# Publishing Intelligence Products for the Public: Design Principles for Indonesia's Governance Model

**Agustina Setianingrum[1]*, Fuad Gani[2], Budi Wiweko[3]**
[1.2]Universitas Indonesia, Depok, Indonesia
[3]Sekolah Tinggi Intelijen Negara, Bogor, Indonesia

**Corresponding Author.**
*Email: agustina.setianingrum41@ui.ac.id

***Abstract**: Unclassified intelligence products published by intelligence organisations, often discussed in the literature as forms of public intelligence, have become more common over the last decade. These products are increasingly used not only to brief policy elites but also to build public resilience, counter disinformation, and strengthen the legitimacy of security measures that affect social and economic stability. This shift creates an information-governance dilemma in which disclosure must improve public preparedness while still protecting sources and methods, managing politicisation risks, and meeting legal duties of secrecy. Using a comparative qualitative document analysis, this paper examines 10 unclassified public documents released in 2021–2025 and the publication portals that host them, across four cases, the United States (Office of the Director of National Intelligence/ODNI), Australia (National Intelligence Community/NIC), Canada (Canadian Security Intelligence Service/CSIS), and the Netherlands (Algemene Inlichtingen- en Veiligheidsdienst/AIVD). The cases are chosen because their public products are produced by coordinator or community-integrator entities, making them a closer analogue to Indonesia's setting where Badan Intelijen Negara (BIN) holds a coordinating mandate. Cross-case findings are synthesised into 12 design principles and translated into an auditable governance model for Indonesia, including a staged release workflow and an audit-trail repository. The paper contributes (i) a comparative variable framework for analysing public intelligence products as governance artefacts, (ii) actionable design principles, and (iii) an implementable governance model that balances transparency, security, and accountability.*
***Keywords:** public intelligence, threat assessment, information governance, transparency, secrecy*

## 1. INTRODUCTION

Over the last decade, more governments have begun publishing intelligence products-based threat assessments in unclassified form for public consumption. The practice responds to a changing threat landscape in which terrorism and violent extremism, cyber and disinformation operations, coercive state activity, and hybrid threats affect not only state decision-makers but also citizens, businesses, and communities. In such contexts, intelligence is increasingly expected to support public preparedness and resilience, not only confidential policy deliberation.

The Russia–Ukraine war highlighted how public intelligence disclosure can function as early warning, deterrence, and strategic communication. Studies of intelligence disclosure in that period show a deliberate effort to pre-empt adversarial narratives and increase coalition cohesion, while still managing the risks of exposing capabilities and sources [1], [2]. In information environments vulnerable to disinformation, credible threat communication also shapes trust in institutions and public compliance with protective measures [3].

Yet openness in the intelligence domain is always bounded by secrecy. Secrecy literature emphasises that state secrets are socially and legally protected to secure sources, methods, liaison relationships, and operational effectiveness [4], [5]. Public releases can therefore create a 'disclosure dilemma' in which the broader and more specific the release, the higher the risk that adversaries infer sensitive capabilities or exploit the information politically [6].

In Indonesia, the tension between secrecy and transparency is sharpened by the coexistence of legal mandates. Intelligence law emphasises compartmentation and protection of intelligence secrets, while the public information regime recognises citizens' right to access information from public bodies, subject to national-security exemptions [7], [8]. Without a clear operational model, intelligence communication to the public risks either under-disclosure (reducing preparedness and legitimacy) or over-disclosure (raising security risks).

This paper addresses two research questions, namely

a. what design characteristics and governance safeguards define successful public threat-assessment products across comparable countries?
b. what design principles can be synthesised into a governance model suitable for Indonesia's institutional and legal context?

The comparative cases are selected because their public products are produced by coordinator or community-integrator entities, which is closer to Indonesia's institutional setting where Badan Intelijen Negara (BIN) performs a coordinating mandate [7].

The paper's novelty lies in treating public intelligence disclosure as an information-governance problem rather than a communication tactic alone. By combining intelligence-disclosure scholarship with information-governance concepts (decision rights, life-cycle controls, and auditability), the study reframes unclassified threat assessments as governance artefacts that must be designed, reviewed, released, and evaluated through traceable procedures. Empirically, the paper contributes a cross-case comparative matrix, a synthesis of 12 design principles, and a practical governance model for Indonesia that specifies a staged release workflow and an audit trail.

## 2. THE COMPREHENSIVE THEORETICAL BASIS AND ANALYTICAL FRAMEWORK

### 2.1 Public Intelligence and Unclassified Intelligence Products

Unclassified intelligence products released to the public can be understood as 'public intelligence', analytic outputs intentionally designed for external audiences, communicated through open channels, and framed to support public understanding and, in some cases, collective action [9], [10]. Recent scholarship argues that such disclosures can be strategic tools in international and domestic politics, particularly when states seek to shape narratives, counter adversarial messaging, or build resilience against information manipulation [1], [2].

Importantly, public intelligence does not imply abandoning analytic tradecraft. Rather, the core challenge is to translate assessment into accessible, actionable content while preserving analytic integrity and protecting sensitive sources and methods. Empirical studies of recent disclosure campaigns highlight three practical moves, namely sanitisation of details, cautious language for confidence and uncertainty, and a consistent emphasis on what is known versus what is assessed [1], [11].

From a governance perspective, public threat assessments should be treated as structured information products with clear purpose statements, stable taxonomies, and documented review procedures. These features are central to preventing misinterpretation and to ensuring that disclosure serves public value rather than short-term political messaging [6], [12].

