. Ensure that their reports are understandable even to non-technical readers.	4	VMI	3	I	4	VMI	4	VMI
10. Revise their reports to remove unnecessary complexity and improve overall clarity.	4	VMI	3	I	4	VMI	4	VMI
OVERALL TOTAL	**4**	**VMI**	**3**	**I**	**4**	**VMI**	**4**	**VMI**

The results in Table 3 reveal that the guiding principles in intelligence writing in terms of clarity are generally very much implemented (VMI) by the respondents, with an overall median score of 4 (VMI). The highest-rated indicators include the use of clear and straightforward language, the logical organization of reports, the use of concise sentences and paragraphs, the highlighting of key points, and the avoidance of vague or ambiguous statements. Other equally strong practices involve the use of formatting techniques such as headings and bullet points, reviewing reports for clarity, ensuring that reports are understandable even to non-technical readers, and revising reports to remove unnecessary complexity. These results suggest that the respondents recognize the value of presenting intelligence reports in a manner that is coherent, precise, and easily comprehensible, which is essential in law enforcement, where decisions often need to be made quickly and accurately.

However, the indicator on explaining technical terms and abbreviations for the reader's understanding was rated only as "Implemented (I)" rather than "Very Much Implemented." This indicates that while reports are generally clear to trained intelligence officers, they may still contain specialized language or jargon that makes them less accessible to policymakers, field operatives, or non-technical readers. Such gaps in clarity can reduce the effectiveness of intelligence dissemination, especially when reports are intended for broader audiences beyond specialized units. Overall, the findings affirm that clarity in intelligence writing is highly prioritized, yet there remains a need

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

to improve in simplifying technical language and ensuring universal comprehensibility of reports.

The results of this study are consistent with both local and international literature on intelligence communication. The United Nations Office on Drugs and Crime (UNODC, 2022) emphasizes that intelligence products must be free from ambiguity and written in a way that prevents misinterpretation, supporting the respondents' strong implementation of clear, straightforward, and logically organized reporting. Similarly, the Organization for Economic Cooperation and Development (OECD, 2020) stresses that clarity and coherence in government reporting promote transparency and strengthen institutional credibility, which aligns with the high ratings on conciseness, logical sequencing, and the use of formatting techniques to improve readability.

At the national level, the Philippine National Police (PNP) Annual Report (2023) highlighted the importance of clear communication in intelligence documentation to ensure that outputs are actionable and easily understood across different command levels. Likewise, the DILG Memorandum Circular No. 2021-125 underscores that intelligence information must be reported in concise and accessible language to improve inter-agency coordination for public safety.

Table 5. Test of Significant Relationship on the Level of Implementation in Clarity.

Comparison	Median (Group 1)	Median (Group 2)	Difference	Significance (p < 0.05)	Interpretation
High R Per vs PNP	*4*	*3*	*1*	***Significant***	*PNP rated lower than High R Per*
High R Per vs Confidential Unit	*4*	*4*	*0*	*Not Significant*	*Both groups rated "Very Much Implemented"*
PNP vs Confidential Unit	*3*	*4*	*1*	***Significant***	*PNP rated lower than the Confidential Unit*

The results of the Kruskal–Wallis H test (H = 11.17, p = 0.0038) revealed a statistically significant difference in the level of implementation of clarity in intelligence writing as perceived by the three groups of respondents. High R Per (Mdn = 4) and the Confidential Unit (Mdn = 4) consistently rated clarity practices as "Very Much Implemented," while the PNP respondents (Mdn = 3) perceived these practices only as "Implemented." This indicates that although the principle of clarity in report writing is generally recognized, its actual application varies among groups.

Further analysis through pairwise comparison showed that the PNP respondents rated significantly lower compared to both High R Per and the Confidential Unit. Meanwhile, no significant difference was observed between High R Per and the Confidential Unit, which suggests that these two groups share a similar perception that clarity in intelligence writing is highly practiced. The divergence in PNP ratings highlights a perceptual and practical gap, implying that clarity standards may not be uniformly implemented across all organizational levels. Possible reasons for these differences could be operational challenges such as heavy workloads, insufficient training, or the absence of a standardized report format, which can affect the way clarity is maintained in intelligence reports.

These findings align with the study of Orongan and Mendoza (2022), who noted that law enforcement agencies often struggle with ensuring clarity in reporting due to workload and the lack of unified documentation systems. Similarly, Santos (2021) observed that frontline police officers tend to simplify intelligence reports for practicality, which may explain their lower ratings compared to specialized or supervisory units that require more rigorous adherence to reporting standards. The PNP Internal Audit of 2023 also revealed gaps in standardization, particularly in clarity and readability, and recommended continuous capacity-building initiatives to address these issues. International perspectives, such as those discussed by Bittner (2020), also stress that clarity in police documentation requires reinforcement through structured training programs and standardized templates to reduce subjective differences in reporting styles.

Table 6. Level of implementation of the respondents on the guiding principles in Intelligence writing in terms of Completeness

Items	High R Per		PNP Per		Confidential Unit		Overall Mean	
	Mdn	DI	Mdn	DI	Mdn	DI	Mdn	DI
1. Include all essential facts and details necessary for a comprehensive intelligence report.	3	I	3	I	4	VMI	3	I
2. Provide sufficient background information to give context to the report.	3	I	4	VMI	4	VMI	4	VMI
3. Present a balanced account of the situation without omitting critical information.	4	VMI	3	I	4	VMI	4	VMI
4. Ensure that reports contain all relevant data to support findings and conclusions.	3	I	3	I	4	VMI	3	I

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

5.	Incorporate supporting documents, references, or attachments when required.	4	VMI	4	VMI	4	VMI	4	VMI
6.	Address all the key questions or issues raised in the intelligence tasking.	4	VMI	4	VMI	4	VMI	4	VMI
7.	Cover the "who, what, when, where, why, and how" in their reports whenever applicable.	3	I	4	VMI	4	VMI	4	VMI
8.	Verify that no important details are left out before finalizing the report.	4	VMI	4	VMI	4	VMI	4	VMI
9.	Make sure the report presents a complete picture to assist decision-makers effectively.	4	VMI	4	VMI	4	VMI	4	VMI
10.	Revise and update reports as necessary to maintain completeness.	3	I	4	VMI	4	VMI	4	VMI
OVERALL TOTAL		**3**	**I**	**4**	**VMI**	**4**	**VMI**	**4**	**VMI**

The results in Table 4 reveal that the overall level of implementation of the guiding principles in intelligence writing in terms of completeness was rated as Very Much Implemented (VMI, Mean = 4). This suggests that respondents generally adhere to the standard of ensuring comprehensive and complete intelligence reports. The Confidential Unit consistently gave higher ratings (VMI) across most items, while the PNP group rated completeness only as Implemented (I, Mean = 3). This discrepancy indicates differences in practices or the degree of compliance between the two groups, with the Confidential Unit demonstrating stricter adherence to reporting guidelines.

Specifically, completeness was most strongly manifested in providing sufficient background information (Item 2), presenting a balanced account (Item 3), incorporating supporting documents (Item 5), addressing tasking questions (Item 6), verifying details before finalizing reports (Item 8), presenting a complete picture for decision-makers (Item 9), and revising or updating reports as necessary (Item 10). These areas were consistently rated as Very Much Implemented, showing that respondents recognize the importance of verification, supporting evidence, and context in intelligence writing. Such practices reflect a strong culture of accountability and reliability, which are vital in ensuring that reports serve as credible bases for decision-making.

On the other hand, some aspects of completeness were only rated as Implemented, such as including all essential facts (Item 1), ensuring reports contain all relevant data (Item 4), and covering the "who, what, when, where, why, and how" (Item 7). These results imply that while respondents are generally consistent in maintaining completeness, certain foundational elements of structured reporting are not always fully observed. These gaps may be due to operational time constraints, assumptions that decision-makers already know certain details, or lack of standardized reporting procedures.

In summary, completeness in intelligence writing is largely upheld by respondents, with strong implementation of verification, contextual background, and supporting documentation. However, the moderate ratings in the inclusion of essential facts and structured reporting suggest areas for improvement. These findings highlight the need for uniform training, stricter compliance monitoring, and harmonized guidelines to ensure that all intelligence reports, regardless of the originating unit, achieve a consistently high standard of completeness.

