Guillaume Nicaise
Mahaut Fanchini

Strategic ignorance in multilateral organisations: obscuring accountability, enabling corruption

Read online

'Strategic ignorance' describes how organisations limit what information is acknowledged or acted upon, and how it can be useful for some things to remain obscure or unknown. This often leads to reduced oversight and misconduct. In multilateral organisations, the ways in which confidentiality, discretion, and organisational culture shape what is shared or silenced can create channels for strategic ignorance. For executive boards, programme managers, and donor agencies, recognising and reducing strategic ignorance is key to strengthening oversight and safeguarding aid integrity.

Main points

- Strategic ignorance is a deliberate or systemic condition where information is selectively concealed, downplayed, or dismissed in ways that obstruct accountability and enable misconduct. It is produced through decisions about what is documented, shared, or silenced within an organisation.

- In multilateral organisations, strategic ignorance is shaped by confidentiality protocols, internal discretion, and organisational incentives. It operates through both formal systems and informal professional cultures.

- These dynamics affect how misconduct is reported, how risks are managed, and what becomes publicly visible.

- Our research draws on empirical material from the UN Office for Project Services (UNOPS) housing-programme scandal, and the UN's Oil-for-Food Programme, as well as interviews with staff across UN agencies.

- We show that reducing strategic ignorance requires more than compliance. It involves embedding transparency into governance routines and fostering a culture where speaking up is enabled, not penalised.

- Finally, we offer practical recommendations to distinguish between necessary confidentiality and illegitimate concealment, along with clear metrics to detect and curb strategic ignorance in multilateral settings.

Contents

Managing knowledge, enabling corruption: How information circulation shapes accountability

During the Iran–Contra affair in the 1980s, President Ronald Reagan's administration secretly sold arms to Iran and channelled the proceeds to support the Contras in Nicaragua, in violation of US law. When confronted, Reagan claimed he was unaware of the financial link between these operations, stating 'I was poorly informed.'

This calculated performance of not knowing is a striking example of what has come to be known as 'strategic ignorance': a condition, whether deliberate or systemic, where information is selectively concealed, downplayed or dismissed in ways that obstruct accountability and enable misconduct. As this paper shows, it arises from both organisational routines and conscious choices, particularly in environments where confidentiality is prioritised over transparency.

While the absence of knowledge is often perceived as a vulnerability, there can be sound organisational reasons for deliberately maintaining patterns of non-knowledge. Strategic ignorance can support organisational resilience by allowing actors to command resources and project confidence in sensitive contexts. It can also be viewed as a useful means of managing risk by evading accountability, obscuring misconduct and corruption, and consolidating power.[1] Yet these same mechanisms can obscure misconduct or shield organisations from scrutiny.

Accordingly, understanding strategic ignorance is a way to uncover strategies and techniques that can be used to hide irregularities, in particular unequal or fraudulent distribution of power and assets.

Multilateral organisations (MOs) are formal institutions established by multiple states through international agreements, operating on behalf of national governments. MOs often adopt compliance-based approaches to manage corruption risks,[2] using tools such as audits, risk assessments, and sanctions.[3] However, the

1. McGoey 2012.
2. Nicaise 2022.
3. Bowra et al. 2022.

effectiveness of these tools remains uncertain.[4] Some scholars suggest they may serve more as performative safeguards than as genuine accountability mechanisms.[5]

Furthermore, if these mechanisms do uncover irregularities, strategic ignorance may play a central role in the evasion of accountability, allowing governance bodies within multilateral organisations to overlook or dismiss inconvenient truths, thereby sustaining environments where corruption persists.

Two critical questions are: Do existing information processes deliver effectively? And if not, what reforms are needed to enhance integrity and transparency?

In this U4 Issue, we examine the concept of strategic ignorance in relation to confidentiality and the management of sensitive information within MOs. Our focus is on intergovernmental MOs, primarily UN agencies which share key governance features such as state-led executive boards, legal immunities, and confidentiality regimes. While confidentiality and trust are essential to their operations, they can also create conditions in which strategic ignorance takes root.

