International Journal of Interdisciplinary Cultural Studies
ISSN: 2327-008X (Print), ISSN: 2327-2554 (Online)
Volume 21, Issue 2, 2026
https://cgscopus.com/index.php/journal

DEVELOPING AN INTEGRATED COMPUTER SECURITY INCIDENT RESPONSE TEAM (CSIRT) STRATEGIC AND POLICY FRAMEWORK TO SUPPORT NATIONAL AIR DEFENSE OPERATIONS

Tedi Rizalihadi[1]; Andriansyah, Andriansyah[2]; Evi, Satispi[3]
[1,2,3] Doctor Public Administration, Faculty of Social and Political Science, Universitas Muhammadiyah Jakarta, Indonesia.

Abstract: National air defense systems increasingly depend on interconnected digital technologies, making cybersecurity incident response a critical component of operational continuity and national security. However, Indonesia lacks an integrated Computer Security Incident Response Team (CSIRT) framework specifically designed for national air defense operations, resulting in fragmented incident response capabilities and interagency coordination challenges. This study aimed to develop an integrated CSIRT strategy and policy framework for Indonesia's National Air Operations Command (Koopsudnas) and its regional air defense commands. An exploratory sequential mixed-methods design was employed. The qualitative phase involved in-depth interviews with 20 informants representing eight institutions, followed by a quantitative validation phase using the Analytic Hierarchy Process (AHP) with the same 20 subject-matter experts. The findings identified five distinctive operational characteristics requiring a specialized CSIRT framework: time-critical response requirements, heterogeneous Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems, geographical dispersion across the Indonesian archipelago, zero-disruption operational requirements, and threats from nation-state-sponsored advanced persistent threat actors. In response, the study developed the CSIRT-PU Framework, incorporating a four-tier architecture, concurrent Observe–Orient–Decide–Act (OODA) cycle integration, a Pre-Authorized Response Matrix, and graceful degradation based on Minimum Viable Defense. The framework adopts a dual-lead network partnership governance model involving Koopsudnas and the National Cyber and Crypto Agency (BSSN). AHP validation produced an aggregate consistency ratio of 0.0127, with cyber resilience receiving the highest priority weight at 33.45%. The study also introduces three theoretical constructs: Mission-Critical Public Service Governance, Hybrid Command-Collaborative Governance, and the Integrated Cyber-Defense Governance Model. These findings provide an institutional and theoretical foundation for developing integrated cybersecurity incident response capabilities tailored to Indonesia's national air defense operations.

Keywords: Cybersecurity governance; computer security incident response team (CSIRT); national air defense; collaborative governance; cyber resilience.

International Journal of Interdisciplinary Cultural Studies
ISSN: 2327-008X (Print), ISSN: 2327-2554 (Online)
Volume 21, Issue 2, 2026
https://cgscopus.com/index.php/journal

INTRODUCTION

The growing integration of digital technologies has made cybersecurity a national defense concern. Air defense operations rely on interconnected infrastructures for radar surveillance, command and control, communications, and intelligence through Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) networks. These technologies improve coordination but create vulnerabilities that threaten critical functions (Freas et al., 2022). Mandiant (2024) reported increased advanced persistent threat (APT) activities targeting Southeast Asia's defense sector. Protecting air defense therefore requires technical capabilities and institutional arrangements for timely decisions, coordinated responses, and operational readiness (Macwan et al., 2024).

The challenge is significant for Indonesia across an extensive archipelagic territory. The National Air Operations Command (Komando Operasi Udara Nasional, Koopsudnas) and four regional Air Defense Sector Commands (Komando Sektor Pertahanan Udara, Kosek Hanud I–IV) operate across dispersed areas (McKenzie et al., 2023). Cyber incidents affecting radar, communication, or command systems may exceed individual units' responsibilities. Effective response requires clear roles and coordination among operational commands, cybersecurity authorities, defense policymakers, and military units (Jeelani & Prieto, 2025). The issue is how institutions organize authority and resources to protect this function.

Indonesia's cybersecurity framework includes Presidential Regulation No. 47 of 2023 on the National Cybersecurity Strategy (Awad & Jung, 2022). Law No. 3 of 2025 concerning the Indonesian National Armed Forces provides an institutional basis for cyber defense. Nevertheless, general commitments do not guarantee integrated incident response in military commands. The dissertation identifies no dedicated Computer Security Incident Response Team (CSIRT) framework for national air defense and fragmented responsibilities across Koopsudnas, the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara, BSSN), the Ministry of Defense, the Indonesian National Armed Forces Cyber Center (Pusat Siber TNI), and regional commands (Gadakh & Jaybhaye, 2025). Without formal mechanisms, responses may rely on informal communication rather than standardized procedures and clear authority.

This is a policy implementation problem involving regulation, coordination, resources, and capacity. The dissertation identifies unclear responsibilities between civilian cybersecurity authorities and military commands, no specialized military CSIRT regulations, limited personnel competencies, and inadequate budgets (Omar et al., 2025). These constraints may weaken

International Journal of Interdisciplinary Cultural Studies
ISSN: 2327-008X (Print), ISSN: 2327-2554 (Online)
Volume 21, Issue 2, 2026
https://cgscopus.com/index.php/journal

implementation. Andriansyah et al. (2023) emphasize that evidence-based implementation requires clear regulations, contextual adaptation, and institutionalized interagency coordination. A framework must integrate technical response with governance of authority, information, and resources (Pramanto et al., 2021).

New Public Governance (NPG) emphasizes interdependent actors, networks, and cross-sector collaboration, while collaborative governance highlights institutional design, shared processes, and trust (Chen et al., 2024). National air defense, however, involves hierarchical command, urgency, information sensitivity, and low tolerance for disruption. Deliberation alone may be inadequate when incidents demand immediate decisions. Governance must combine interagency collaboration with the command authority and response speed required for mission-critical operations (Abdelwanis et al., 2025).

A review of 24 studies reveals a gap in integrated CSIRT frameworks tailored to Indonesia's national air defense. Previous research addresses organizational CSIRT capabilities, military cybersecurity, C4ISR protection, collaborative governance, and policy implementation (Çeken & Acar, 2025). However, it does not comprehensively connect operational requirements, institutional authority, regulation, and implementation strategies in Indonesia's air defense commands. This limits guidance for translating national commitments into coordinated action (Ayoola et al., 2025). Addressing the gap extends public administration scholarship to a mission-critical setting shaped by interorganizational dependence and hierarchical command (Ezekiel et al., 2022).