Table 7: Test of Significant Difference on the Level of Implementation of Completeness in Intelligence Writing

Comparison	*Median (High R Per)*	*Median (PNP)*	*Median (Confidential Unit)*	*Sig. Difference*	*Interpretation*
High R Per vs PNP	*3*	*4*	*4*	*Significant*	*PNP rated higher (VMI) compared to High R Per (I)*
High R Per vs Confidential	*3*	*4*	*4*	*Significant*	*Confidential Unit perceived stronger implementation (VMI) than High R Per (I)*
PNP vs Confidential Unit	*0*	*4*	*4*	*Not Significant*	*Both groups share the same perception (VMI)*
Overall (Kruskal-Wallis)	*3*	*4*	*4*	*Significant*	*There is a significant difference among the three groups overall*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

The test of significant difference revealed notable variations in the assessment of the respondents regarding the implementation of the guiding principle of completeness in intelligence writing. As shown in the results, the PNP and Confidential Unit both rated completeness as "Very Much Implemented (VMI)", while the High R Per group rated it lower, at "Implemented (I)." This disparity indicates that the High R Per respondents may perceive certain gaps in the inclusion of essential facts, background details, or contextual information required for a fully comprehensive report.

Further analysis showed that there was no significant difference between the PNP and Confidential Unit, as both groups recognized a consistent practice of providing thorough and detailed reports. They perceived that reports sufficiently address critical questions, incorporate supporting documents, and ensure no key details are omitted. However, a significant difference was observed between the High R Per and the other two groups. This implies that the High R Per group exercises a more critical stance in evaluating completeness, possibly reflecting stricter standards or a heightened awareness of lapses in intelligence documentation.

The overall Kruskal-Wallis test confirmed a significant difference across the three groups, highlighting that perceptions of completeness vary depending on the role and context of the respondents. These findings align with Mendoza and Orongan (2022), who argued that completeness is often assessed differently between intelligence producers and evaluators. Similarly, Bittner (2020) emphasized that completeness entails not only the presence of information but also its contextual adequacy, which may explain why evaluators like High R Per respondents identify shortcomings that may not be apparent to operational units.

In sum, the results underscore the need for a uniform reporting standard and stronger validation mechanisms to ensure that all units consistently achieve high levels of completeness in intelligence writing. By aligning practices across different groups, decision-makers can be assured of reports that are not only factually comprehensive but also contextually relevant and actionable.

Table 8. Level of implementation of the respondents on the guiding principles in Intelligence writing in terms of timeliness

Items	High R Per		PNP Per		Confidential Unit		Overall Mean	
	Mdn	DI	Mdn	DI	Mdn	DI	Mdn	DI
1. Submit their intelligence reports within the required deadline	4	VMI	3	I	4	VMI	4	VMI
2. Provide information while it is still current and relevant.	4	VMI	3	I	4	VMI	4	VMI
3. Ensure that urgent or time-sensitive reports are prioritized and delivered promptly.	4	VMI	3	I	3	I	3	I
4. Implement measures to avoid unnecessary delays in report preparation.	4	VMI	3	I	3	I	3	I
5. Update reports regularly to reflect the most recent developments.	4	VMI	3	I	4	VMI	4	VMI
6. Respond quickly to intelligence requirements or taskings from superiors.	4	VMI	3	I	4	VMI	4	VMI
7. Coordinate efficiently with sources to gather timely information.	4	VMI	3	I	3		3	I
8. Use available resources effectively to speed up report completion without sacrificing quality.	4	VMI	3	I	4	VMI	4	VMI
9. Review and finalize reports promptly to ensure delivery within the needed time frame.	4	VMI	3	I	3	I	3	I
10. Implement practices that balance speed with accuracy in producing intelligence reports.	4	VMI	3	I	4	VMI	4	VMI
OVERALL TOTAL	**4**	**VMI**	**3**	**I**	**3**	**I**	**4**	**VMI**

The results presented in Table 5 show that the respondents generally rated the implementation of the guiding principles in intelligence writing in terms of timeliness as Very Much Implemented (VMI, Mean = 4). This indicates that, overall, intelligence personnel recognize the importance of submitting reports promptly and ensuring information remains current and relevant. The Confidential Unit consistently gave higher ratings (VMI) across most items, while the PNP group rated timeliness as only Implemented (I, Mean = 3). This again highlights a discrepancy between the two groups, suggesting that specialized units may adhere more strictly to deadlines and timely dissemination than their PNP counterparts.

Strong practices were noted in the timely submission of reports within deadlines (Item 1), providing current and relevant information (Item 2), updating reports to reflect recent developments (Item 5), responding quickly to taskings (Item 6), effective use of resources (Item 8), and balancing speed with

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

accuracy (Item 10). These were all rated as Very Much Implemented, showing that respondents prioritize promptness and responsiveness, which are essential in operational decision-making.

However, areas such as prioritizing urgent/time-sensitive reports (Item 3), avoiding unnecessary delays (Item 4), efficient coordination with sources (Item 7), and prompt review and finalization of reports (Item 9) received only an Implemented (I) rating overall.

These gaps suggest that while timeliness is emphasized, challenges remain in handling urgent intelligence tasks, source coordination, and the final processing stages of reports. Such limitations may be attributed to workload, limited manpower, or resource constraints that affect the speed of certain intelligence processes.

Table 9: ***Test of Significant Difference on the Level of Implementation of Timeliness in Intelligence Writing***

Comparison	***Median (High R Per)***	***Median (PNP)***	***Median (Confidential Unit)***	***Sig. Difference***	***Interpretation***
High R Per vs PNP	*4*	*3*	*3*	*Significant*	*PNP rated lower (I) compared to High R Per (VMI)*
High R Per vs Confidential	*4*	*3*	*3*	*Significant*	*High R Per perceived a stronger implementation than the Confidential Unit*
PNP vs Confidential Unit	*4*	*3*	*0*	*Not Significant*	*Both groups share the same perception (I)*
Overall (Kruskal-Wallis)	*4*	*3*	*3*	*Significant*	*There is a significant difference among the three groups overall*

The test of significant difference revealed variations in the assessment of the respondents on the principle of timeliness in intelligence writing. Results showed that the High R Per consistently rated timeliness as "Very Much Implemented (VMI)," while the PNP and Confidential Unit rated it only as "Implemented (I)." This indicates a disparity in perceptions, where the High R Per group perceived stronger adherence to deadlines, promptness, and the delivery of up-to-date reports compared to the other groups.

Pairwise comparisons revealed that there is a significant difference between High R Per and both the PNP and Confidential Unit, with the latter two groups rating timeliness lower. However, there was no significant difference between the PNP and Confidential Unit, as both shared the same median value of "Implemented." This suggests that operational units perceive greater challenges in meeting time-sensitive requirements and updating reports promptly, whereas the High R Per group holds a more favorable view of timeliness implementation.

The overall Kruskal-Wallis result confirmed a statistically significant difference among the three groups, emphasizing that perceptions of timeliness vary depending on roles and responsibilities. High R Per, who may function in oversight and evaluation, perceive timeliness to be strongly practiced, while field units like the PNP and Confidential Unit may encounter delays due to operational constraints such as workload, limited resources, and coordination difficulties.

These findings are consistent with Bittner (2020), who noted that timeliness in intelligence reporting is often hampered by practical barriers in field operations. Similarly, the PNP Internal Audit Service (2023) reported recurring delays in the submission and updating of intelligence reports, particularly at the operational level. Mendoza and Orongan (2022) also emphasized that maintaining timeliness requires efficient coordination with sources and effective use of resources, aligning with the lower ratings given by operational units in this study.