The analysis focuses on two emblematic cases: the Oil-for-Food scandal, which revealed how information practices enabled systemic corruption; and the more recent UNOPS scandal, where strategic ignorance facilitated large-scale financial mismanagement. We examine how strategic ignorance is produced and sustained through internal information governance, and how it affects oversight and accountability. We conclude with recommendations to mitigate its effects.

The analysis draws on a review of investigation reports, academic literature, and 15 semi-structured interviews with senior officers from MOs (notably the UN Development Programme (UNDP), the UN Population Fund (UNFPA), and UNICEF), and from donor agencies. All interviewees chose to remain anonymous.

Some of the terms used in this analysis may not be familiar to all readers. A brief glossary is provided below to clarify how we define and apply these concepts in the context of multilateral governance.

4. Hafner-Burton and Schneider 2019.
5. Bowra et al. 2022; Kohler and Bowra 2020

Key terms

Strategic ignorance

Theoretical notion describing tactics and techniques used to withhold, downplay, or filter information in ways that deflect oversight and avoid accountability. It can result from intentional choices or from entrenched routines and organisational blind spots.

Selective visibility

Deliberate practice to direct attention and ensure certain issues remain visible only to a limited group. This dynamic is shaped by discretion, power relations, and informal norms that determine who sees what, when, and under what conditions.

Information asymmetry

A situation where some stakeholders (eg donors or oversight bodies) lack access to relevant information held by others (eg senior management), limiting their ability to monitor risks, assess performance, or intervene effectively.

1 From procedure to practice: Operationalising strategic ignorance in multilateral organisations

Strategic ignorance is enacted through routine practices that govern how information is classified, restricted, and shared. In multilateral organisations (MOs), confidentiality protocols play a central role in shaping these practices. While intended to safeguard sensitive operations and build trust, confidentiality also creates discretionary spaces where information may be selectively retained, delayed, or suppressed.

Professionals working within these systems develop a procedural skillset: deciding what to disclose, to whom, and under what conditions. Over time, this discretion becomes habitual, embedded in routines and professional norms that equate limited sharing with good judgement. As a result, information flow is often minimised not through formal censorship but through informal strategies of caution and containment.

This routinised discretion does more than protect operational integrity; it can also obscure emerging risks and undermine oversight. The next sections explore how these practices contribute to a culture of selective visibility, in which information governance becomes a mechanism for strategic ignorance.

The power of information: Circulation, control, and confidentiality

The UN Oil-for-Food Programme (1995–2003) was designed to mitigate the humanitarian impact of sanctions imposed on Iraq after its 1990 invasion of Kuwait. Under the programme, Iraq was permitted to sell oil, but the proceeds were deposited into an account under UN oversight, and could be used only for purchasing essential humanitarian goods such as food and medicine.

The programme became one of the UN's largest corruption scandals,[6] with over US$1.8 billion in illicit payments, channelled through kickbacks on humanitarian

---

6. Gordon 2006.

contracts and surcharges on oil sales. High-level officials, including the programme's director, were implicated. The Iraqi government exploited the system to reward allies and influence foreign actors, highlighting how weak controls and selective disclosure allowed manipulation on a global scale.

After the fall of Saddam Hussein in 2003, records uncovered by the Coalition Provisional Authority exposed widespread corruption throughout the years of the Oil-for-Food Programme. This led to the creation of the Independent Inquiry Committee (IIC), which reviewed 10 million documents and conducted thousands of interviews, uncovering how mismanagement and strategic inaction enabled fraud across the UN system.[7]

Despite extensive evidence, accountability was limited. While some individuals faced legal action, systemic governance failures were largely unaddressed. The case illustrates key aspects of strategic ignorance, explored in Box 2.