This study develops an integrated strategic and policy framework for a CSIRT in Indonesia's national air defense in a geographically complex and operationally sensitive environment (Rahmita et al., 2022). It examines operational characteristics shaping requirements, develops an organizational and governance model, and formulates implementation strategies (Eugene, 2025). An exploratory sequential mixed-methods design combines qualitative exploration with quantitative prioritization through the Analytic Hierarchy Process (AHP). The study links air defense requirements with institutional and regulatory mechanisms for integrated response. It also advances three theoretical constructs: Mission-Critical Public Service Governance (MCPSG), Hybrid Command-Collaborative Governance (HCCG), and the Integrated Cyber-Defense Governance Model (ICDGM). These constructs adapt collaborative governance to public functions requiring continuity, clear authority, and coordinated action.

International Journal of Interdisciplinary Cultural Studies
ISSN: 2327-008X (Print), ISSN: 2327-2554 (Online)
Volume 21, Issue 2, 2026
https://cgscopus.com/index.php/journal

New Public Governance (NPG) provides a foundation for understanding cybersecurity incident response as a governance challenge (Panić & Xiaojun, 2025). Osborne (2010) emphasizes interdependence in public service delivery: complex problems require networks through which institutions coordinate expertise, responsibilities, and resources. Network governance explains how organizations cooperate while retaining distinct mandates. Provan and Kenis (2008) identify shared participant governance, lead organization governance, and network administrative organization governance, distinguished by their decision-making and coordination arrangements.

This perspective applies to Indonesia's national air defense. Koopsudnas leads operational air defense, while the National Cyber and Crypto Agency (Badan Siber dan Sandi Negara, BSSN) performs national cybersecurity coordination and regulatory functions (Mushtaq et al., 2023). Because no institution controls all necessary authority and resources, this study proposes dual leadership: Koopsudnas leads operational continuity decisions, while BSSN provides regulatory coordination and cybersecurity expertise. This arrangement coordinates complementary mandates while retaining military command (Sun et al., 2023).

Network governance cannot, however, be transferred uncritically to military settings, where hierarchical authority, classified information, and urgent decisions are essential. Deliberation may delay action during mission-critical incidents (Cheng, 2023). Collaborative governance offers insight into institutional coordination. Ansell and Gash (2008) identify institutional design, initial conditions, collaborative processes, and facilitative leadership as key elements. In national air defense, collaboration must accommodate unequal authority, protect confidential information, and meet operational requirements (Liu, 2025). The study develops Hybrid Command-Collaborative Governance (HCCG), comprising collaboration under normal conditions, accelerated coordination during heightened alert, and command-led decisions during emergencies. Appropriate mode depends on urgency, delay, and authority.

Policy implementation theory explains why formal commitments alone do not create operational capability. Sabatier and Mazmanian (2019) emphasize legislative capacity, implementing institutions, and non-legislative conditions (Minutolo, 2023). An integrated Computer Security Incident Response Team (CSIRT) requires clear responsibilities, standardized procedures, qualified personnel, sustainable funding, and coordination (Natarajan et al., 2022). The dissertation identifies three interdependent dimensions: regulatory capacity, concerning arrangements between military authority and national cybersecurity coordination; institutional capacity, concerning responsibilities and procedures; and resource capacity, covering personnel,

technical capabilities, and budgets. The study introduces the Integrated Cyber-Defense Governance Model (ICDGM), aligning legal authority, organizational arrangements, and implementation resources (Akbar et al., 2021).

CSIRTs receive and analyze incident reports, coordinate responses, and support system recovery. Military air defense requires adaptation because interconnected command, surveillance, communication, and information systems can transmit incident effects across components (Nurrahma & Berlilana, 2024). Responses must enable technical intervention while preserving command authority, confidentiality, and essential operations. Cyber resilience involves anticipating, withstanding, responding to, and recovering from disruption while maintaining critical functions. The dissertation applies a Minimum Viable Defense approach to graceful degradation, preserving essential capabilities when full performance is unavailable. It also integrates the Observe–Orient–Decide–Act (OODA) cycle and proposes a Pre-Authorized Response Matrix (PARM), linking incident assessment to predefined authorization thresholds to reduce delays and maintain accountability (Jiang, 2021).

A review of 24 studies across five clusters organizational CSIRT capabilities, military cybersecurity, air defense and C4ISR threats, multistakeholder governance, and policy implementation reveals an empirical and theoretical gap. Existing research discusses these dimensions separately but does not integrate them into a framework tailored to Indonesia's archipelagic air defense. General CSIRT guidance does not fully address military command requirements; military cyber research does not comprehensively examine Indonesia's institutional configuration; and conventional governance theories do not resolve the tension between collaboration and time-critical command (Bhadu et al., 2023).

This study addresses the gap by integrating NPG, network and collaborative governance, policy implementation, and cyber resilience into the CSIRT-PU framework. It advances three constructs: Mission-Critical Public Service Governance (MCPSG), emphasizing continuity, accountability, and mission-aligned decisions; HCCG, explaining transitions among collaborative, coordinative, and command-led modes; and ICDGM, linking regulation, institutional responsibilities, and resources. Qualitative exploration and quantitative prioritization using the Analytic Hierarchy Process (AHP) examine the framework. The study contributes to public administration by explaining how institutions can coordinate while preserving rapid decisions and public functions.

International Journal of Interdisciplinary Cultural Studies
ISSN: 2327-008X (Print), ISSN: 2327-2554 (Online)
Volume 21, Issue 2, 2026
https://cgscopus.com/index.php/journal

METHODOLOGY

This study employed an exploratory sequential mixed-methods design to develop an integrated strategic and policy framework for a Computer Security Incident Response Team (CSIRT) supporting Indonesia's national air defense (Kotte, 2025). Following Creswell and Plano Clark (2018), qualitative exploration identified operational, institutional, and regulatory requirements, informing quantitative prioritization through the Analytic Hierarchy Process (AHP). The design combined stakeholder perspectives with systematic assessment of framework components.

The research comprised three stages. First, qualitative analysis identified distinctive air defense characteristics and institutional gaps in cybersecurity incident response. Second, findings informed a preliminary CSIRT-PU framework and its AHP hierarchy. Third, qualitative themes and quantitative priorities were integrated to establish the final framework and implementation recommendations. The study examined arrangements across eight institutions. The scope included the National Air Operations Command (Koopsudnas), Regional Air Defense Sector Commands I–IV (Kosek Hanud I–IV), the National Cyber and Crypto Agency (BSSN), the Ministry of Defense, and the Indonesian National Armed Forces Cyber Center (Pussiber TNI) (Belinda et al., 2021). Purposive sampling selected participants based on professional responsibilities, cybersecurity or air defense knowledge, incident response or defense policy experience, and coordination expertise. Participation was voluntary. The qualitative phase involved 20 informants: eight strategic air defense officials, eight cybersecurity technical and policy practitioners, and four academics or policy experts. All 20 completed the AHP assessment, ensuring continuity between exploration and prioritization.