### 2.2 Intelligence Communication Modes: Awareness, Advice and Co-production

Building on intelligence communication research, Petersen distinguishes three communication modes, namely awareness, advice, and co-production [13]. Awareness aims to raise understanding and legitimacy, advice provides guidance and recommendations for behaviour, while co-production invites collaborative sensing and reporting between institutions and the public, which in turn requires clear roles, procedures, and information protections [14].

For public threat assessments, advice-oriented communication is particularly relevant when threats require broad societal mitigation (for example: cyber hygiene, disinformation recognition, or reporting suspicious approaches). Co-production can be supported through safe feedback channels that allow citizens and private-sector actors to contribute indicators without exposing sensitive operational details. The communication mode selected shapes not only content but also governance requirements, especially around accountability and feedback management [13].

### 2.3 Secrecy–Transparency Dilemma and Selective Declassification Risks

Public intelligence releases sit in the long-standing tension between secrecy as a security necessity and transparency as a democratic requirement. Secrecy studies describe state secrecy as a social construct with legal protections that enable intelligence effectiveness and protect individuals and international liaison relationships [4], [5]. At the same time, democracies rely on transparency to enable informed consent and to reduce abuse of power.

One key risk is selective declassification, namely the deliberate public release of only supportive fragments while withholding contradictory material, which can mislead public debate and erode trust. Legal and policy scholarship shows how selective declassification can distort the 'marketplace of ideas' and create durable misperceptions even after corrections emerge [6]. In the intelligence domain, this risk is heightened by asymmetric access because the executive holds most classified material and can shape narratives through what it chooses to reveal.

Therefore, a governance model for public threat assessments must include safeguards that separate analytic production from political spin and that document redactions, confidence levels, and limitations. These safeguards support both legitimacy and security by making the disclosure process auditable while keeping operational secrets protected [6]. When formal accountability channels are weak, whistleblowing is often treated as a last-resort accountability mechanism, even though it creates serious legal and ethical dilemmas for intelligence insiders [15], [16]. Comparative legal analysis of espionage law in the UK and Australia shows why secrecy protections should remain effective but also appropriate and proportionate, a consideration relevant when designing disclosure boundaries [17].

### 2.4 Oversight and Accountability in Intelligence Governance

Intelligence oversight is often framed as a balance between necessary secrecy and democratic control. Comparative studies of oversight reform indicate a shift from parliamentarian-only bodies toward parliamentary committees with stronger mandates, resources, and access to scrutinise policy, budgets, and selected operations [18]. In the digital era, oversight challenges intensify due to data scale, cross-agency collaboration, and new analytic tools, which is why Dutch experience emphasises adaptive accountability arrangements for intelligence and security domains [19]. External oversight models also stress institutional independence, clear legal mandates, secure access to documents, secrecy safeguards, and adequate resourcing as key conditions for credible review [20].

However, oversight can be weakened when secrecy simply expands the circle of insiders. Normative analyses propose that transparency should be understood as procedural and selective, not full disclosure of all information, but an accountable system in which decisions, rationales, and controls can be reviewed by authorised bodies [4], [15].

In the context of public releases, oversight needs to focus on process integrity, examining whether products follow defined tradecraft standards, whether risks were assessed, and whether redaction decisions are recorded and reviewable. This shifts oversight away from 'what is revealed' and toward how disclosure decisions are made, which is a key move for information governance.

### 2.5 Information Governance for Public Intelligence Dissemination

Information governance provides concepts and tools to manage high-stakes information across its life-cycle, from creation, review, and release, to archiving and reuse. In digitised public administration, information governance is often discussed as an organisational capability to use information resources effectively while minimising risk and cost [21]. Governance focuses on decision rights, accountability, quality assurance, and risk management, which is why it is useful for public intelligence products that are both informative and potentially sensitive. Work connecting records management to information governance further underscores that governance is not only a technical procedure but also an institutional arrangement of roles, authority, and cross-unit accountability [22].

Governance literature also highlights metadata, version control, and retention schedules as foundations for traceability, especially where information governance intersects with IT governance [23]. Data-governance research shows that clarifying decision rights and controls can increase value while reducing cost and risk, a logic that also fits the management of sensitive information released in limited form [24]. ISO/IEC 38505-1 extends IT-governance principles to data governance, emphasising responsibility, strategy, performance, conformance, and human behaviour, which can be adapted as guiding principles for public-sector disclosure governance [25].

At the national level, integrated information-governance frameworks help ensure that disclosure policies across agencies are consistent, evaluable, and not dependent on ad hoc judgement [26]. Yet governance effectiveness is also shaped by organisational culture, because internal norms and routines can strengthen or undermine formal rules [27]. Studies of data professionals in the Netherlands likewise show a persistent gap between legal and ethical frameworks on paper and everyday practice, a warning for Indonesia that governance must be operable, not merely declarative [28]. Taken together, the secrecy–transparency dilemma and politicisation risk indicate that Indonesia needs a governance-ready model that operationalises legal boundaries

while enabling credible public-facing products.

### 2.6 Analytical Framework and Operationalisation of Comparative Variables

Drawing on the concepts above, the analytical framework maps comparative variables into four dimensions, namely (a) strategic purpose and audiences; (b) communication mode (awareness, advice, and co-production); (c) content structure and analytic tradecraft (summaries, confidence, limitations, threat taxonomy); and (d) information-governance safeguards (review process, redaction, dissemination infrastructure, archiving, and auditability). These dimensions are operationalised through a coding matrix (Table 2) applied consistently to each national corpus.