In summary, the results indicate that timeliness is unevenly perceived and implemented across units. While oversight groups view reporting as prompt and current, operational units highlight challenges that may hinder consistent timeliness. This suggests the need for streamlined processes, improved coordination, and resource allocation to ensure that intelligence reporting remains both timely and reliable.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

Table 10. Impact on the effectiveness of security operations according to Inaccuracies

Items	High R Per		PNP Per		Confidential Unit		Overall Mean	
	Mdn	DI	Mdn	DI	Mdn	DI	Mdn	DI
1. Inaccuracies in intelligence reports result in poor decision-making during security operations.	4	VME	3	E	4	VME	4	VME
2. Inaccurate information causes delays in the timely response to security threats.	4	VME	3	E	4	VME	4	VME
3. Wrong or misleading data leads to misallocation of resources (e.g., personnel, equipment, funds).	4	VME	4	VME	4	VME	4	VME
4. Inaccuracies increase the risk of overlooking real threats and vulnerabilities.	4	VME	3	E	4	VME	4	VME
5. Security personnel may be deployed unnecessarily or to the wrong locations due to inaccurate reports.	4	VME	3	E	4	VME	4	VME
6. Inaccurate reporting decreases the efficiency of operational planning.	4	VME	4	VME	4	VME	4	VME
7. Inaccuracies compromise the safety of operatives and civilians during security missions.	4	VME	3	E	4	VME	4	VME
8. Continuous inaccuracies undermine the credibility and trustworthiness of intelligence units.	4	VME	4	VME	3	E	4	VME
9. 9 Inaccurate intelligence creates . security agencies.	4	VME	3	E	3	E	3	E
10. Inaccuracies reduce the overall effectiveness and success rate of security operations.	4	VME	3	E	3	E	3	E
OVERALL TOTAL	**4**	**VME**	**3**	**E**	**4**	**VME**	**4**	**VME**

The results in Table 8 show that respondents strongly agree that inaccuracies in intelligence reporting have a very much effective (VME) impact on undermining the effectiveness of security operations. The overall mean rating of 4 (VME) indicates that intelligence errors substantially influence decision-making, timely responses, allocation of resources, and the overall success of security operations. Specifically, items such as poor decision-making, delays in response, overlooking threats, and compromised safety of operatives and civilians were rated highly, reflecting the practical dangers posed by inaccurate information. The Confidential Unit generally provided slightly lower ratings (E = Effective) in some areas, such as decision-making, delays, safety, and inter-agency coordination, suggesting that while they acknowledge the problem, they may perceive greater resilience or compensatory measures in their specialized operations. Nonetheless, both groups agreed that continuous inaccuracies erode trustworthiness and hinder operational planning.

The findings align with several scholarly and institutional reports. The United Nations Office on Drugs and Crime (2021) noted that flawed intelligence creates delays, inefficiencies, and overlooked vulnerabilities, directly supporting the present results on decision-making and timeliness. Interpol (2022) highlighted that misleading or incomplete intelligence compromises safety and coordination among agencies, echoing Items 5, 7, and 9. Similarly, the Philippine National Police (2022) recognized in its annual assessment that inaccurate intelligence reduces operational success and diminishes public trust, consistent with Item 8 on credibility. Meanwhile, Carter and Phillips (2020) emphasized that poor-quality intelligence leads to resource misallocation and planning inefficiencies, corroborating Items 3 and 6. These studies strengthen the argument that accuracy is indispensable for both tactical and strategic security outcomes.

The implications of these findings are multifaceted. At the operational level, inaccuracies threaten the lives of both operatives and civilians, necessitating stricter verification and cross-checking mechanisms before intelligence dissemination. In terms of resources, incorrect data wastes personnel, funds, and equipment, which underscores the importance of adopting accuracy-driven intelligence systems. Institutionally, repeated inaccuracies weaken credibility, not only within agencies but also in the eyes of the public, which calls for greater accountability and investments in analytical tools that minimize errors. The moderate ratings on inter-agency miscoordination further imply that communication systems between units need harmonization through standardized reporting formats and collaborative platforms. Finally, from a policy standpoint, the results suggest the need for continuous training of intelligence officers, integration of advanced technologies such as automated validation systems, and the strengthening of oversight mechanisms to ensure intelligence accuracy.

In summary, Table 8 highlights that inaccuracies in intelligence reporting generate a chain of operational, institutional, and policy-related consequences that diminish the overall

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

effectiveness of security operations. Supported by global and local literature, the study underscores that maintaining accuracy is not just a technical requirement but a foundational element of security governance. Addressing this issue through training, technology, and inter-agency reforms will significantly improve operational outcomes and reinforce public confidence in security institutions.

Table 11: Test of Significant Difference on the Impact of Inaccuracies in Intelligence Writing on Security Operations

Comparison	*Median (High R Per)*	*Median (PNP)*	*Median (Confidential Unit)*	*Sig. Difference*	*Interpretation*
High R Per vs PNP	*4*	*3*	*4*	*Significant*	*High R Per rated impact stronger than PNP*
High R Per vs Confidential	*0*	*3*	*4*	*Not Significant*	*Both perceived a strong impact of inaccuracies*
PNP vs Confidential Unit	*4*	*3*	*4*	*Significant*	*Confidential Unit rated impact stronger than PNP*
Overall (Kruskal-Wallis)	*4*	*3*	*4*	*Significant*	*Overall, perceptions differ significantly across groups*

The test of significant difference revealed that the respondents differed in their assessment of how inaccuracies in intelligence writing affect the effectiveness of security operations. The High R Per and the Confidential Unit consistently rated the impact as "Very Much Effective (VME)," while the PNP rated it only as "Effective" (E)." This indicates that evaluative and specialized intelligence groups perceive inaccuracies as having a stronger and more critical effect on operational outcomes compared to the perception of the PNP.

Pairwise comparisons confirmed a significant difference between the PNP and both the High R Per and Confidential Unit, as the latter two groups recognized inaccuracies as having severe consequences such as poor decision-making, delayed responses, and compromised safety of personnel and civilians. However, there was no significant difference between High R Per and Confidential Unit, as both emphasized the heightened risks and inefficiencies that stem from inaccurate reporting. The overall Kruskal-Wallis test also confirmed a significant difference across all three groups, reflecting variability in how strongly inaccuracies are perceived to undermine security operations.

The lower rating of the PNP suggests that operational personnel may see inaccuracies as part of manageable challenges in the field, possibly due to their focus on immediate response and adaptability. On the other hand, the High R Per and Confidential Unit's stronger ratings (VME) reflect their broader perspective on the long-term and systemic effects of inaccuracies—particularly in undermining trust, misallocating resources, and creating vulnerabilities that may endanger both operatives and civilians.

These results are consistent with Bittner (2020), who argued that inaccurate intelligence often leads to flawed decision-making and misdirected responses in security operations. Mendoza and Orongan (2022) also emphasized that continuous inaccuracies erode the credibility of intelligence units, making it harder for agencies to maintain trust with stakeholders. Likewise, the PNP Internal Audit Service (2023) found recurring issues of inaccuracies in reports that directly impacted response times and operational planning.

In conclusion, the findings underscore that inaccuracies in intelligence writing significantly affect the overall effectiveness of security operations. While all groups acknowledged this impact, oversight and specialized units recognized it more critically than field operatives. The significant difference highlights the need for rigorous data verification, systematic review processes, and training interventions to minimize inaccuracies and ensure reliable intelligence reporting.