Qualitative data were collected through semi-structured interviews, focus group discussions (FGDs), non-participant observation, and document analysis. Interviews lasted 60–90 minutes and examined operational requirements, response arrangements, coordination, regulatory constraints, and CSIRT capabilities. With consent, interviews were recorded and transcribed verbatim. Three FGDs, lasting 90–120 minutes each, addressed operational requirements, technical capabilities and interagency coordination, and framework integration. Observation examined interunit coordination, incident reporting, interaction during exercises or simulations, C4ISR infrastructure, and relevant procedures. Document analysis covered regulations, air defense doctrines, operational procedures, cybersecurity guidance, and selected international CSIRT arrangements.

International Journal of Interdisciplinary Cultural Studies
ISSN: 2327-008X (Print), ISSN: 2327-2554 (Online)
Volume 21, Issue 2, 2026
https://cgscopus.com/index.php/journal

The quantitative phase applied Saaty's (1980) AHP to prioritize six framework parameters. Respondents compared criteria in pairs using the nine-point fundamental scale, completing 15 unique comparisons. Individual judgments were aggregated using the Geometric Mean Method (GMM), following Forman and Peniwati (1998).

Qualitative data were analyzed using Miles, Huberman, and Saldaña's (2014) interactive model: data condensation, display, and conclusion drawing and verification. Materials were coded, categorized, and thematically synthesized through deductive coding based on six initial parameters and inductive coding for emerging themes. NVivo supported data management. Comparative matrices, gap analyses, and institutional relationship maps displayed operational requirements and patterns of authority, information exchange, and resource coordination. Verification used source and methodological triangulation and member checking; five key informants reviewed interpretations.

AHP analysis involved hierarchy construction, pairwise comparisons, aggregation, consistency testing, and priority-weight calculation. Consistency used $CI = (\lambda max - n)/(n - 1)$ and $CR = CI/RI$, with $RI = 1.24$ for six criteria. A CR of 0.10 or below was acceptable; assessments exceeding this threshold were revised under the study protocol (Muhaqiqin et al., 2021). Normalized comparisons generated priority weights. All 20 respondents met the individual consistency threshold, while the aggregate matrix achieved a CR of 0.0127.

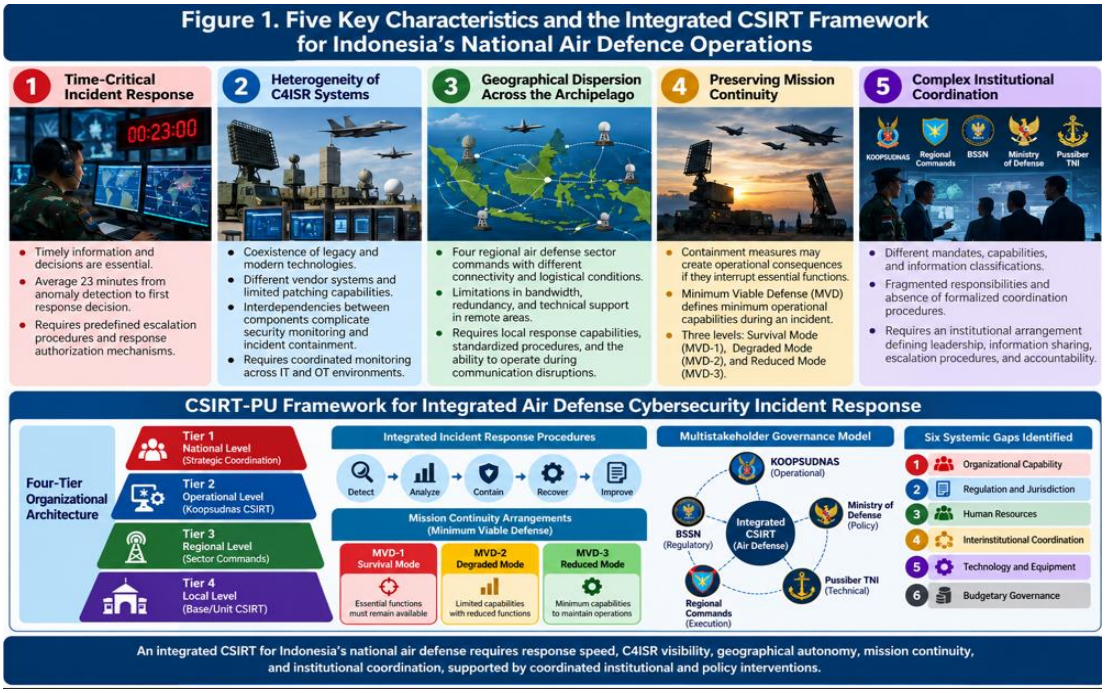
Integration occurred at three points: qualitative findings shaped the AHP hierarchy; qualitative themes were compared with priority weights through a convergence matrix; and both strands informed the final framework. Differences prompted further interpretation. Qualitative quality was assessed through credibility, transferability, dependability, and confirmability (Guba & Lincoln, 1994), supported by triangulation, member checking, peer debriefing, and contextual description. Quantitative quality relied on expert relevance and AHP consistency (Gilbreath, 2023). Ethical safeguards included voluntary participation, informed consent, dual-layer coding, restricted access, encrypted storage, and reporting that protected identities and sensitive operational information. The hierarchy linked the overall objective with six criteria and alternatives together.

International Journal of Interdisciplinary Cultural Studies
ISSN: 2327-008X (Print), ISSN: 2327-2554 (Online)
Volume 21, Issue 2, 2026
https://cgscopus.com/index.php/journal

RESULT AND DISCUSSION

Result

The qualitative analysis identified five distinctive characteristics of Indonesia's national air defense operations that shape the requirements for an integrated Computer Security Incident Response Team (CSIRT). These characteristics emerged from interviews with 20 informants, focus group discussions, non-participant observation, and document analysis. The findings indicate that cybersecurity incident response in national air defense involves interconnected operational, technological, geographical, and institutional challenges that cannot be addressed through technical controls alone.