## 3. METHOD

This study uses a qualitative approach based on comparative document analysis and a synthesis of design principles. The comparative document analysis examines unclassified intelligence products published for the public and identifies recurring design elements and governance safeguards across cases. The synthesis step translates the comparative findings into a set of reusable design principles and a proposed governance model for Indonesia. The workflow follows qualitative document-analysis guidance and the READ approach (**R**eady your materials, **E**xtract data, **A**nalyse data, and **D**istil your findings) to keep extraction and synthesis traceable [29], [30].

### 3.1 Document Corpus

The corpus was selected in two stages. First, we reviewed the primary publication portals of ODNI (dni.gov), Australia's National Intelligence Community (intelligence.gov.au), CSIS (canada.ca), and AIVD (english.aivd.nl), screening items released in 2021–2025 that are unclassified and intended for external audiences (the public, sectors, or broad stakeholders). Second, from the screened set we selected a core corpus that represents (i) at least one flagship product communicating national or macro threat priorities and (ii) supporting publications that make governance safeguards visible, such as procedural transparency, accountability reporting, or risk-control arrangements. The core corpus comprises 10 documents, while the portal structures and archives are analysed as governance artefacts to capture metadata, retention, and findability signals (Table 1).

Table 1. Comparative Document Corpus

| Country | Organisation/Unit | Public Products/Documents |
|---|---|---|
| United States | Office of the Director of National Intelligence (ODNI) | - 2025 Annual Threat Assessment of the U.S. Intelligence Community (unclassified, flagship) [31]<br>- ODNI Annual Statistical Transparency Report CY2024 [32]<br>- ODNI Reports & Publications portal (2021–2025 archive) [33] |
| Australia | National Intelligence Community Australia (NIC) | - ASIO Annual Threat Assessment 2025 (via intelligence.gov.au) [34]<br>- ASIO Annual Threat Assessment 2024 (via intelligence.gov.au) [35]<br>- National Terrorism Threat Level statement [36]<br>- NIC News portal [37] |
| Canada | Canadian Security Intelligence Service – Integrated Threat Assessment Centre (CSIS/ITAC) | - CSIS Public Report 2024 [38]<br>- CSIS Public Report 2022 [39]<br>- Avoiding Complicity in Mistreatment by Foreign Entities Act 2024: Annual Report to the Minister of Public Safety (information-sharing & human-rights governance; includes ITAC) [40]<br>- ITAC page [41]<br>- CSIS Publications portal [42] |
| Netherlands | Algemene Inlichtingen- en Veiligheidsdienst (AIVD) | - AIVD Annual Report 2024 [43] |

- Threat Assessment of State Actors 2025 [44]
- AIVD document/publications portal [45]

### 3.1.1 Case-Selection Rationale

The four cases were selected because they share a mature model of public threat-assessment production and because their public products are generated by coordinator or community-integrator entities. Across the cases, (i) there is a navigable portfolio of public products hosted on official portals; (ii) a flagship product explicitly presents national or macro threat priorities; (iii) there are signals of accountability through annual reporting, transparency documentation, or connection to external review; and (iv) the production and release function is located in an organisation or unit that integrates intelligence across the community (whole-of-community). This fourth criterion increases comparability with Indonesia, where BIN carries a statutory coordinating role in the national intelligence system [7]. In the corpus, this integrator role is reflected by ODNI in the United States, the National Intelligence Community framework in Australia, ITAC within CSIS in Canada, and AIVD as the general intelligence and security service that issues national-level assessments in the Netherlands [33], [37], [41], [45].

### 3.1.2 Data Collection and Metadata Management

All documents were downloaded from the official portals of each organisation (Table 1). For each item, structured metadata were recorded, including title, year, issuing body, document type, classification status (unclassified/declassified), source URL, and contextual notes. In addition, portal-level cues surrounding each publication, such as the page-level release date, archive placement, and download links, were logged as evidence of authority and as part of the research audit trail. Maintaining structured metadata supports traceability and enables replication, consistent with information-governance practice.

## 3.2 Coding Technique and Comparative Matrix

Coding was performed in two passes. In the first pass, open coding identified recurring elements such as document structure, threat categories, audience cues, confidence language, and explicit redaction markers. In the second pass, axial coding mapped these elements onto the four analytical dimensions and structured them into a cross-case matrix. Table 2 summarises the operational codebook used to guide consistent coding and comparison.

Table 2. Codebook and Comparative Variables

| Dimension | Indicator | Coding question |
|---|---|---|
| Strategic purpose & audience | Deterrence; resilience; counter-disinformation; accountability; target publics/segments | What purpose is stated/implied? Who is the primary audience (general public, sectors, government)? |
| Communication mode | Awareness / advice / co- production | Is the product primarily awareness, advice, or co-production, collaboration/feedback)? |
| Structure & tradecraft | Key judgements; executive summary; confidence level; limitations | Is there a structured summary (key judgments) and tradecraft notes (confidence, limitations)? |
| Threat taxonomy & scope | State/non-state actors; cross-domain (cyber, interference, economy); time horizon | How are threats grouped, prioritised, and bounded (time cut-off/scope)? |
| Actionability | Recommendations; indicators; mitigation steps; referrals to support resources | Is there clear and realistic guidance for public/sector audiences? |

| | | |
|---|---|---|
| Disclosure governance | Mandate; declassification/redaction process; risk testing; separation of roles | Is the release mechanism explained (approval, redaction, legal/risk review) and is there a separation between analytic and communications functions? |
| Oversight & accountability | Internal/external oversight; transparency reporting; correction/complaints mechanism | How is accountability expressed, through oversight bodies, transparency reports, or correction and complaint channels? |
| Distribution, archiving & metadata | Portal; yearly archive; version control; accessibility; dissemination channels | Is there a searchable portal/archive, structured metadata (year, version), and accessible formats? |

### 3.3 Unit of Analysis

The unit of analysis is the public product as an information artefact, including its structure, content, tradecraft cues, and the surrounding governance signals visible on the publishing portal (archiving, disclaimers, updates, and related transparency pages). Cross-case comparison focuses on regularities and differences that can be distilled into design principles relevant for Indonesia.