Table 12. Impact on the effectiveness of security operations according to Security Breaches

Items	High R Per		PNP Per		Confidential Unit		Over all Mean	
	Mdn	DI	Mdn	DI	Mdn	DI	Mdn	DI
1. Security breaches expose sensitive information that compromises operational planning.	4	VME	4	VME	4	VME	4	VME
2. Breaches disrupt the continuity of ongoing security operations.	4	VME	4	VME	4	VME	4	VME
3. Unauthorized access during breaches increases the vulnerability of security systems.	4	VME	4	VME	4	VME	4	VME
4. Security breaches delay the implementation of security responses.	4	VME	4	VME	4	VME	4	VME

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

5.	Breaches cause miscoordination among security agencies and units.	4	VME	4	VME	4	VME	4	VME
6.	Security breaches lead to financial and resource losses in operations.	4	VME	4	VME	4	VME	4	VME
7.	Breaches undermine the trust and confidence of stakeholders in security operations.	4	VME	4	VME	4	VME	4	VME
8.	Compromised information from breaches puts operatives and civilians at risk.	4	VME	4	VME	4	VME	4	VME
9.	Security breaches reduce the overall effectiveness of intelligence gathering.	4	VME	4	VME	4	VME	4	VME
10.	Breaches damage the credibility and reliability of the entire security organization.	4	VME	4	VME	4	VME	4	VME
OVERALL TOTAL		**4**	**VME**	**4**	**VME**	**4**	**VME**	**4**	**VME**

The findings in Table 9 reveal that respondents unanimously rated all items under the impact of security breaches as Very Much Effective (VME) with an overall mean of 4 (VME) across both the PNP and Confidential Units. This consistency indicates a strong consensus that breaches severely compromise security operations. Specifically, breaches were seen as exposing sensitive information, disrupting operational continuity, and delaying responses. They were also rated highly for causing miscoordination among agencies, financial and resource losses, and undermining the trust of stakeholders. Moreover, compromised data was perceived to put both operatives and civilians at risk, while also weakening intelligence gathering processes and damaging the credibility of the entire security organization. The unanimous VME ratings emphasize that breaches are universally acknowledged as one of the gravest threats to the effectiveness of security operations.

These results are consistent with existing literature. UNODC (2021) stressed that breaches of sensitive intelligence compromise planning and execution, leading to delayed responses and weakened strategies, which directly supports Items 1 and 4. Interpol (2022) highlighted that unauthorized access and cyber intrusions heighten vulnerabilities and disrupt inter-agency coordination, aligning with Items 3 and 5. Similarly, Estrella and Santos (2022) found that breaches lead to financial strain and loss of operational resources, consistent with Item 6. The PNP Annual Report (2022) also documented cases where breaches of confidential data undermined public trust and damaged institutional credibility, reinforcing Items 7 and 10. Finally, Carter and Phillips (2020) pointed out that breaches degrade the quality of intelligence collection, validating Item 9 in this study.

The implications of these findings are critical for both operational and institutional security. At the operational level, breaches place missions, operatives, and civilians at risk, highlighting the need for stricter access controls, cybersecurity measures, and continuous monitoring systems. At the resource level, breaches result in avoidable financial losses, which implies the necessity of investing in stronger prevention and recovery mechanisms. Institutionally, breaches severely undermine credibility and stakeholder trust, pointing to the importance of transparency in addressing incidents and reinforcing accountability. These findings also imply that inter-agency coordination protocols must be fortified to reduce vulnerabilities arising from breaches and ensure rapid recovery when they occur.

Table 13: Test of Significant Difference on the Impact of Security Breaches on Security Operations

Comparison	ian (High R Per)	ian (PNP)	ian (Confidential Unit)	Difference	Interpretation
High R Per vs PNP	*4*	*4*	*4*	*Significant*	*Both rated breaches as highly impactful*
ı R Per vs Confidential	*4*	*4*	*4*	*Significant*	*Shared perception of very high impact*
P vs Confidential Unit	*4*	*4*	*4*	*Significant*	*No variation in perception*
rall (Kruskal-Wallis)	***4***	***4***	***4***	***Significant***	***Groups uniformly recognized the impact***

The analysis revealed no significant difference among the responses of the High R Per, PNP, and Confidential Unit in terms of the impact of security breaches on the effectiveness of security operations. All groups uniformly rated the items as "Very Much Evident (VME)", indicating strong agreement that breaches pose a critical threat across multiple dimensions of intelligence and operational security.

Respondents consistently emphasized that security breaches compromise sensitive information, disrupt continuity of operations, delay timely responses, and increase the vulnerability of systems. Likewise, breaches were perceived to undermine coordination among security units, cause financial losses, reduce effectiveness in intelligence gathering, and damage credibility with stakeholders. The uniform "VME" rating across groups

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

highlights a shared recognition that breaches are among the most severe challenges in maintaining effective security operations.

The absence of significant difference suggests that regardless of role or affiliation, all security sectors have experienced or observed the serious consequences of breaches. This aligns with the findings of Flores & Arcenas (2021), who noted that unauthorized access and data leaks are considered universal risks in both field operations and intelligence units. Similarly, Castillo (2022) emphasized that breaches erode organizational trust and operational efficiency, a concern echoed in the 2023 PNP Annual Security Report, which identified cyber intrusions and internal leaks as major threats to Philippine security systems.

Overall, the results indicate that security breaches are universally regarded as a very critical factor undermining the effectiveness of security operations. This consensus points to the urgent need for strengthened cybersecurity protocols, stricter access control, continuous monitoring, and inter-agency coordination to prevent breaches and mitigate their devastating consequences.

Table 14. Impact on the effectiveness of security operations according to Malicious Reporting

Items	High R Per		PNP Per		Confidential Unit		Overall Mean	
	Mdn	DI	Mdn	DI	Mdn	DI	Mdn	DI
1. Malicious reporting misleads decision-makers and results in poor security strategies.	4	VME	4	VME	4	VME	4	VME
2. False or malicious reports waste critical time and resources during operations.	4	VME	4	VME	4	VME	4	VME
3. Malicious reporting causes confusion and miscoordination among security personnel.	4	VME	4	VME	4	VME	4	VME
4. Security responses are delayed or misdirected due to false information.	4	VME	4	VME	4	VME	4	VME
5. Malicious reporting undermines the credibility of legitimate intelligence reports.	4	VME	4	VME	4	VME	4	VME
6. Operatives and civilians may be placed at risk because of deceptive information.	4	VME	4	VME	4	VME	4	VME
7. Malicious reports reduce trust and cooperation between security agencies and the community.	4	VME	4	VME	4	VME	4	VME
8. Continuous malicious reporting lowers the morale of security personnel.	4	VME	4	VME	4	VME	4	VME
9. Malicious reporting creates operational setbacks and lowers the overall success rate of missions.	4	VME	4	VME	4	VME	4	VME
10. Malicious reporting damages the reputation and reliability of security organizations.	4	VME	4	VME	4	VME	4	VME
OVERALL TOTAL	**4**	**VME**	**4**	**VME**	**4**	**VME**	**4**	**VME**

The findings in Table 10 reveal that respondents across the High-Rank personnel, PNP, and Confidential Unit unanimously rated the impact of malicious reporting as Very Much Effective (VME) in undermining security operations. All ten indicators, including misleading decision-makers, wasting resources, creating confusion, delaying responses, undermining credibility, endangering operatives and civilians, and damaging institutional reputation, received consistently high scores (Mdn = 4). This indicates a strong consensus that malicious reporting poses one of the most critical threats to intelligence reliability and operational success. Unlike unintentional inaccuracies, malicious reports are deliberate acts of deception, making them more dangerous because they erode trust not only within security organizations but also between law enforcement and the public.

These results are consistent with the UNODC (2021) handbook on intelligence integrity, which warns that false and malicious reporting distorts operational decision-making and severely compromises the credibility of intelligence institutions. Similarly, Interpol (2022) reported that disinformation campaigns targeting law enforcement agencies have become a growing global threat, causing miscoordination and delayed responses during critical missions. In the Philippine context, Estrella & Santos (2022) highlighted how malicious reporting wastes scarce operational resources and damages public trust in community-police relations. Moreover, the PNP Annual Report (2022) emphasized the need to strengthen internal vetting and validation procedures to counter the proliferation of malicious or fabricated reports in both traditional and digital channels. This aligns directly with the high concern reflected in the present study.

The implications of these findings are significant for both policy and practice. First, malicious reporting calls for stronger intelligence vetting protocols and multi-source validation systems to ensure accuracy before action is taken. Second, there is a need

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

for capacity building and technological upgrades, such as artificial intelligence-driven cross-checking systems, to detect inconsistencies and prevent reliance on fabricated information. Third, addressing malicious reporting requires not only operational solutions but also community engagement strategies, since public trust and cooperation play a vital role in filtering credible intelligence from false submissions. Finally, malicious reporting, if left unchecked, may lower the morale of security personnel and weaken institutional credibility, thereby reducing overall effectiveness in safeguarding communities. Therefore, proactive countermeasures and accountability systems are necessary to mitigate its impact on national security operations.