The first characteristic is the requirement for time-critical incident response. Air defense operations depend on timely information and decisions, making prolonged incident assessment and approval procedures potentially incompatible with operational requirements. The dissertation reports that a tabletop exercise at Koopsudnas recorded an average of 23 minutes between anomaly detection and the first response decision, exceeding the operational response target identified in the study. This finding highlights the need for predefined escalation procedures and response authorization mechanisms that reduce unnecessary decision delays.

The second characteristic concerns the heterogeneity of Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems. The dissertation identifies the coexistence of legacy and modern technologies, differences in vendor systems, limited patching capabilities, and dependencies between interconnected

components. These conditions complicate security monitoring and incident containment because actions affecting one component may influence other operational systems. The findings consequently indicate a need for coordinated monitoring and incident response capabilities that account for both information technology and operational technology environments.

The third characteristic is geographical dispersion across the Indonesian archipelago. The four regional air defense sector commands operate under different connectivity and logistical conditions. The dissertation identifies limitations in bandwidth, redundancy, and access to technical support in geographically remote locations, particularly in the eastern sector. A centralized response model that depends on continuous connectivity may therefore be insufficient. Local response capabilities, standardized procedures, and the ability to operate during communication disruptions are essential design considerations.

The fourth characteristic is the requirement to preserve mission continuity during cybersecurity incidents. The study finds that conventional containment measures, including system isolation, may create operational consequences if they interrupt essential air defense functions. The proposed Minimum Viable Defense (MVD) concept addresses this problem by defining minimum operational capabilities that must remain available during an incident. The framework distinguishes Survival Mode (MVD-1), Degraded Mode (MVD-2), and Reduced Mode (MVD-3), with different operational capabilities and authorization requirements for each level.

The fifth characteristic is the complexity of coordination among institutions with distinct mandates. Koopsudnas, regional air defense commands, BSSN, the Ministry of Defense, and Pussiber TNI contribute different operational, regulatory, policy, and technical capabilities. However, the dissertation identifies fragmented responsibilities, differences in information classification, and the absence of formalized coordination procedures for active cybersecurity incidents. The findings suggest that an integrated CSIRT requires an institutional arrangement that defines leadership, information-sharing responsibilities, escalation procedures, and accountability across participating organizations.

Taken together, these findings demonstrate that the requirements for an air defense CSIRT extend beyond incident detection and technical recovery. They encompass response speed, C4ISR visibility, geographical autonomy, mission continuity, and institutional coordination. The dissertation further identifies six systemic gaps: organizational capability, regulation and jurisdiction, human resources, interinstitutional coordination, technology and equipment, and

International Journal of Interdisciplinary Cultural Studies
ISSN: 2327-008X (Print), ISSN: 2327-2554 (Online)
Volume 21, Issue 2, 2026
https://cgscopus.com/index.php/journal

budgetary governance. These gaps are interdependent, indicating that the development of an integrated CSIRT requires coordinated institutional and policy interventions. The study developed the CSIRT-PU framework to address the operational and institutional gaps identified in the qualitative phase. The framework combines a four-tier organizational architecture with integrated incident response procedures, mission continuity arrangements, and a multistakeholder governance model.

The four-tier architecture distributes capabilities according to operational scope and technical specialization. Tier 1, the Field CSIRT, operates at the regional air defense sector level and focuses on local anomaly detection, initial containment, and response under limited connectivity. Tier 2, the Operational CSIRT, is positioned at Koopsudnas and integrates information from regional units, supports incident analysis, and assesses the operational consequences of response measures. Tier 3, the TNI Air Force CSIRT, provides advanced technical capabilities, including operational technology forensics and malware analysis. Tier 4, the Military National CSIRT under Pussiber TNI, provides advanced cross-service capabilities and coordinates military-level technical support.

The proposed architecture is intended to distribute technical response capabilities without transferring the military operational chain of command to the CSIRT structure. Each tier performs complementary functions, enabling incidents to be handled locally when possible and escalated when additional expertise or coordination is required. This arrangement responds to the combination of geographical dispersion and the need for specialized capabilities that cannot be replicated at every operational location.

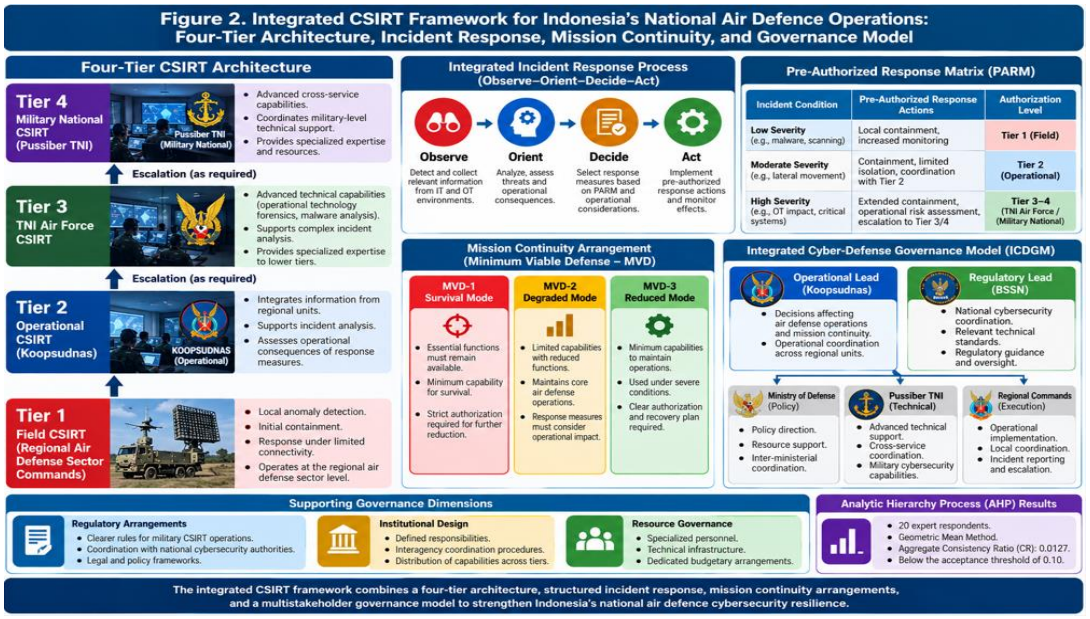


Figure 2. Integrated CSIRT Framework for Indonesia's National Air Defence Operations: Four-Tier Architecture, Incident Response, Mission Continuity, and Governance Model

International Journal of Interdisciplinary Cultural Studies
ISSN: 2327-008X (Print), ISSN: 2327-2554 (Online)
Volume 21, Issue 2, 2026
https://cgscopus.com/index.php/journal

The framework also integrates the Observe–Orient–Decide–Act (OODA) cycle into incident response and introduces a Pre-Authorized Response Matrix (PARM). OODA provides a decision-making sequence that links observation, assessment, decision, and action. PARM establishes predefined response actions and authorization arrangements for specified incident conditions. Together, these mechanisms are intended to reduce delays between incident detection and the initiation of appropriate response measures while retaining clear operational accountability.