### 3.4 Design-Principle Synthesis Procedure

Design-principle synthesis translates empirical patterns into reusable guidance for a target context. The procedure applied here follows a five-step logic. (1) Prepare the corpus and verify authority. (2) Extract design and governance elements using the codebook. (3) Analyse cross-case patterns and contrasts. (4) Distil recurring patterns into candidate principles. (5) Evaluate the principles for reusability and refinement using criteria of accessibility, importance, novelty or insightfulness, actability (guidance), and effectiveness [46]. The outputs are (a) a cross-case element summary (Table 3), (b) synthesised design principles (Table 4), and (c) the proposed governance model (Figure 2) with an auditable release workflow (Table 5).

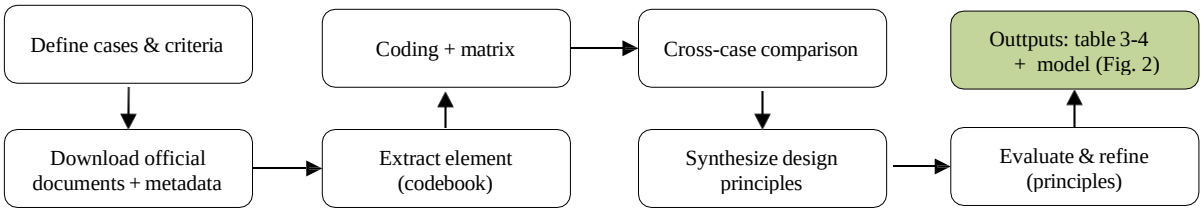


Figure 1. The algorithm of comparative document analysis and design-principle synthesis flowchart

The flowchart clarifies the end-to-end pipeline, from corpus preparation and metadata logging, to codebook-guided extraction and coding, cross-case comparison, principle distillation, and reusability-focused evaluation. An audit trail is maintained at each step to support replication and procedural transparency [24], [29], [46].

## 4. RESULTS AND DISCUSSION

### 4.1. Cross-Case Patterns in Public Intelligence Products

#### 4.1.1. Portfolio, Cadence, and Stated Purpose

Across the four cases, public threat communication is institutionalised through recurring flagship products and supporting governance-oriented publications. In our corpus, the United States case combines the Intelligence Community's Annual Threat Assessment with a statistical transparency report that exposes aspects of surveillance-authority use. Australia's public output is centred on a high-visibility annual threat assessment delivered by ASIO leadership and complemented by public statements such as the National Terrorism Threat Level. Canada pairs public reports with an integrated threat-assessment function (ITAC) and publishes a dedicated annual report on human-rights safeguards in foreign information sharing. The Netherlands combines annual reporting with thematic state-actor threat assessments. Despite differences in format, the stated purposes converge

around resilience-building, countering disinformation, and legitimising protective measures, while also shaping external perceptions [1], [2].

#### 4.1.2. Procedural Transparency and Quality Assurance

Procedural transparency appears as an enabling condition for legitimacy. Even when internal review cannot be disclosed in full, each case provides signals of process, including page-level dating and archiving, prefaces that specify scope, audience, and analytic limitations, and stable document structures. Quality assurance is communicated through tradecraft markers such as confidence language and clear separation between evidence, assessment, and advice. Importantly, governance-oriented publications in the corpus also make decision rights and safeguards partially visible, for example through descriptions of escalation paths, restriction mechanisms, and mitigation measures in higher-risk information-sharing contexts. These practices align with the literature's emphasis on safeguarding analytic integrity when intelligence is used for public diplomacy and strategic communication [1], [6].

#### 4.1.3. Content Structure and Threat Taxonomy

All cases employ relatively stable threat taxonomies that help readers navigate complex risk landscapes. Threats are commonly organised by actor (state and non-state), domain (cyber, influence operations), and modality (terrorism, espionage, sabotage). Structured summaries, such as key judgments or executive summaries, reduce cognitive load and make the products usable for non-specialists. From an information-governance standpoint, threat taxonomies function like public classification schemes that improve findability and comparability across years.

#### 4.1.4. Actionability and Audience Segmentation

Actionability varies across cases but a common trend is the inclusion of baseline advice, such as behavioural guidance, reporting channels, or sector-specific protective measures. Advice-oriented content is most visible where threats require distributed mitigation (cyber and influence threats), aligning with Petersen's 'advice' and 'co-production' modes [13]. In environments marked by disinformation and low trust, actionability also reinforces credibility because publics are more likely to treat the product as a practical reference rather than political messaging [3].