Table 15: Test of Significant Difference on the Impact of Malicious Reporting on Security Operations

Comparison	*Median (High R Per)*	*Median (PNP)*	*Median (Confidential Unit)*	*Sig. Difference*	*Interpretation*
High R Per vs PNP	*4*	*4*	*4*	*Not Significant*	*Both rated malicious reporting as highly impactful*
High R Per vs Confidential	*4*	*4*	*4*	*Not Significant*	*Shared perception of very high impact*
PNP vs Confidential Unit	*4*	*4*	*4*	*Not Significant*	*No variation in perception*
Overall (Kruskal-Wallis)	*4*	*4*	*4*	*Not Significant*	*Groups uniformly recognized the impact*

The findings revealed no significant difference among the perceptions of the High R Per, PNP, and Confidential Unit regarding the impact of malicious reporting on the effectiveness of security operations. All groups consistently assessed the phenomenon as "Very Much Evident (VME)", signifying strong consensus that false or malicious intelligence reports severely compromise operational effectiveness.

Respondents commonly recognized that malicious reporting misleads decision-makers, wastes valuable time and resources, causes confusion, delays responses, and undermines the credibility of legitimate intelligence. Moreover, such reports were perceived to reduce trust between agencies and communities, damage organizational reputation, and demoralize personnel. The uniformity of the responses reflects a collective recognition that malicious reporting is not a trivial issue but a systemic threat to security effectiveness.

The absence of significant difference implies that regardless of institutional affiliation, all groups share similar experiences or awareness of the destructive impact of malicious reporting. This finding is supported by Cruz and De Guzman (2021), who highlighted that the spread of false intelligence often leads to strategic missteps and wasted operational resources in Philippine security agencies. Likewise, Santos (2022) argued that malicious reports erode inter-agency trust, a sentiment further supported by the 2023 PNP Directorate for Intelligence Report, which emphasized the dangers of misinformation campaigns and internal sabotage on organizational credibility.

In summary, the results demonstrate that malicious reporting is unanimously regarded as a very serious threat to effective security operations, warranting stricter mechanisms for intelligence validation, inter-agency coordination, and accountability measures to prevent its occurrence and mitigate its negative consequences.

The measures in verifying intelligence reports by independent reviews

Verifying intelligence reports is an indispensable component in safeguarding the credibility, reliability, and accuracy of information used in national security. Given the classified nature of intelligence work, verification processes are often shielded from public view. However, thematic analysis of practitioner insights reveals several institutional strategies used by agencies like the National Intelligence Coordinating Agency (NICA). These include multi-source validation, technological enhancement, inter-agency collaboration, and the challenge of balancing secrecy with transparency.

What are the measures for verifying intelligence reports by independent reviews?

Thirteen (13) high-ranking intelligence officers (PNP Personnel and Confidential Unit) participated.

Multi-Source Verification and HUMINT Validation - Several respondents emphasized the importance of cross-referencing human intelligence. For example, Respondent 1 shared, *"We use other HUMINT sources to validate information,"* while Respondent 2 noted, *"Information is screened and cross-checked before submission."* Similarly, Respondent 4 added, *"Case officers ensure intel validity by comparing reports on the ground."* These responses demonstrate reliance on triangulation across multiple sources, reducing bias and error, consistent with Triangulation Theory (Denzin, 1978) and the intelligence cycle validation framework (Betts, 2007).

Technological Tools for Intelligence Validation - Modern verification incorporates technological tools. Respondent 5 highlighted, *"Tools like GIS help validate location accuracy,"* while Respondent 6 explained, *"Digital forensics support is requested in analyzing seized devices."* Respondent 7 further noted, *"OSINT platforms help filter false information."* These insights underscore the integration of GIS, forensic analysis, and

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

OSINT into intelligence validation, aligning with geo-intelligence principles (Esri, 2013) and digital forensic readiness (Rowlingson, 2004).

Secure Coordination and Inter-Agency Collaboration - Coordination across agencies and secure communication were also highlighted. Respondent 3 said, *"Coordination with other agencies is part of internal verification."* Respondent 8 emphasized, *"Communication channels are encrypted to ensure secure collaboration,"* while Respondent 9 noted, *"Regional offices coordinate closely with other officials."* These responses reflect the importance of inter-agency checks and encrypted communication systems in ensuring reliable validation, supported by Carter & Carter (2020) and INTERPOL (2021).

Limited Transparency and the Challenge of Independent Reviews - several respondents pointed out the constraints of secrecy. Respondent 10 asserted, *"The work of the agency is largely classified."* Similarly, Respondent 11 admitted, *"There is limited public access to how intelligence is verified,"* while Respondent 12 explained, *"Independent review is conducted only when needed,"* and Respondent 13 concluded, *"Oversight is constrained by confidentiality."* These illustrate the inherent tension between secrecy and transparency in intelligence work (Born & Leigh, 2018; Caparini, 2020).

Measures or actions should be taken when a report is verified as maliciously fabricated against individuals or events

Ensuring the integrity and credibility of intelligence reports is a fundamental responsibility of intelligence agencies. The National Intelligence Coordinating Agency (NICA), as reflected in statements from intelligence officers and operatives, employs a structured and multi-layered approach to verify and validate information before it is disseminated. The thematic analysis below presents patterns emerging from the narratives shared, focusing on how NICA maintains report accuracy, prevents misinformation, and enforces accountability within its ranks.

Multi-Level Validation of Intelligence Reports. - The validation of intelligence reports is a cornerstone of the agency's operations, with participants consistently emphasizing a rigorous, multi-level approach that leverages diverse sources. As one participant articulated, *"In the Intel community, we always conduct validation through our sources and confirmation by other agency/units before reporting to avoid misinformation."* This aligns with recent studies highlighting that intelligence-led organizations reduce the risk of flawed reporting by systematically cross-referencing information across independent channels before dissemination (Ratcliffe, 2019; Carter & Carter, 2020).

This initial layer of validation often begins at the ground level, as another participant stated, *"We validate, and verify the information first. Ask questions from the field operatives."* Field-level verification is critical, as research on human intelligence (HUMINT) stresses that feedback loops between collectors and analysts help resolve ambiguities, verify timelines, and assess reliability in real time (Maguire et al., 2019; Born et al., 2020). Furthermore, ensuring the reliability of human assets is vital, with a participant noting the importance of *"Review access and placement of HUMINT sources"* to understand their vantage points and potential biases. This is consistent with recent operational security literature recommending periodic review of source positioning to detect misinformation risks and identify compromised channels (Bakker et al., 2021).

The theme underlines the agency's robust commitment to verifying intelligence through multiple HUMINT sources, coordination with other units, and confirmation from independent or external agencies. As current scholarship affirms, such structured, multi-layered validation not only prevents the dissemination of misinformation but also enhances the credibility of intelligence products, ensuring they are both accurate and operationally actionable in a national security context (Marks et al., 2022; Wirtz, 2021).

Accountability and Disciplinary Measures in Intelligence Reporting - A foundational element of the agency's operational integrity is a clear and robust system of accountability for fabricated or inaccurate intelligence reports. This commitment to ethical standards and professional conduct among its personnel is evident in the strict disciplinary measures in place. As one participant unequivocally stated, *"If a report is found to be purposely made up… the staff responsible can face investigations, punishments like suspension or firing, and even legal charges."* This comprehensive spectrum of consequences—ranging from internal investigation to potential legal prosecution—reflects what recent studies identify as a hallmark of professional intelligence practice: the establishment of enforceable sanctions to deter intentional misinformation and negligence (Born et al., 2020; Caparini, 2020). In contemporary intelligence governance frameworks, such measures are considered essential for maintaining public trust and safeguarding the credibility of security institutions (Leigh et al., 2021).

Proactive Correction and Public Clarification - In the dynamic landscape of information, NICA takes a proactive stance when misinformation reaches the public, swiftly acting to correct the narrative and safeguard its credibility. As one participant articulated, *"NICA quickly sets the record straight by sharing correct details through official channels."* This reflects a best practice identified in recent crisis communication research, which emphasizes the importance of rapid, authoritative messaging to prevent false narratives from gaining traction (Boin et al., 2019; Olsson, 2020). Studies in security communication highlight that timeliness and official sourcing are critical factors in preserving institutional trust during periods of heightened public uncertainty (Liu et al., 2022).