Mission continuity is supported by the MVD concept and a doctrine of proportional response. Under this arrangement, response decisions must consider both the cybersecurity threat and the operational consequences of containment. Measures that would reduce capabilities below the applicable MVD level require authorization from the designated operational authority. This approach seeks to prevent technically appropriate containment actions from unintentionally compromising essential air defense functions.

At the institutional level, the framework proposes a dual-lead governance arrangement. Koopsudnas serves as the Operational Lead, responsible for decisions affecting air defense operations and mission continuity, while BSSN serves as the Regulatory Lead, contributing national cybersecurity coordination and relevant technical standards. The Ministry of Defense, Pussiber TNI, and regional air defense commands participate according to their respective policy, technical, and operational responsibilities.

The framework is supported by three governance dimensions: regulatory arrangements, institutional design, and resource governance. The regulatory dimension addresses the need for clearer rules governing military CSIRT operations and coordination with national cybersecurity authorities. The institutional dimension defines responsibilities and interagency coordination procedures. The resource dimension addresses specialized personnel, technical infrastructure, and dedicated budgetary arrangements. These dimensions form the proposed Integrated Cyber-Defense Governance Model (ICDGM).

The quantitative phase assessed the relative importance of six CSIRT-PU framework components using the Analytic Hierarchy Process. The judgments of 20 expert respondents were aggregated using the Geometric Mean Method. The dissertation reports an aggregate Consistency Ratio (CR) of 0.0127, below the study's acceptance threshold of 0.10.

International Journal of Interdisciplinary Cultural Studies
ISSN: 2327-008X (Print), ISSN: 2327-2554 (Online)
Volume 21, Issue 2, 2026
https://cgscopus.com/index.php/journal

Cyber resilience received the highest priority weight at 33.45%, followed by critical operational tempo at 19.26% and C2 integration at 17.07%. Multistakeholder coordination accounted for 14.23%, while doctrinal alignment and human resource capacity received weights of 9.52% and 6.47%, respectively.

The priority distribution indicates that the experts assigned the greatest relative importance to the framework's ability to preserve operational capabilities during cybersecurity incidents. Critical response speed and integration with command and control functions also received substantial weights. The aggregate CR of 0.0127 indicates that the combined pairwise comparison matrix met the study's consistency criterion.

These results informed the proposed implementation priorities. Cyber resilience and mission continuity were positioned as central design requirements, followed by rapid response procedures and integration with operational command structures. The study also emphasized that institutional coordination, doctrinal alignment, and personnel development remain necessary components of the framework, despite their lower relative weights.

Overall, the qualitative and quantitative findings were combined to produce a framework that links operational requirements with organizational structure, incident response procedures, and public governance arrangements. The resulting CSIRT-PU model is intended to provide an institutional basis for integrated cybersecurity incident response in Indonesia's national air defense system.

Discussion

The findings position cybersecurity incident response in national air defense as a public governance problem involving the coordination of authority, institutional capacity, and operational responsibility. The absence of a specialized CSIRT framework, as identified in the dissertation, reflects more than a technical capability gap. It also indicates difficulties in translating general cybersecurity policy commitments into arrangements that address the specific requirements of military operations.

International Journal of Interdisciplinary Cultural Studies
ISSN: 2327-008X (Print), ISSN: 2327-2554 (Online)
Volume 21, Issue 2, 2026
https://cgscopus.com/index.php/journal

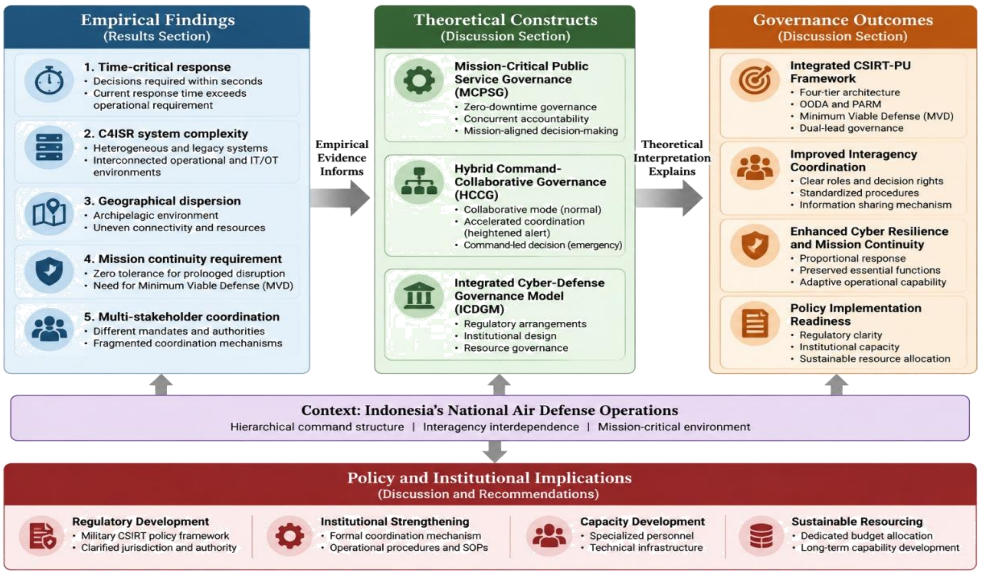


Figure 3. Discussion Framework: Linking Empirical Findings, Theoretical Constructs, and Policy Implications.

This study extends New Public Governance (NPG) to mission-critical institutions in Indonesia, where complex public problems require interdependent organizations (Osborne, 2010). In the CSIRT-PU context, no institution possesses all authority, expertise, capabilities, and resources required for integrated incident response. Coordination among Koopsudnas, BSSN, the Ministry of Defense, Pussiber TNI, and regional commands is essential.

Institutional interdependence does not eliminate differences in authority. Military decisions follow the chain of command, whereas national cybersecurity coordination involves distinct regulatory and technical responsibilities. The proposed dual-lead arrangement addresses this distinction: Koopsudnas leads operational continuity decisions, while BSSN provides cybersecurity coordination and expertise. This adapts network governance without consolidating institutional mandates, demonstrating how collaboration can coexist with differentiated authority.