#### 4.1.5. Dissemination Infrastructure, Archiving, and Auditability

All cases rely on official web portals as the primary dissemination infrastructure. The portals differ in usability, but each provides some combination of searchable archives, thematic groupings, and supporting transparency pages. Versioning and retention are particularly visible through annual archives and updated documents, which together support a public-facing audit trail, the ability to retrieve what was published, when it was published, and how it relates to the institution's broader portfolio. This infrastructure is essential to avoid the 'vanishing document' problem and to support ex-post accountability without exposing classified sources [4].

Table 3. Salient Design Elements by Country

| Country | Salient design elements |
|---|---|
| United States | ODNI's portal provides a wide, year-by-year archive of public products (2021–2025), including the Annual Threat Assessment (with key-judgement style summaries) and statistical transparency reporting. The portfolio stands out for consistent document structuring, stable threat taxonomy, and retrievability through a clear archive design. [31], [32], [33] |
| Australia | Public products on Australia's National Intelligence Community portal are anchored in high- visibility statements and the Annual Threat Assessment, which frames macro threats and emphasises advice and shared responsibility. The news/archive function supports continuity and public access across years. [34], [37] |
| Canada | CSIS combines an annual public report that educates audiences about threats with an Integrated Threat Assessment Centre (ITAC) mandate that signals coordination of threat assessment across partners. The publication set supports both awareness and actionable guidance for sectors. [38], [41], [42] |
| Netherlands | AIVD publishes an annual report that combines threat overview with performance |

| | |
|---|---|
| | accountability, alongside thematic threat assessments (e.g., on state actors) that describe actors, tactics, and risks such as sabotage. The publications portal and links to oversight/annual reporting reinforce accountability signals. [43], [44], [45] |

### 4.2. Synthesised Design Principles

Comparative patterns were distilled into a set of design principles intended to be reusable for Indonesia's context. The principles integrate product design (readability, structure, taxonomy, advice) with governance requirements (decision rights, redaction logging, legal-ethical checks, archiving, and oversight traceability). Table 4 summarises the synthesised principles in a concise form.

Table 4. Design Principles (DP) for Indonesia (Synthesis)

| Code | Design principle (brief) |
|---|---|
| DP1. Mandate and public purpose | Define an explicit mandate for the public product (aims, namely awareness/resilience, deterrence, counter-disinformation, and/or accountability) and specify scope and time horizon. |
| DP2. Audience segmentation and communication mode | Identify primary audiences and select a communication mode (awareness/advice/co-production) per product so that messaging and actionability match public/sector needs [13]. |
| DP3. Proportional transparency and redaction discipline | Apply a proportional-disclosure logic that maximises public value while minimising harm to sources, methods, and liaison relationships; document the rationale for redactions [4], [5]. |
| DP4. Analytic integrity and quality assurance | Protect analytic integrity through structured tradecraft cues (key judgements, confidence language, evidence–assessment separation) and internal review before release. |
| DP5. Stable threat taxonomy and comparability over time | Use a consistent threat taxonomy and recurring structure to enable year-to-year comparison, trend reading, and policy tracking [31], [33], [43]. |
| DP6. Action-oriented guidance | Where appropriate, translate assessments into clear, role-specific guidance (what to watch, what to do, where to report) without drifting into operational detail [13], [47]. |
| DP7. Coordination signals and 'whole-of-community' framing | Make coordination visible through references to cross-agency integration or community framing, strengthening credibility and shared responsibility. |
| DP8. Anti-politicisation safeguards | Separate intelligence assessment from partisan messaging; use process safeguards and oversight hooks to reduce selective disclosure and instrumentalisation risks [2], [6]. |
| DP9. Archiving, version control, and audit trail | Maintain a searchable archive, version history, and correction mechanism so the public can trace what was released, when, and under which basis [21], [23]. |
| DP10. Legal basis and decision rights | Clarify legal authority, decision rights, and accountability roles for drafting, redaction, approval, and publication, anchored in national law and oversight arrangements [7], [8]. |
| DP11. Feedback, evaluation, and learning loop | Provide feedback channels and evaluate reach, comprehension, and unintended effects; use findings to improve subsequent releases [21], |

| | |
|---|---|
| | [47]. |
| DP12. Social sensitivity and trustbuilding | Design messaging with sensitivity to social impact (including minority communities) and provide engagement channels so transparency supports trust and legitimacy [13], [47]. |

### 4.3. Implications for Indonesia: Governance Model and Release Workflow

For Indonesia, the key lesson is that publishing public threat assessments requires an explicit governance model that treats disclosure as a controlled process rather than an ad hoc communication act. Such a model should be anchored in BIN's coordinating mandate and should operationalise decision rights and accountability across drafting, redaction, review, approval, release, and evaluation. Figure 2 visualises the proposed governance model, focusing on the release flow and the audit-trail repository that supports procedural transparency while protecting sources and methods. In Figure 2, blue arrows indicate decision flow, orange diamonds denote control points, and green dashed links indicate audit-trail records. Italic labels within each stage indicate the BIN unit leading that step [6], [7], [15].

**Tiered Release Flow and Control Points: Mapping to BIN Units**

Operationally, a tiered release model can be embedded in BIN's existing functional separation. Under Presidential Regulation No. 90/2012 (as amended), the Deputy for Analysis and Intelligence Production can serve as the analytic integrator; the Deputy for Communications and Information can manage public-facing dissemination; the Main Secretariat can provide legal support, documentation, and archiving; and the Main Inspectorate can conduct audit, review, evaluation, and monitoring of procedural compliance [48]. Strengthened thematic functions, such as cyber intelligence and apparatus-protection intelligence, can provide domain inputs at the drafting stage, enabling a whole-of-agency view without collapsing decision rights [49], [50]. Control points (CP1–CP5) align with drafting sign-off, redaction log approval, impact-test clearance, tiered approval, and release/archiving verification, each producing an auditable artefact (Table 5).