7. IIC 2005a, p. 170.

Box 2. Strategic ignorance in the administration of the Oil-for-Food programme

Several aspects related to information circulation facilitated **financial mismanagement and political manipulation**:

- **Selective inaction and bureaucratic inefficiencies:** Oversight mechanisms were weakened by intentional delays and organisational inertia. As the IIC documented, UN officials 'failed to adequately control and supervise the activities of the Agencies, who resisted any attempts at supervision.' This lack of enforcement reflects a form of strategic inaction, where known risks were tolerated to preserve operational continuity.

- **Suppression of internal alerts:** Whistleblower reports were ignored or undermined. The IIC found that follow-up investigations were limited due to financial constraints as well as 'an inability to obtain Iraqi visas for OIOS [the UN Office of Internal Oversight Services] investigators.'[8] This undermining of internal warning systems reveals a pattern of insulation from disruptive information.

- **Selective disclosure and misinformation**: Key actors were able to disregard evidence that should have triggered intervention. This included concealing operational failures, such as the strategic distribution of oil allocations for political influence. These practices reflect strategic ignorance, whereby information was actively curated to avoid organisational accountability and to protect senior leadership from scrutiny.

- **Obfuscation of financial irregularities**: According to the IIC, 'kickbacks were disguised as "service fees" or by inflating unit prices, with payments sent to Iraqi-controlled accounts.'[9] Those inflated contracts were noticeable but went unaddressed by oversight bodies. This intentional disregard suggests strategic ignorance, where attention was purposely diverted to keep up the appearance that the programme was running smoothly.

While this example reflects large-scale corruption, it highlights systemic patterns of information management that can be present at the operational level.

---

8. IIC 2005b, p. 71.
9. IIC 2005b, p. 27.

Understanding these patterns requires moving beyond extreme cases to examine how information is governed in daily professional practice.

The circulation of information in MOs is routine and strategic. Though framed as operational necessity, it can reinforce opacity and restrict oversight. The next section explores the handling of information in practice.

How staff manage information and why it matters

In MOs, confidentiality is a professional norm that shapes how information circulates, who accesses it, and ultimately how oversight and accountability are enabled, or obstructed. This routinised handling of sensitive information creates fertile ground for strategic ignorance.

Professionals in these settings operate within well-established systems for managing information: classification protocols, restricted access, and role-based authorisations. These norms are not isolated to specific organisations; they circulate across agencies through staff mobility and professional socialisation within the multilateral system.

Our interviewees describe routine procedures such as labelling attachments, determining recipient lists, or managing log-in systems for secure files. As one officer noted:

> If it's internal, like contractual settlements or personal matters, HR [human resources] already labels it confidential. I may also receive confidential information from an external partner and classify it as such because it was shared with the clear understanding that it remains within a narrow circle of trust. *(Senior officer, multilateral organisation)*

Confidential information includes audits, legal opinions, and internal reporting. While such classifications are justified, they are rarely neutral, often shaped by discretion, culture, and perceived reputational risk, even before any formal vetting.

Importantly, the professional identity of staff is partly shaped by their ability to handle sensitive material with discretion. Several interviewees highlighted how context determines what is shareable, and with whom. For example, one officer said:

> I have to determine which information is confidential to my organisation, which one is confidential within the ministry, and which formed the shared working basis between the two. (*Senior manager, UN organisation*)

Discretion functions not only as compliance, but also as an adaptive strategy. As Weaver (2019) shows in her study of the World Bank, staff can resist transparency despite organisational reforms to encourage or mandate it, due to fears of reputational damage and weak incentives for openness. Strategic ignorance persists not only through internalised routines and discretionary practices, but also due to identifiable policy gaps. For instance, both the World Bank (2020) and the UN (2018) maintain personal data policies with vague or inconsistently applied data classification criteria, allowing broad discretion over information disclosure. As one interviewee put it:

> You don't share information with everyone who might be interested, only with those who need it to do their job. (*Senior advisor, multilateral organisation*)

While such practices ensure operational control, they also produce an organisational architecture in which visibility is asymmetrically distributed. Sensitive issues are often 'kept under the radar', not necessarily to protect individuals, but to limit exposure, avoid controversy, or manage donor relations. As a result, crucial governance information may be accessible only to a small inner circle, further entrenching power asymmetries.