The Analytic Hierarchy Process (AHP) reinforces the priority of mission continuity. Cyber resilience received the highest weight (33.45%), followed by critical operational tempo (19.26%). Response effectiveness depends on maintaining essential air defense functions, not merely detecting and containing incidents quickly. These findings inform Mission-Critical Public Service Governance (MCPSG), which advances three principles: zero-downtime governance, concurrent accountability, and mission-aligned decision-making. Together, they maintain essential functions, ensure reporting and escalation during response, and require interventions to consider operational consequences.

International Journal of Interdisciplinary Cultural Studies
ISSN: 2327-008X (Print), ISSN: 2327-2554 (Online)
Volume 21, Issue 2, 2026
https://cgscopus.com/index.php/journal

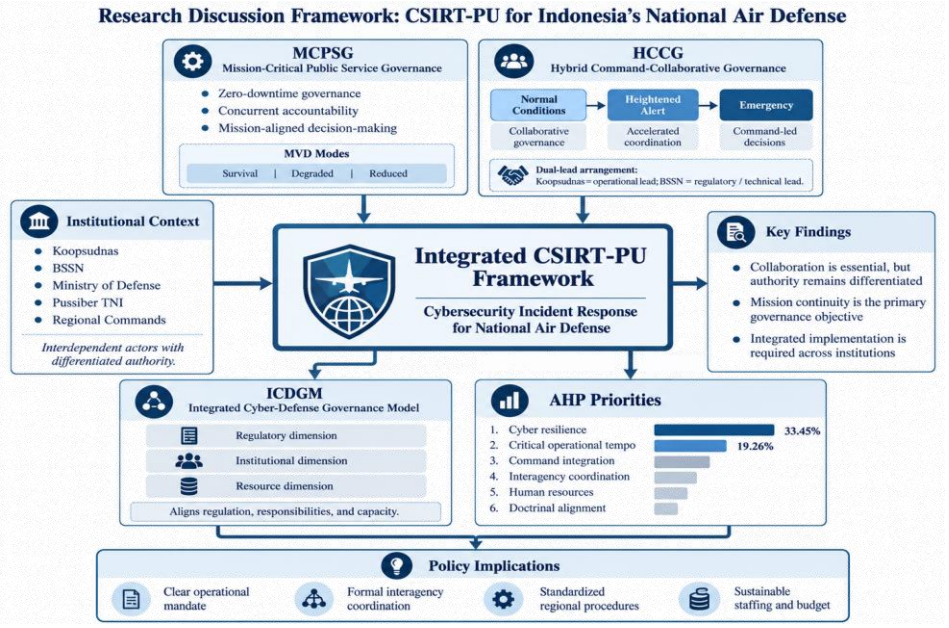


Figure 4. Author's elaboration based on Provan and Kenis (2008), Ansell and Gash (2008), Emerson et al. (2012), Ardebili et al. (2024), Staves et al. (2022), and Putro et al. (2024), integrated with the empirical findings of the present study.

The Minimum Viable Defense (MVD) approach translates these principles into Survival, Degraded, and Reduced modes. It identifies essential capabilities and authorization requirements for actions that may reduce operational capacity. Cybersecurity interventions can create operational risks if they disable critical systems without considering mission consequences.

The findings reveal tension between interagency collaboration and rapid decisions during urgent incidents. Collaborative governance emphasizes institutional design, shared motivation, and joint-action capacity (Ansell & Gash, 2008; Emerson et al., 2012). However, collaboration must reflect incident urgency. Hybrid Command-Collaborative Governance (HCCG) establishes three modes: collaboration under normal conditions, accelerated coordination during heightened alert, and command-led decisions during emergencies. This preserves routine collaboration while enabling timely action and accountability. Policy agreements should define decision rights, activation thresholds, escalation procedures, information-sharing protocols, and post-incident review.

The study identifies six implementation gaps involving organizational capability, regulatory authority, human resources, institutional coordination, technology, and budgetary governance. The Integrated Cyber-Defense Governance Model (ICDGM) connects regulatory arrangements, institutional responsibilities, and resource capacity. Clear regulations cannot create capabilities without trained personnel, infrastructure, and sustainable funding. Technical tools also require

agreed authorization and information-sharing procedures. ICDGM treats implementation as an integrated institutional process rather than separate procurement or regulatory reform.

Together, MCPSG, HCCG, and ICDGM contribute to public administration through mission-centered continuity, integration of collaboration and command, and an implementation model linking regulation, institutions, and resources.

The policy implications extend beyond establishing a technical team. CSIRT-PU requires a defined mandate, formal coordination with national cybersecurity authorities, standardized regional procedures, and sustainable staffing and budgets. Its four-tier architecture distributes technical capabilities, while dual leadership coordinates operational and regulatory responsibilities. Although AHP prioritizes cyber resilience, response speed, and command integration, lower-ranked components remain necessary. The framework reflects Indonesia's national air defense context and judgments from 20 experts; it does not demonstrate improved operational outcomes. Future studies should assess feasibility, response performance, institutional acceptance, and adaptability.

CONCLUSION

This study developed the CSIRT-PU framework as a context-specific strategic and policy response to the cybersecurity challenges facing Indonesia’s national air defense. The findings demonstrate that incident response in this environment is shaped by five interconnected characteristics: time-critical operational decisions, heterogeneous Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) systems, geographical dispersion across the archipelago, the imperative to maintain mission continuity, and advanced persistent threats associated with state actors. These characteristics show why conventional CSIRT arrangements cannot be adopted without adapting their structures, authority, and procedures to military operational requirements.

The framework integrates four mutually reinforcing components: a four-tier organizational architecture, the Observe–Orient–Decide–Act (OODA) cycle, a Pre-Authorized Response Matrix (PARM), and a Minimum Viable Defense (MVD) approach. Together, these components distribute technical capabilities across operational levels, accelerate incident assessment and response, clarify authorization, and protect essential air defense functions during disruption. The proposed dual-lead governance arrangement assigns operational leadership to Koopsudnas and regulatory coordination to the National Cyber and Crypto Agency (BSSN), while involving the

International Journal of Interdisciplinary Cultural Studies
ISSN: 2327-008X (Print), ISSN: 2327-2554 (Online)
Volume 21, Issue 2, 2026
https://cgscopus.com/index.php/journal

Ministry of Defense, Pussiber TNI, and regional commands according to their respective mandates.