In decision-rights terms, each control point assigns a clear 'who decides what'. At CP1, the Deputy for Analysis and Intelligence Production authorise the analytic draft to enter the redaction track and sets the scope limits. At CP2, designated classification and information-security officers authorise the redacted version for downstream review and approve the redaction log, with the Deputy for Communications and Information validating public readability. At CP3, the Main Secretariat (legal and compliance) clears the consequence test and risk-mitigation memo. At CP4, the Deputy Head endorses cross-functional readiness and the Head of BIN issues final public-release authorisation. At CP5, the Deputy for Communications and Information with the Main Secretariat confirms version freeze, metadata and retention, and hands the audit-trail package to the Main Inspectorate for post-release audit.

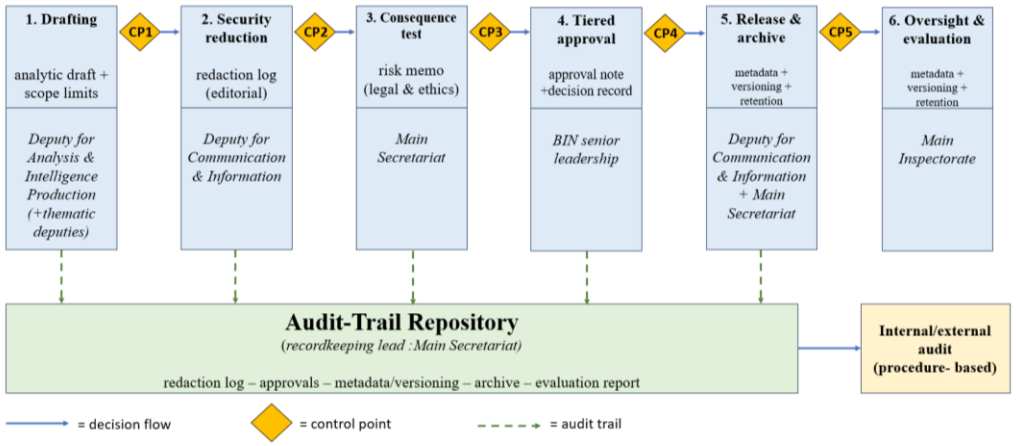


Figure 2. Indonesia's Governance Model for Publishing Unclassified Threat Assessments (BIN Units per Stage) and Audit Trail

Table 5. Release Stages and Audit-Trail Artefacts

| Stage/Control point | Primary actor (examples) | Audit-trail artefact (examples) |
|---|---|---|
| 1. Drafting (analytic writing) | Deputy for Analysis & Intelligence Production (integrator) + thematic deputies | Analytic draft; assumptions memo; date; accountable analyst; (optional) open-source references list. |
| 2. Information-security redaction | Information-security editorial team (analysts + classification authority); input from Deputy for Communications & Information | Redaction log; list of edited sections; redaction rationale; document version history and change log. |
| 3. Harm / risk assessment | Main Secretariat + legal/ethics advisers; input from counterintelligence | Consequence assessment memo; classification decision note; risk register; mitigation actions. |
| 4. Release approval | BIN senior leadership; cross-functional clearance committee | Approval memo; decision record; sign- off list; release date and authority. |
| 5. Publication and archiving | Deputy for Communications & Information (portal/PR) + Main Secretariat (metadata/archive) | Published document; metadata (version, date, tags); archive entry; permanent identifier/link. |
| 6. Oversight and evaluation | Inspectorate + external oversight (where applicable) | Evaluation report; access statistics; correction records; improvement recommendations. |

### 4.4. Implementation Roadmap (High Level)

Implementation can be staged. Phase 0 (0–6 months) should establish mandate and objectives for publishing (e.g., annual macro threat assessment), define audience segments, and issue a risk-based editorial guideline aligned with secrecy and public-information laws [7], [8]. It should also assign decision rights across analysis, information-security editorial, legal/ethics review, communications, and archiving, and define how internal and external oversight can review the process without requiring full public disclosure. Phase 1 (6–12 months) can pilot a flagship product, validate readability and relevance with stakeholder feedback, and test safe feedback channels to support limited co-production indicators. Phase 2 (12–24 months) can expand the product portfolio, strengthen metadata and retention schedules, and institutionalise evaluation metrics (reach,

comprehension, behavioural uptake, and misinterpretation risks).

## 5. CONCLUSION

This paper examined how unclassified intelligence products, especially public threat assessments, are designed and governed in four comparable cases and translated the cross-case findings into design principles and a governance model for Indonesia. Based on 10 public documents released in 2021–2025 and the surrounding portal signals, the comparison shows that high-credibility public products combine structured summaries, stable threat taxonomies, explicit confidence and limitations language, and actionable advice. Equally important, the cases demonstrate that legitimacy depends on procedural transparency, documented review steps, risk-based redaction, clear decision rights, and strong archiving with metadata and version control. For Indonesia, aligning these practices with BIN's coordinating mandate suggests a governance model that makes release decisions traceable and auditable, balancing public value with source-and-method protection, legal compliance, and safeguards against politicisation.

## REFERENCES


[1] H. Dylan and T. J. Maguire, "Secret Intelligence and Public Diplomacy in the Ukraine War," *Survival*, vol. 64, no. 4, pp. 33–74, Jul. 2022, doi: 10.1080/00396338.2022.2103257.