Beyond simply releasing correct details, the agency recognizes the value of collaborative efforts in managing public perception.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

Another participant noted that NICA *"Works with the media and other agencies to clear up misunderstandings."* This aligns with findings from contemporary disinformation management studies, which stress that multi-actor coordination—linking government agencies, traditional media, and credible third parties—significantly increases the reach and perceived legitimacy of corrective information (Wardle & Derakhshan, 2018; European Commission, 2022). Strategic engagement with news outlets ensures wide dissemination of verified details, while coordination with other government bodies promotes a unified and coherent public message, reducing the risk of mixed signals that can undermine credibility (Hameleers et al., 2020).

This theme underscores NICA's vital role in combating the spread of disinformation. By coupling swift corrective messaging with coordinated outreach, the agency demonstrates adherence to the principles of effective public communication in security contexts—clarity, accuracy, speed, and credibility. Current literature affirms that such integrated strategies are essential not only for protecting an agency's reputation but also for maintaining public trust in government institutions tasked with safeguarding national security (Van der Meer et al., 2021; Boin et al., 2019).

"Based on the results, what system enhancement may be proposed?". Ten (10) high-ranking intelligence officers (PNP Personnel and Confidential Unit) participated. For confidentiality, participants are labeled as Respondent 1–10. Each code refers to the same officer across all SOP questions.

Professionalization and Capacity-Building of Intelligence Personnel - A strong and consistent emphasis within the agency is placed on the professionalization and continuous capacity-building of its intelligence personnel, ensuring they are equipped with a comprehensive suite of necessary skills. This commitment to development is highlighted by the directive to *"conduct trainings on recruitment and handling of sources,"* underscoring the critical importance of ethical and effective engagement with human intelligence assets. Contemporary security literature affirms that structured training in source recruitment and management is vital to the integrity of intelligence operations, reducing risks of misinformation and fostering trust between operatives and informants (Gentry & Gordon, 2019; Lowenthal, 2020).

Beyond source management, the scope of training is broad and forward-looking. As another participant detailed, *"Training for intelligence personnel needs to focus on analyzing data, understanding cyber threats, and appreciating local cultures."* This aligns with recent scholarship emphasizing the need for hybrid skill sets in intelligence work, combining advanced data analytics, cyber threat detection, and socio-cultural awareness to respond effectively to complex, multidimensional threats (Hulnick, 2021; Prunckun, 2022). Cybersecurity research further underscores that intelligence agencies must integrate cyber literacy into their training frameworks to anticipate and counter increasingly sophisticated digital threats (Bada & Nurse, 2019).

Integration of Advanced Technology and Technical Intelligence - Participants consistently recognized the critical need for robust investment in advanced Technical Intelligence (TECHINT) capabilities to significantly enhance the agency's intelligence gathering and analysis functions. This commitment extends across various domains, as highlighted by one participant who urged, *"Use invest technologies (equipment) for TECHINT, SIGINT, GEOINT to aid intel operations."* This underscores the necessity of acquiring and deploying sophisticated tools for signals intelligence (SIGINT)—which involves intercepting and analyzing electronic communications—and geospatial intelligence (GEOINT), which leverages satellite imagery, mapping technologies, and spatial data for strategic analysis. Recent studies affirm that expanding these capabilities directly correlates with improved situational awareness, operational readiness, and threat anticipation (Carley et al., 2020; Lowenthal, 2022).

Beyond these foundational TECHINT components, there is a clear recognition of emerging technological frontiers. As another participant articulated, the agency needs to *"Improve these processes with the use of more advanced technologies such as artificial intelligence."* AI has been identified as a transformative force in intelligence operations, offering unprecedented speed and accuracy in data analysis, pattern recognition, anomaly detection, and predictive modeling (Allen & Chan, 2018; Gentry & Gordon, 2019). Its integration is seen as crucial for processing the vast and complex datasets that modern intelligence work demands.

Furthermore, the integration of new technologies is framed not as a discrete upgrade but as a comprehensive enhancement to the entire intelligence cycle. As one participant noted, *"Using new technologies in data analysis, secure communication and equipment can improve how information is collected and protected."* This highlights the growing importance of cybersecurity measures and secure communication platforms to safeguard sensitive information from interception or compromise—an imperative underscored in recent cybersecurity and defense literature (Bada & Nurse, 2019; Prunckun, 2022).

Finally, participants viewed these technological investments as essential to achieving more efficient and timely operations. One stressed the need to *"Sustain intelligence sharing and utilize platforms for timely validation of information."* This aligns with research indicating that digital collaboration platforms, when paired with secure, real-time validation protocols, significantly enhance the operational value and reliability of intelligence outputs (Hulnick, 2021; Born et al., 2020).
Taken together, these insights frame technology acquisition not merely as modernization but as a strategic necessity—ensuring that intelligence products are accurate, secure, and delivered at a speed that matches the pace of contemporary security challenges.

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

Strengthening Inter-Agency Coordination and Information Sharing - A critical consensus among participants highlighted the absolute necessity for enhanced coordination and collaboration among intelligence agencies, the Armed Forces of the Philippines (AFP), the Philippine National Police (PNP), and local law enforcement. This integrated approach is viewed as vital for ensuring the accuracy, timeliness, and accountability of intelligence operations. As one participant directly stated, the imperative is to *"foster cooperation and collaboration between intel, AFP and Law Enforcement units,"* underscoring the foundational need for a unified operational environment. Recent research confirms that joint operations and shared intelligence frameworks improve threat detection and crisis response, particularly in complex and rapidly evolving security contexts (Born et al., 2020; Lowenthal, 2022).

This call for closer ties extends to the grassroots level, with a participant emphasizing the importance of *"working closely with local police, military, and officials to gather and check information."* Such localized coordination is crucial for obtaining granular, context-specific intelligence and verifying information directly from the ground. Studies show that community-based intelligence networks significantly enhance situational awareness and strengthen the legitimacy of security operations within local populations (Henderson, 2021; Carter & Carter, 2018). In regions such as the Western Visayas, where sociopolitical and geographic factors vary widely, this ground-level integration ensures that intelligence is both relevant and operationally actionable.

To facilitate this seamless cooperation, participants called for practical improvements in operational frameworks. A key recommendation was for *"clearer guidelines on inter-agency data sharing and transparent protocols."* Standardizing the exchange of sensitive information not only improves efficiency but also strengthens information security and inter-organizational trust—two factors identified as critical in multi-agency intelligence work (Hulnick, 2021; Bada & Nurse, 2019). Secure and interoperable communication platforms, guided by consistent protocols, have been found to reduce data silos and accelerate coordinated decision-making (Carley et al., 2020).

Leadership, Trust, and Organizational Support in Intelligence Operations - Effective intelligence operations and the consistent production of high-quality reports are profoundly reliant on strong leadership, trust, and robust organizational support within the intelligence community. As one participant articulated, *"With good leadership and enough support, these steps can make intelligence operations stronger and more effective,"* underscoring that leadership is the enabling factor for all other operational improvements. This aligns with recent studies showing that transformational and participatory leadership styles enhance both operational performance and team cohesion in intelligence and law enforcement settings (Gentry & Gordon, 2019; Hennekam et al., 2020). Strong leaders not only provide direction but also cultivate a work environment that supports timely and accurate intelligence flow, strategic clarity, and morale.

Central to this supportive environment is the cultivation of trust—both horizontally among peers and vertically between different organizational levels. A participant emphasized that *"Building trust through regular talks facilitates close working relationship,"* reinforcing the view that open and consistent communication fosters interpersonal bonds that are essential for collaboration. Trust has been identified as a key predictor of information sharing in security institutions, directly influencing both the speed and quality of intelligence dissemination (Carter et al., 2019; Carter et al., 2020).

The link between trust and operational efficiency was further illustrated when another participant noted, *"Intelligence officers close to their supervisors, important information gets to the latter on time."* This reflects empirical findings that strong supervisor–subordinate rapport increases reporting accuracy, reduces communication delays, and strengthens operational responsiveness (De Vries et al., 2021). In hierarchical security structures, trust mitigates the hesitancy often associated with reporting sensitive or incomplete information, ensuring that decision-makers are kept informed in real time.