This dynamic is particularly visible in donor relations, where the fear of a 'transparency penalty' influences disclosure decisions:

> UN agencies, for example, will tell us that they're frightened that there will be a transparency penalty. So if they tell us about cases [of malpractices] we will stop funding them. (*Senior officer, donor agency*)

This cost-benefit logic transforms confidentiality from a protective mechanism into a tool of control. Strategic opacity is maintained not by formal censorship but by a culture of cautious disclosure, driven by both risk aversion and organisational self-preservation.

In sum, confidentiality in MOs functions both as a procedural safeguard and a strategic practice. Its professionalisation makes it difficult to distinguish between legitimate caution and systematic information control. While rules define what may be shared, organisational culture shapes how those rules are applied. Staff learn not only when to follow protocol, but also when to stay silent. In this way, strategic ignorance is sustained through both formal structures and informal norms. This suggests that onboarding processes and integrity training should include not only formal rules but also concrete examples of discretionary boundaries.

The next section examines how this discretion becomes embedded in norms, shaping the limits of acceptable information sharing and influencing the governance of risk.

The rules, limits, and risks of information sharing

In Mos, confidentiality is more than a rule – it is a behavioural norm that disciplines how staff think, communicate, and act. While designed to protect sensitive processes, it can also constrain transparency.

Professionals in these organisations are trained to manage information with caution. Most are familiar with protocols for classifying and limiting information flows. In some settings, formal systems guide classification while in others classification is more intuitive and context-dependent:

> There's a whole process of formalising, whenever you write or produce a document, you have to classify it in your head: public, internal use, confidential, or strictly confidential. Of course, classification applies to anything related to compliance cases. Even in conceptual work, much of the data we handle, such as reported risks, is inherently confidential. (*Senior officer, multilateral organisation*)

Yet, classification is only one layer. Discretionary judgment governs everyday decisions about what to say, how to say it, and to whom. Even unclassified information is shared selectively, reinforcing a culture where caution outweighs openness.

> There's no such thing as 'normal information.' Even when it's not classified, you always consider who you share it with. You don't just spread it anywhere. (*Senior advisor, multilateral organisation*)

This cautious sharing becomes habitual. Staff internalise the principle of 'need-to-know' and avoid over-disclosure. Such practices may serve operational efficiency, but they also limit spontaneous communication, which in organisational theory is known to facilitate oversight and informal accountability. As another interviewee noted, 'there is no chit-chat', an absence that reflects the suppression of unstructured information flow.

Protective protocols can also limit *necessary* information flows. Staff may avoid copying colleagues into messages, exclude actors from meetings, or delay reporting risks unless formally required. At the same time, trust-based exceptions emerge,

close collaborators may share sensitive information informally, shaping internal risk visibility in uneven ways:

> With certain colleagues, you develop a close relationship. You trust that anything shared remains confidential. (*Senior officer, multilateral organisation*)

This results in a dual system: formal confidentiality frameworks restrict access, while informal trust networks govern disclosure. This uneven distribution of knowledge creates selective visibility, where insiders operate with far more information than others, and where governance gaps can be hidden to outsiders.

Trust as a filter: How informal norms shape knowledge sharing

Trust plays a central role in these dynamics, particularly in advisory roles where professionals must navigate political sensitivities and organisational boundaries. These exchanges are not only about discretion, they also involve informal processes that determine what gets acknowledged and what stays off the record. In complex or politically sensitive settings, informal conversations and relational cues help define what is actionable, how risks are interpreted, and which insights are better left undocumented.

While trust enables collaboration, it also defines the boundaries of what can be said or shared, effectively co-producing silences that can shield wrongdoing. The process of defining these boundaries shapes not just disclosure, but the construction of what counts as knowledge.