[2] R. Buluc, R. Arcos, and C. Ivan, "When spies go public! Lessons learnt from the instrumentalization of intelligence for strategic communication in the run-up to the Russian-Ukrainian war," *Intell. Natl. Secur.*, vol. 40, no. 1, pp. 42–57, Jan. 2025, doi: 10.1080/02684527.2024.2405255.

[3] W. L. Bennett and S. Livingston, "The disinformation order: Disruptive communication and the decline of democratic institutions," *Eur. J. Commun.*, vol. 33, no. 2, pp. 122–139, Apr. 2018, doi: 10.1177/0267323118760317.

[4] S. Lefebvre, "State Secrecy: A Literature Review," *Secrecy Soc.*, vol. 2, no. 2, Jan. 2021, doi: 10.31979/2377-6188.2021.020209.

[5] S. Lefebvre, "What do judges say on the protection of intelligence secrets?," *Intell. Natl. Secur.*, vol. 34, no. 1, pp. 62–77, Jan. 2019, doi: 10.1080/02684527.2018.1526494.

[6] S. Dudding, "Spinning Secrets: The Dangers of Selective Declassification," *Yale Law J.*, vol. 130, no. 3, pp. 708–777, Jan. 2021.

[7] R. Indonesia, "Undang-Undang Nomor 17 Tahun 2011 tentang Intelijen Negara." 2011.

[8] Republik Indonesia, "Undang-Undang Nomor 14 Tahun 2008 tentang Keterbukaan Informasi Publik." 2008.

[9] S. Lóránt, "Public Intelligence in Public Diplomacy: U.S. Strategic Intelligence Sharing in the New Age of Great Power Competition," *Nemzetbiztonsági Szle.*, vol. 13, no. 2, pp. 3–17, Aug. 2025, doi: 10.32561/nsz.2025.2.1.

[10] A. Marleku, "Public intelligence as a strategic tool: The role of real-time intelligence disclosure in the Ukraine War," *Secur. Def. Q.*, vol. 50, no. 2, pp. 50–65, Jun. 2025, doi: 10.35467/sdq/205566.

[11] K. Gustafson, D. Lomas, S. Wagner, N. S. Abdalla, and P. H. J. Davies, "Intelligence warning in the Ukraine war, Autumn 2021 – Summer 2022," *Intell. Natl. Secur.*, vol. 39, no. 3, pp. 400–419, Apr. 2024, doi: 10.1080/02684527.2024.2322214.

[12] O. Riemer, "Politics is not everything: New perspectives on the public disclosure of intelligence by states," *Contemp. Secur. Policy*, vol. 42, no. 4, pp. 554–583, Oct. 2021, doi: 10.1080/13523260.2021.1994238.

[13] K. L. Petersen, "Three concepts of intelligence communication: awareness, advice or co-production?," *Intell. Natl. Secur.*, vol. 34, no. 3, pp. 317–328, Apr. 2019, doi: 10.1080/02684527.2019.1553371.

[14] J. Evans, S. McKemmish, and G. Rolan, "Participatory information governance: Transforming recordkeeping for childhood out-of-home Care," *Rec. Manag. J.*, vol. 29, no. 1/2, pp. 178–193, Mar. 2019, doi: 10.1108/RMJ-09-2018-0041.

[15] W. H. Harwood, "Secrecy, transparency and government whistleblowing," *Philos. Soc. Crit.*, vol. 43, no. 2, pp. 164–186, Feb. 2017, doi: 10.1177/0191453716677178.

[16] R. W. Bellaby, "The ethics of whistleblowing: Creating a new limit on intelligence activity," *J. Int. Polit. Theory*, vol. 14, no. 1, pp. 60–84, Feb. 2018, doi: 10.1177/1755088217712069.

[17] S. Kendall, "Espionage law in the UK and Australia: Balancing effectiveness and appropriateness," *Camb.*