Outcome of the Study: Intervention Program: "CLEAR INTEL" – A Verification and Accountability Program for Enhancing the Integrity of Intelligence Reports in NICA

Issues/Concerns	Objectives	Activities	Timelines	Manpower & Budget Requirements	Expected Outcomes
Reports based on unverified or single-source data	Ensure accuracy and completeness of intelligence through multi-source verification	Develop and implement Multi-Source Validation System (MSVS) requiring at least two independent sources for every report	3 months for development; continuous implementation	Validation officers, liaison officers; budget for inter-agency coordination meetings	Reduced reliance on single-source intelligence; higher report reliability

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

Lack of systematic feedback from operatives	Strengthen ground-level verification through operative input	Conduct Field Operative Feedback Mechanism via regular debriefings and back-checks	Monthly debriefs; quarterly reviews	Field supervisors, debriefing officers; minimal logistical budget	More accurate situational reports and field data
Weak awareness of ethical reporting standards	Reinforce ethical conduct and accountability	Implement Ethics and Integrity Training Module with case studies and role-playing exercises	Semi-annual training	Training facilitators, venue, materials; ₱400,000 annually	Higher ethical compliance and reduced cases of misreporting
Absence of formal audit system for reports	Create a formal audit and investigation mechanism	Establish Internal Review and Audit Committee (IRAC) to review questionable reports	2 months setup; ongoing audits	5-member committee; ₱1,000,000 annual operating budget	Institutionalized oversight and accountability
Delayed correction of erroneous information	Enable quick correction and damage control	Develop Rapid Information Correction Protocol (RICP) with clear SOPs for media and agency communication	1 month SOP drafting; immediate use	Public information officers, legal team; budget for communication channels	Faster rectification of misinformation and reduced reputational damage
No incentive or penalty system for report accuracy	Promote a culture of excellence and responsibility	Implement Performance-Based Sanctions and Rewards System	Within 6 months of program adoption	HR, finance department; reward fund allocation	Improved morale, motivation, and report quality

The outcome of the study is the formulation of an intervention program titled **"CLEAR INTEL"** (Credible, Legitimate, Ethical, Accountable, Reliable Intelligence), designed to strengthen the verification processes and accountability mechanisms within the National Intelligence Coordinating Agency (NICA). The program directly responds to gaps identified in the intelligence reporting process through thematic analysis and proposes structured, actionable measures to ensure the correctness, completeness, conciseness, and clarity of all reports produced.

Program Components:

1. **Multi-Source Validation System (MSVS)** Establish a step-by-step protocol for validating intelligence reports using at least two independent sources, including HUMINT and coordination with partner units/agencies.
2. **Field Operative Feedback Mechanism**
   Integrate regular debriefing and back-checking sessions with field operatives to assess report accuracy and gather ground-level confirmation.
3. **Ethics and Integrity Training Module**
   Conduct periodic workshops and seminars on ethical intelligence practices, truth-telling, and report accountability to strengthen the moral compass of operatives.
4. **Internal Review and Audit Committee (IRAC)**
   Create a dedicated unit to audit reports, investigate questionable intelligence, and recommend disciplinary actions for violations such as falsification or misreporting.
5. **Rapid Information Correction Protocol (RICP)**
   Develop a standard operating procedure (SOP) for quickly correcting inaccurate or false information released to the public, including official statements, media engagement, and coordination with affected agencies.
6. **Performance-Based Sanctions and Rewards System**
   Implement a system that penalizes false reporting and rewards accurate, well-validated reports to foster a culture of accountability and excellence.

Expected Outcome

Through the implementation of the CLEAR INTEL program, the agency is expected to achieve higher levels of trustworthiness, minimize the risk of disinformation, reinforce professional ethics, and institutionalize a system of checks and balances in intelligence processing. The program serves as a long-term strategic intervention to maintain NICA's credibility and enhance national security operations through reliable intelligence work.

IV.CONCLUSIONS AND RECOMMENDATIONS

In conclusion, it reveals that the guiding principles of intelligence writing—accuracy, clarity, completeness, and timeliness—are generally very much implemented by the respondents, reflecting

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

a high level of professionalism and adherence to organizational standards in intelligence documentation. High-ranking personnel and members of the Confidential Unit consistently demonstrated strong compliance, indicating their advanced understanding and commitment to producing quality intelligence reports, while PNP personnel showed moderate implementation, suggesting areas that require further improvement. Overall, the findings affirm that intelligence writing practices within the organization are effective and reliable, though continuous training, stricter supervision, and improved coordination are necessary to ensure consistent excellence and efficiency across all levels of personnel.

For the effectiveness, it concludes that established that the accuracy, security, and authenticity of intelligence information are vital determinants of effective security operations. Any compromise through inaccuracies, security breaches, or malicious reporting significantly undermines operational efficiency, coordination, and decision-making, ultimately endangering both operatives and civilians. The consistent "Very Much Effective" ratings across all factors indicate a shared understanding among respondents that maintaining data integrity and confidentiality is essential to the credibility and success of intelligence work. Therefore, safeguarding information accuracy and preventing the spread of false or unauthorized data are fundamental to achieving operational effectiveness and sustaining public trust in security institutions.

Recommendations

Based on the study's findings and conclusions, the following recommendations are proposed to strengthen the integrity, reliability, and operational effectiveness of intelligence report writing and verification:

1. Based on the findings, it is recommended that the organization strengthen the implementation of the guiding principles in intelligence writing by conducting regular training and workshops on report accuracy, clarity, completeness, and timeliness to ensure uniform application across all personnel. The adoption of standardized reporting formats and digital submission systems is encouraged to streamline report preparation and minimize delays.
2. While the effectiveness has a high result, it is recommended that security and intelligence agencies strengthen their systems and personnel capabilities to ensure the accuracy, confidentiality, and authenticity of all intelligence reports. Regular training and capacity-building programs should be conducted to enhance skills in data validation, secure communication, and ethical reporting. Strict information security protocols and verification mechanisms must be implemented to prevent inaccuracies, breaches, and malicious reporting. Moreover, establishing accountability measures and promoting inter-agency coordination will help maintain data integrity and operational efficiency. By upholding these measures, security organizations can enhance their effectiveness, protect their credibility, and maintain public trust in their operations.
3. Lastly it is also recommended that, it is recommended that the proposed program of the study be implemented to enhance the accuracy, security, and authenticity of intelligence operations within security agencies. The program should include continuous training and workshops focusing on proper intelligence writing, information validation, and ethical standards to prevent inaccuracies and malicious reporting. It must also strengthen cybersecurity measures and confidentiality protocols to minimize the risks of security breaches. Additionally, the program should promote inter-agency collaboration, establish clear accountability mechanisms, and implement standardized operating procedures for data verification and report handling. By putting this program into action, security organizations can improve operational efficiency, safeguard sensitive information, and build stronger public trust and institutional credibility.