> Sometimes I advised partner organisations or had informal talks with government officials. They wouldn't say, 'this is off the record,' but you just knew not to spread the word. In an advisory role, trust is the foundation of your work. (*Senior advisor, multilateral organisation*)

In such environments, professionals learn to manage not only information but exposure. Minimal disclosure becomes a strategy in contexts where risk and visibility are tightly linked. For instance, even non-sensitive decisions, such as job postings, might be delayed or concealed to nurture internal relationships. These everyday decisions reveal how discretion operates not only through formal classifications but through subtle, relational practices.

> Most information gathering starts informally, through conversations, before moving to written exchanges. You can often get a better sense of things in an informal setting. (*Partnership director, national agency*)

In effect, information becomes a strategic resource, distributed according not only to organisational roles but also to networks of trust and influence. This dynamic contributes to the production of strategic ignorance, not because information is absent, but because it is asymmetrically managed, held back, or kept informal.

The next section explores how these dynamics translate into organisational structures of control and how strategic ignorance becomes embedded in governance frameworks.

2 Confidentiality and strategic ignorance as information governance

Confidentiality protocols shape how multilateral organisations handle information, balancing the protection of sensitive processes with discretion over disclosure. Yet over time, this discretion becomes routinised, embedded in professional norms that favour caution, minimal documentation, and selective circulation.

As Carson and Thompson (2019) argue, opacity is more than bureaucratic inertia; it functions as organisational power. By controlling visibility, institutions shape what counts as a problem and who is accountable. Ambiguous rules create space for discretion, and selective disclosure curates public narratives while concealing internal tensions.

The UNOPS case demonstrates how information governance can be used to maintain an illusion of control while enabling misconduct. Through its S3i (Sustainable Investments in Infrastructure and Innovation) initiative, UNOPS aimed to finance social housing. Yet by 2022, over US$60 million had been disbursed – primarily to a single contractor, SHS Holdings – without any housing units constructed. The governance failure was not only financial but informational: critical data were withheld from donors and oversight bodies.[10]

A third-party review revealed that senior leadership at UNOPS had concentrated decision-making power, bypassing oversight mechanisms and ignoring critical financial and operational risks.[11] Independent auditing firm KPMG confirmed that investment decisions were made without adequate due diligence, leaving UNOPS highly vulnerable to financial losses.[12]

The breakthrough came from whistleblower Mukesh Kapila, who exposed the misconduct publicly. Under pressure, Executive Director Grete Faremo resigned, and her deputy was dismissed. UNOPS announced governance reforms, but the episode highlighted how control over information had enabled organisational evasion rather than governance (see Box 3).

---

10. KPMG 2022a, p. 7.
11. KPMG 2022b, p. 6.
12. KPMG 2023, p.3.

Box 3: The UNOPS case: Manipulating the information system to cover wrongdoing

Deliberate weakening of oversight

Senior leadership at UNOPS actively bypassed accountability mechanisms, ensuring that internal audits and compliance units lacked the authority to challenge misconduct. The Internal Audit and Investigation Group (IAIG), which should have operated independently, reported directly to the executive director, reducing its ability to challenge misconduct.[13] Similarly, the Audit Advisory Committee (AAC) functioned as a passive advisory body without enforcement authority, further weakening internal oversight.[14]

This deliberate restructuring of oversight created a governance architecture in which ignorance of critical risks could be maintained, insulating leadership from scrutiny and allowing irregularities to continue unchallenged.

Suppression of internal warnings

Despite multiple red flags, including concerns raised by staff and a formal whistleblower complaint in 2019, UNOPS leadership ignored or silenced these warnings.[15] Fear of retaliation and distrust in the whistleblowing system further discouraged employees from coming forward.[16] Multiple red flags were ignored, including warnings about procurement irregularities and financial mismanagement.

By suppressing internal alerts and cultivating an environment in which risks could not be voiced without consequence, leadership enabled a form of strategic ignorance, where known problems were systematically unacknowledged to preserve organisational control and protect reputational interests.