*Law J.*, vol. 83, no. 1, pp. 62–98, Mar. 2024, doi: 10.1017/S0008197323000466.
[18] A. Defty, "From committees of parliamentarians to parliamentary committees: comparing intelligence oversight reform in Australia, Canada, New Zealand and the UK," *Intell. Natl. Secur.*, vol. 35, no. 3, pp. 367–384, Apr. 2020, doi: 10.1080/02684527.2020.1732646.
[19] J. Constantino and B. Wagner, "Accountability and oversight in the Dutch intelligence and security domains in the digital age," *Front. Polit. Sci.*, vol. 6, p. 1383026, Jun. 2024, doi: 10.3389/fpos.2024.1383026.
[20] C. Klöckner and L. A. Joia, "External oversight of Intelligence activities in the digital age: An exploratory model," *Braz. J. Public Adm.*, vol. 59, no. 3, 2025.
[21] D. C. G. Brown and S. Toze, "Information governance in digitized public administration," *Can. Public Adm.*, vol. 60, no. 4, pp. 581–604, Dec. 2017, doi: 10.1111/capa.12227.
[22] J. Brooks, "Perspectives on the relationship between records management and information governance," *Rec. Manag. J.*, vol. 29, no. 1/2, pp. 5–17, Mar. 2019, doi: 10.1108/RMJ-09-2018-0032.
[23] H. Borgman, H. Heier, B. Bahli, and T. Boekamp, "Dotting the I and Crossing (out) the T in IT Governance: New Challenges for Information Governance," in *2016 49th Hawaii International Conference on System Sciences (HICSS)*, Koloa, HI, USA: IEEE, Jan. 2016, pp. 4901–4909. doi: 10.1109/HICSS.2016.608.
[24] R. Abraham, J. Schneider, and J. Vom Brocke, "Data governance: A conceptual framework, structured review, and research agenda," *Int. J. Inf. Manag.*, vol. 49, pp. 424–438, Dec. 2019, doi: 10.1016/j.ijinfomgt.2019.07.008.
[25] ISO/IEC, "ISO/IEC 38505-1:2017 Information technology—Governance of IT—Governance of data—Part 1: Application of ISO/IEC 38500 to the governance of data." 2017.
[26] P. A. Mullon and M. Ngoepe, "An integrated framework to elevate information governance to a national level in South Africa," *Rec. Manag. J.*, vol. 29, no. 1/2, pp. 103–116, Mar. 2019, doi: 10.1108/RMJ-09-2018-0030.
[27] A. Daneshmandnia, "The influence of organizational culture on information governance effectiveness," *Rec. Manag. J.*, vol. 29, no. 1/2, pp. 18–41, Mar. 2019, doi: 10.1108/RMJ-09-2018-0033.
[28] I. Fest, M. Wieringa, and B. Wagner, "Paper vs. practice: How legal and ethical frameworks influence public sector data professionals in the Netherlands," *Patterns*, vol. 3, no. 10, p. 100604, Oct. 2022, doi: 10.1016/j.patter.2022.100604.
[29] H. Morgan, "Conducting a Qualitative Document Analysis," *Qual. Rep.*, vol. 27, no. 1, pp. 64–77, 2022, doi: 10.46743/2160-3715/2022.5044.
[30] S. L. Dalglish, H. Khalid, and S. A. McMahon, "Document analysis in health policy research: the READ approach," *Health Policy Plan.*, vol. 35, no. 10, pp. 1424–1431, Feb. 2021, doi: 10.1093/heapol/czaa064.
[31] Office of the Director of National Intelligence, "Annual Threat Assessment of the U.S. Intelligence Community." 2025.
[32] Office of the Director of National Intelligence, "Annual Statistical Transparency Report." 2025.
[33] "Reports & Publications of the Office of the Director of National Intelligence." [Online]. Available: https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2025
[34] Australian National Intelligence Community, "ASIO Annual Threat Assessment 2025." Accessed: Mar. 05, 2026. [Online]. Available: https://www.intelligence.gov.au/news/asio-annual-threat-assessment-2025
[35] Australian National Intelligence Community, "ASIO Annual Threat Assessment 2024." Accessed: Mar. 05, 2026. [Online]. Available: https://www.intelligence.gov.au/news/asio-annual-threat-assessment-2024
[36] Director-General of Security, Mike Burgess AM, "National Terrorism Threat Level." Accessed: Mar. 05, 2026. [Online]. Available: https://www.intelligence.gov.au/news/national-terrorism-threat-level
[37] "News and Updates of the National Intelligence Community." [Online]. Available: https://www.intelligence.gov.au/news
[38] Canadian Security Intelligence Service, "CSIS Public Report 2024," p. 90, Mar. 2025.
[39] Canadian Security Intelligence Service, "CSIS Public Report 2022," p. 90, 2022.
[40] Canadian Security Intelligence Service, "Avoiding Complicity in Mistreatment by Foreign Entities Act : Annual Report to the Minister of Public Safety."
[41] Canadian Security Intelligence Service, "Integrated Threat Assessment Centre." Accessed: Mar. 05, 2026. [Online]. Available: https://www.canada.ca/en/security-intelligence-service/integrated-threat-assessment-centre.html
[42] "Publications of the Canadian Security Intelligence Service." [Online]. Available: https://www.canada.ca/en/security-intelligence-service/corporate/publications.html

[43] Algemene Inlichtingen- en Veiligheidsdienst (AIVD), “AIVD annual report 2024,” 2024.
[44] Algemene Inlichtingen- en Veiligheidsdienst (AIVD), “Threat Assessment of State Actors 2025.” Algemene Inlichtingen- en Veiligheidsdienst (AIVD), 2025.
[45] “Publications of General Intelligence and Security Service.” [Online]. Available: https://english.aivd.nl/documents/2025/09/26/threat-assessment-of-state-actors-2025
[46] J. Iivari, M. R. P. Hansen, and A. Haj-Bolouri, “A Framework for Light Reusability Evaluation of Design Principles in Design Science Research,” *Proc Des. Sci. Res. Inf. Syst. Technol. DESRIST*, 2018.
[47] T. Juneau, “National Security Transparency and Relations with Minority Communities,” *Int. J. Intell. CounterIntelligence*, vol. 37, no. 1, pp. 156–174, Jan. 2024, doi: 10.1080/08850607.2023.2175630.
[48] Republik Indonesia, “Peraturan Presiden Nomor 90 Tahun 2012 tentang Badan Intelijen Negara.” 2012.
[49] Republik Indonesia, “Peraturan Presiden Nomor 73 Tahun 2017 tentang Perubahan atas Peraturan Presiden Nomor 90 Tahun 2012 tentang Badan Intelijen Negara.” 2017.
[50] Republik Indonesia, “Peraturan Presiden Nomor 79 Tahun 2020 tentang Perubahan Kedua atas Peraturan Presiden Nomor 90 Tahun 2012 tentang Badan Intelijen Negara.” 2020.