The AHP assessment of 20 experts from eight institutions identified cyber resilience (33.45%), critical operational tempo (19.26%), and command-and-control integration (17.07%) as the three highest priorities, collectively accounting for 69.78%. The aggregate Consistency Ratio of 0.0127 indicates that the expert judgments met the study's consistency threshold; it does not, however, prove operational effectiveness. The study also advances three theoretical constructs: Mission-Critical Public Service Governance, Hybrid Command-Collaborative Governance, and the Integrated Cyber-Defense Governance Model. Overall, CSIRT-PU provides an integrated institutional and analytical foundation for strengthening cyber resilience while preserving military command authority, accountability, and continuity of Indonesia's national air defense mission. This contribution is particularly relevant to geographically dispersed defense operations where coordination and continuity must be maintained under pressure and uncertainty.

RECOMMENDATIONS

Implementation should begin with a regulatory instrument that establishes the CSIRT-PU mandate, scope, authority, and national cybersecurity coordination. The instrument should clarify the responsibilities of Koopsudnas as Operational Lead and BSSN as Regulatory Lead, while defining the roles of the Ministry of Defense, Pussiber TNI, and regional air defense commands. It should also specify information-classification rules, incident notification requirements, decision rights, escalation thresholds, and accountability mechanisms without transferring the military operational chain of command to the CSIRT structure.

Second, the four-tier architecture should be operationalized through standard operating procedures, role descriptions, and communication channels. Regional Field CSIRTs should be equipped to detect anomalies and undertake authorized initial response despite connectivity limitations. Koopsudnas should integrate regional reporting and assess operational consequences, while the TNI Air Force CSIRT and Pussiber TNI provide forensic, malware-analysis, and cross-service support. Coordination exercises should test escalation between tiers and clarify procedures during communication disruption.

Third, OODA and PARM should be translated into incident playbooks that define response options and authorization levels for specified conditions. The MVD framework should identify essential functions and thresholds for Survival, Degraded, and Reduced modes. Any action that

could reduce capabilities below the applicable MVD level should require authorization from the designated operational authority. Exercises should assess decision time, response coordination, mission continuity, recovery, and post-incident accountability.

Fourth, implementation requires an investment plan covering personnel, training, technical infrastructure, monitoring tools, and budgets. Resource allocation should reflect the AHP priorities while retaining the supporting importance of coordination, doctrinal alignment, and human-resource capacity. Finally, the framework should be introduced through pilot implementation and evaluated longitudinally. Future research should examine feasibility, institutional acceptance, response performance, and adaptability across other mission-critical public services. Evaluation should use operational exercises and indicators; the AHP consistency result alone should not be treated as evidence of effectiveness.

REFERENCE

Abdelwanis, N. S., Kashbur, A. M., & Elmnifi, M. (2025). Optimizing Wireless Telecommunication Tower Placement in Libya Using the Analytic Hierarchy Process (AHP). In *2025 IEEE 4th International Conference on Computing, Communication, Perception and Quantum Technology (CCPQT)* (hal. 1–9). IEEE. https://doi.org/10.1109/ccpqt66408.2025.11382604

Akbar, W., Mohezar, S., & Jaafar, N. I. (2021). Prioritizing Psychosocial Work Environment Factors for Knowledge Workers using Analytic Hierarchy Process (AHP). In *Studies of Applied Economics* (Vol. 39, Nomor 10). Editorial Universidad de Almeria. https://doi.org/10.25115/eea.v39i10.6299

Awad, J., & Jung, C. (2022). Extracting the Planning Elements for Sustainable Urban Regeneration in Dubai with AHP (Analytic Hierarchy Process). In *Sustainable Cities and Society* (Vol. 76, hal. 103496). Elsevier BV. https://doi.org/10.1016/j.scs.2021.103496

Ayoola, V., George, O. A., & Ogbemhe, J. (2025). Review and Application of the Analytic Hierarchy Process (AHP) for Maintenance Planning: A Case Study of Egbin Power Plant. In *ABUAD Journal of Engineering Research and Development (AJERD)* (Vol. 8, Nomor 3, hal. 221–230). Afe Babalola University Ado-Ekiti. https://doi.org/10.53982/ajerd.2025.0803.20-j

Belinda, B. I., Akintoba, A., Solomon, N., & Boniface, A. (2021). Evaluating Software Quality Attributes using Analytic Hierarchy Process (AHP). In *International Journal of Advanced Computer Science and Applications* (Vol. 12, Nomor 3). The Science and Information

Organization. https://doi.org/10.14569/ijacsa.2021.0120321

Bhadu, J., Bhamu, J., & Saraswat, P. (2023). An Analytic Hierarchy Process (AHP) Approach for Prioritizing the Industries 4.0 Technologies (I4.0T). In *Evergreen* (Vol. 10, Nomor 2, hal. 667–675). Kyushu University. https://doi.org/10.5109/6792813

Çeken, S., & Acar, A. B. (2025). Evaluating Non-Technical Skills of Airline Pilot Candidates Using an Analytic Hierarchy Process (AHP) Approach. In *Journal of Aviation* (Vol. 9, Nomor 1, hal. 207–215). Journal of Aviation. https://doi.org/10.30518/jav.1600583

Chen, G., Zhang, Y., & Jiang, R. (2024). A Novel Artificial General Intelligence Security Evaluation Scheme Based on an Analytic Hierarchy Process Model with a Generic Algorithm. In *Applied Sciences* (Vol. 14, Nomor 20, hal. 9609). MDPI AG. https://doi.org/10.3390/app14209609

Cheng, F. (2023). Evaluation of campus public space transformation with the analytic hierarchy process (AHP) approach: A case study from Bingwen academy of southeast university, China. In *Applied and Computational Engineering* (Vol. 24, Nomor 1, hal. 113–123). EWA Publishing. https://doi.org/10.54254/2755-2721/24/20230689

Eugene, C. (2025). Using Fuzzy Analytic Hierarchy Process to Rank Policy Aspirations for Child Protection in Aruba: A Capability Approach. In *Public Policy Making, Gender, and Human Security in the Caribbean* (hal. 285–327). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-81592-8_14

Ezekiel, B. B., Mustafa, F. B., Adelalu, G. T., & Yusuf, B. M. (2022). Site Selection Method Using the Geographic Information System (GIS) and Analytic Hierarchy Process (AHP). In *Geography of the Physical Environment* (hal. 11–26). Springer International Publishing. https://doi.org/10.1007/978-3-031-07113-3_2