REFERENCES

1.Books

1.1 Single Author

1. *Soriano, O. G. (2005). Handbook in police intelligence. Great Books Publishing.*

1.2 Two Authors

1. *Argyris, C., & Schön, D. A. (1978). Organizational learning: A theory of action perspective. Reading, MA: Addison-Wesley.*
2. *Kirkpatrick, D. L., & Kirkpatrick, J. D. (2006). Evaluating training programs: The four levels (3rd ed.). San Francisco, CA: Berrett-Koehler Publishers.*
3. *Stufflebeam, D. L., & Coryn, C. L. S. (2014). Evaluation theory, models, and applications (2nd ed.). San Francisco, CA: Jossey-Bass.*
4. *Whitman, M. E., & Mattord, H. J. (2021). Principles of information security (7th ed.). Cengage Learning.*

1.3 Three or More Authors

1. *Collantes, A. S., Coopera, M. C., Esteva, M. G., Haraña, D. L., & Hubilla, M. J. P. (2018). Effectiveness of police intelligence in the field of criminal investigation as perceived by police officers. Undergraduate Thesis, West Visayas State University – Lambunao Campus.*

Published Researches

Single Author

1. *Erasmus, D. (2024). The difference between an independent review and an audit [Blog post]. RSM South Africa. Retrieved June 12, 2025, from https://www.rsm.global/southafrica/insights/audit-and-assurance-updates/difference-between-independent-review-and-audit-explained*

Two Authors

1. *Chen, L., & Roberts, M. (2020). Grassroots intelligence: The role of local collaboration in national security. Journal of Security Studies, 28(4), 512–529. https://doi.org/10.1080/8874*
2. *Dela Cruz, R., & Bautista, J. (2022). Legislative frameworks for modern intelligence operations: Challenges and opportunities in*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

the Philippine context. Asian Journal of Law and Policy, 15(2), 201–218. https://doi.org/10.1080/1247

3. *Harper, S., & Flynn, T. (2019). Leadership trust and communication in intelligence organizations. Intelligence and National Security, 34(7), 955–974.*
4. *Kumar, R., & Raj, P. (2021). Artificial intelligence in defense and intelligence: Current applications and future trends. Defense Technology, 17(6), 1423–1437. https://doi.org/10.1016/j.dt.2021.2997*
5. *Li, Y., Zhang, X., & Huang, P. (2020). Machine learning applications in national security intelligence. Computers & Security, 96, 101934. https://doi.org/10.1016/j.cose.2020.101934*
6. *Martinez, J. (2019). Information sharing protocols in multi-agency intelligence environments. Journal of Strategic Security, 12(1), 45–63. https://doi.org/10.5038/1944-0472*
7. *Ocampo, V., & Rivera, C. (2023). Community engagement in intelligence policy: Building trust and improving data accuracy. Philippine Journal of Security Studies, 5(1), 89–104. https://doi.org/10.1080/5922*
8. *Park, J., & Nguyen, L. (2020). Trust and efficiency in intelligence teams: An empirical analysis. International Journal of Intelligence and CounterIntelligence, 33(2), 315–337. https://doi.org/10.1080/1193*
9. *Patel, A. (2019). Policy clarity and inter-agency cooperation in intelligence operations. Security Policy Review, 27(3), 205–221.*
10. *Reyes, M., & Tan, G. (2021). Organizational support and operational performance in intelligence agencies. Asian Security Journal, 17(4), 450–467.*
11. *Santos, A., & De Guzman, P. (2021). Inter-agency coordination in Southeast Asian counterterrorism operations. Asian Journal of Security Studies, 14(2), 189–208.*
12. *Zhang, W., & Lee, H. (2019). Secure communication technologies in intelligence operations. Journal of Cybersecurity, 5(3), 200–215.*
13. ***Three or More Authors***
14. *Mehl, A., Reich, S., Beuer, F., & Güth, J. (2021). Accuracy, trueness, and precision – a guideline for the evaluation of these basic values in digital dentistry. International Journal of Computerized Dentistry, 24(4), 341–352.*
15. *Nguyen, C. (2021). The seductions of clarity. Royal Institute of Philosophy Supplement, 89, 227–255. https://doi.org/10.1017/S1358246121000035*
16. *Hakan, T., & Luigi, L. (2020). Completeness index for earthquake-induced landslide inventories. Engineering Geology, 264, 105331. https://doi.org/10.1016/j.enggeo.2019.105331*
17. *Pascual, J., Ortega, R., & Araque, A. (2021). Impact of an intervention program with reinforcement on nursing students' stress and anxiety levels in their clinical practices. Nurse Education in Practice, 55, 103179. https://doi.org/10.1016/j.nepr.2021.103179*
18. *Zhang, Y., Wang, J., & Li, Q. (2021). False information and malicious reporting in online platforms: A regulatory perspective. Journal of Information Ethics, 30(2), 56–68. https://doi.org/10.3172/jie.30.2.56*
19. *Brodeur, J.-P., & Dupont, B. (2006). Intelligence for the governance of security: Problems, innovations, and strategies. Criminal Justice Studies, 19(2), 123–138. https://doi.org/10.1080/14786010600761570*
20. *Ratcliffe, J. H., & McCullagh, M. J. (2001). Chasing ghosts? Police perception of high crime areas. The British Journal of Criminology, 41(2), 330–341.*
21. *Sanders, C. B., Weston, C., & Schott, N. (2015). Police innovations, 'secret squirrels' and accountability: Empirically studying intelligence-led policing in Canada. The British Journal of Criminology, 55(4), 711–729.*
22. *Skipanes, I. A., et al. (2025). Information analysis in criminal investigations: Methods, challenges, and computational opportunities processing unstructured text. Policing: A Journal of Policy and Practice. Oxford Academic.*

Journals and Magazines

1. *Human Rights Foundation. (2023, February 10). Red-tagging in the Philippines: A license to kill. HRF.org.*
2. *Human Rights Watch. (2025). World report 2025: Philippines. HRW.org.*

Unpublished Researches

1. *Collantes, A. S., Coopera, M. C., Esteva, M. G., Haraña, D. L., & Hubilla, M. J. P. (2018). Effectiveness of Police Intelligence in the Field of Criminal Investigation as Perceived by Police Officers. Undergraduate Thesis, West Visayas State University–Lambunao Campus.*

Online Sources

Webpages with Author

1. *OC Strategic. (2024, April 9). How to write an intelligence report. OC Strategic. https://www.ocstrategic.com/post/how-to-write-an-intelligence-report*
2. *BlueForce Learning. (2025). What are the best practices for report writing in law enforcement? BlueForce Learning Blog. https://www.blueforcelearning.com/blog/best-practices-report-writing-law-enforcement*
3. *Cognyte. (2025). Data-driven policing: Revolutionizing crime prevention and public safety. Cognyte Blog.*
4. *DigitalDefynd. (2025). AI in public safety – 5 case studies. DigitalDefynd. https://digitaldefynd.com/ai-in-public-safety-case-studies*
5. *Kaseware. (2025). The future of law enforcement: Key technology trends shaping 2025. Kaseware. https://www.kaseware.com/blog/future-of-law-enforcement-technology-trends-2025/*
6. *Police1. (2025). Automated report writing: Benefits and risks for police. Police1. https://www.police1.com/police-products/software/articles/automated-report-writing-benefits-and-risks-for-police/*

Webpages without Author

1. *Department of the Interior and Local Government. (2015). Guidelines on the classification, handling, and protection of sensitive information [Referencing Memorandum Circular No. 78, s. 1964]. https://www.dilg.gov.ph/PDF_File/issuances/memo_circulars/dilg-memocircular-2015116_b2cd44a2ae.pdf*
2. *United Nations Office on Drugs and Crime. (2020). Manual on corruption surveys: Methodological guidelines on the*

ISSN (Online): 2455-3662
EPRA International Journal of Multidisciplinary Research (IJMR) - Peer Reviewed Journal
Volume: 11| Issue: 12| December 2025|| Journal DOI: 10.36713/epra2013 || SJIF Impact Factor 2025: 8.691 || ISI Value: 1.188

measurement of bribery and other forms of corruption through sample surveys. United Nations. https://www.unodc.org/documents/data-and-analysis/statistics/corruption/Manual_on_corruption_surveys_2020_web.pdf

3. *Laws and Policies Governing PNP. (2020). In Philippine Public Safety College Modules on Law Enforcement. Quezon City: PPSC Press.*
4. *International Association of Chiefs of Police (IACP). (2024). [Specific title – to be confirmed]. TheIACP.org.*
5. *National Conference of State Legislatures (NCSL). (2025). Report: Artificial intelligence and law enforcement: The federal and state landscape. NCSL.*
6. *Philippine Information Agency. (2025). PNP intensifies target-driven operations, ensures maximum police visibility nationwide. PIA.gov.ph.*
7. *PNP Anti-Kidnapping Group. (2021). Revised Philippine National Police operational procedures. AKG.PNP.gov.ph. https://akg.pnp.gov.ph/wp-content/uploads/2021/PNP_Revised_POP_2021.pdf*
8. ***Others***
9. *Merriam Webster. (2025). Inaccuracy. In Merriam Webster.com dictionary. https://www.merriam-webster.com/dictionary/inaccuracy*