Freas, R. L., Adair, H. F., & Hammad, E. (2022). An Engineering Process Framework for Cybersecurity Incident Response Assessment. In *2022 IEEE Conference on Dependable and Secure Computing (DSC)* (hal. 1–8). IEEE. https://doi.org/10.1109/dsc54232.2022.9888795

Gadakh, B. L., & Jaybhaye, R. G. (2025). Bridging Analytic Hierarchy Process (AHP) and GeoAI: Innovations in Geographical Decision- Making and Spatial Planning. In *Geo-Eye* (Vol. 14, Nomor 2, hal. 70–77). Bangalore University. https://doi.org/10.53989/bu.ge.v14.i2.25.22

Gilbreath, R. (2023). *The Nuclear System-of-Systems Capabilities Analytic Process (Doctoral Dissertation Defense) [Slides]*. Office of Scientific and Technical Information (OSTI). https://doi.org/10.2172/1993200

Jeelani, M., & Prieto, M. (2025). Using the Analytic Hierarchy Process (AHP) to Prioritize Augmented Reality (AR) Device Considerations. In *AHFE International* (Vol. 195). AHFE International. https://doi.org/10.54941/ahfe1006249

Jiang, M. (2021). Research on Supply Chain Integrated Planning Model Based on Analytic Hierarchy Process and Optimization Theory. In *2021 2nd International Conference on Computer Science and Management Technology (ICCSMT)* (hal. 60–63). IEEE. https://doi.org/10.1109/iccsmt54525.2021.00020

Kotte, G. (2025). AI-Powered Automated Incident Response in Healthcare Cybersecurity Operations. In *International Journal of All Research Education & Scientific Methods* (Vol. 13, Nomor 5, hal. 3369–3375). International Journal of All Research Education and Scientific Methods (IJARESM) Publication. https://doi.org/10.56025/ijaresm.2025.1210243369

Liu, Y. (2025). Prompt Engineering for GenAI in Cybersecurity Incident Response: A Multi-Platform Evaluation Based on NICE PR-IR-001. In *Journal of Cybersecurity Education, Research and Practice* (Vol. 2025, Nomor 1). Kennesaw State University - DIGITAL COMMONS JOURNALS. https://doi.org/10.62915/2472-2707.1259

Macwan, R., Martin, M., Waligoske, E., Williams, G., & Wright, V. (2024). *Cyber-Informed Engineering Research and Development Guide*. Office of Scientific and Technical Information (OSTI). https://doi.org/10.2172/2448074

McKenzie, L. R., Lee, D., & Amoako-Attah, J. (2023). Analysis of Hydrogen Production Methods Using the Analytic Hierarchy Process. In *Engineering Future Sustainability* (Vol. 1, Nomor 1). University of West London. https://doi.org/10.36828/efs.206

Minutolo, M. (2023). Application of the Analytic Hierarchy Process for Solving Social Wicked Problems. In *International Journal of the Analytic Hierarchy Process* (Vol. 15, Nomor 1). Creative Decisions Foundation. https://doi.org/10.13033/ijahp.v15i1.1156

Muhaqiqin, Sufathona, U., & Jupriyadi. (2021). Decision Support System Using Analytic Hierarchy Process Algorithm to Determine Cattle Worth to Sell. In *2021 International Conference on Computer Science and Engineering (IC2SE)* (hal. 1–8). IEEE. https://doi.org/10.1109/ic2se52832.2021.9791922

Mushtaq, F., Farooq, M., Tirkey, A. S., & Sheikh, B. A. (2023). Analytic Hierarchy Process (AHP) Based Soil Erosion Susceptibility Mapping in Northwestern Himalayas: A Case Study of Central Kashmir Province. In *Conservation* (Vol. 3, Nomor 1, hal. 32–52). MDPI AG. https://doi.org/10.3390/conservation3010003

Natarajan, N., Vasudevan, M., Dineshkumar, S. K., & Anuja, R. (2022). Comparison of Analytic Hierarchy Process (AHP) and Fuzzy Analytic Hierarchy Process (f-AHP) for the Sustainability Assessment of a Water Supply Project. In *Journal of The Institution of Engineers (India): Series A* (Vol. 103, Nomor 4, hal. 1029–1039). Springer Science and Business Media LLC. https://doi.org/10.1007/s40030-022-00665-x

Nurrahma, E., & Berlilana, B. (2024). Implementation of Analytical Hierarchy Process (AHP) Method on Teacher Performance Appraisal Decision Support System. In *CSRID (Computer Science Research and Its Development Journal)* (Vol. 16, Nomor 3, hal. 330–343). University of Potensi Utama Medan. https://doi.org/10.22303/csrid-.16.3.2024.330-343

Omar, M. A., Etebaai, I., Taher, M., & Tawfik, A. (2025). Landslide susceptibility mapping in the Bokoya Massif, Northern Morocco: A geospatial and multi-factor analysis using the analytic hierarchy process (AHP). In *Scientific African* (Vol. 30). Elsevier BV. https://doi.org/10.1016/j.sciaf.2025.e02980

Panić, M., & Xiaojun, Q. (2025). Failure mode and effects analysis–analytic hierarchy process (FMEA-AHP) model in supplier risk management. In *The Journal of Risk Model Validation*. Infopro Digital Services Limited. https://doi.org/10.21314/jrmv.2025.009

Pramanto, F. X. A., Oktora, E., Ramlan, R., Drajat, M., & Nasullah, I. (2021). ERP Software Selection Strategy Using Analytic Hierarchy Process (AHP) Case Study: PT Gramedia Printing. In *bit-Tech* (Vol. 4, Nomor 2, hal. 40–46). Komunitas Dosen Indonesia. https://doi.org/10.32877/bt.v4i2.286

Rahmita, D., Purwanto, E., Pranoto, E., & Rusmandani, P. (2022). Determining the Priority Element in Safety Management System of Public Transport with Analytic Hierarchy Process (AHP). In *RSF Conference Series: Engineering and Technology* (Vol. 2, Nomor 2, hal. 37–48). Research Synergy Foundation. https://doi.org/10.31098/cset.v2i2.557

Sun, Y., Hoi, L. M., & Im, S. K. (2023). Constructing the Evaluation Index System of Chinese-Portuguese Machine Translation using the Delphi and Analytic Hierarchy Process Methods. In *2023 IEEE 3rd International Conference on Power, Electronics and Computer Applications (ICPECA)* (hal. 190–195). IEEE. https://doi.org/10.1109/icpeca56706.2023.10075920