Selective disclosure and information control

The AAC received selective information focused on progress updates, with little evidence that significant risks and challenges were raised for review.[17]

Similarly, senior management ensured that the executive board and donors received only fragmented or misleading information, with financial risks either downplayed or

13. KPMG 2022b, p.9.
14. KPMG 2023, p.5.
15. KPMG 2022a, p.31.
16. KPMG 2022b, p.10.
17. KPMG 2022b, p. 26.

omitted. Donors, such as the Norwegian Ministry of Foreign Affairs, were alerted but failed to act due to their reliance on incomplete information.[18]

This selective disclosure illustrates strategic ignorance in action: information was carefully curated to sustain plausible deniability, avoid donor alarm, and protect leadership from external accountability. This resulted in an asymmetry of knowledge, and this allowed oversight breakdowns to be concealed behind a facade of organisational normalcy.

For board members, the UNOPS case shows that formal oversight structures without independent reporting lines are vulnerable to manipulation. By bypassing independent checks, restricting access to critical data, and fostering a culture of fear, UNOPS leadership insulated itself from accountability, enabling large-scale financial mismanagement. To avoid similar failures, boards should regularly review who controls access to information and how dissent is handled.

More broadly, the case highlights systemic vulnerabilities within other MOs, as these vulnerabilities are not unique to UNOPS. As Baumann (2021) explains, across the UN development system, there are stark disparities in project-level transparency: while UNDP and the World Food Programme (WFP) provide detailed data on project content, funding, and performance, agencies like UNICEF and UNFPA prioritise programme-level reporting and disclose little at the project level. Others, such as UN-Habitat and the UN Environment Programme (UNEP), offer minimal or no project information. These inconsistencies reflect not technical constraints but divergent organisational incentives and the absence of a system-wide transparency standard.

The following sections will further explore these structural weaknesses, examining power asymmetries, information control, and organisational cultures that discourage speaking up.

How organisations handle and restrict information

Access to information is a defining factor in governance, shaping how decisions are made, risks are managed, and accountability is enforced. In MOs, who controls

18. Bolle 2024.

information and how it is shared, or withheld, can determine the extent to which oversight mechanisms function effectively.

As illustrated in the UNOPS case, confidentiality can serve as a tool for limiting scrutiny and consolidating power, where senior leadership control the flow of critical information, restricting access to oversight bodies and donors. One interviewee described how UNICEF, like many multilateral agencies, tightly manages internal information:

> Only the compliance office has information on cases. No one else in UNICEF can access it. The compliance office gives very limited briefings only when necessary to the functioning of the organisation to the most senior staff of the organisation. Other than that, we don't share this information. (*Senior Manager, UNICEF*)

Information control is often framed as necessary to protect confidentiality or ensure impartial investigations. Yet in practice, it can insulate senior leadership from scrutiny, especially when oversight is weak or accountability diffuse. This centralisation of discretion allows a small group of decision-makers to manage visibility with limited external challenge.

This selective knowledge management reflects a broader pattern in multilateral governance, where accountability is primarily vertical, directed towards senior leadership. However, leadership is not a neutral entity; it operates based on its own rationale and interests. Accordingly, it exercises discretion in deciding which cases to follow up, weighing multiple factors beyond strict compliance or ethical considerations.

Decisions around investigations are often shaped less by governance norms than by organisational imperatives: budget continuity, reputational protection, or the shielding of key individuals. Information management becomes a strategic calculation, determining which risks are acknowledged and which remain invisible.

Yet, when knowledge is selectively disclosed, delayed, or fragmented, it creates an environment where fraud or corruption can persist unchecked. One interviewee noted how agencies often disclose information reluctantly and in a fragmented manner, referencing the UNOPS case:

> Some agencies did not disclose when they should have disclosed, and when they did disclose, it came out in dribs and drabs. (*Middle-level manager, UN organization*)

Strategic ignorance can be produced not only by withholding information, but by timing its release to prevent scrutiny. As one official from a Danish donor organisation noted, the delay turns donors into passive observers, undermining their ability to engage meaningfully with risk mitigation:

> Some UN organisations will only inform us of actual cases following the conclusion of any investigation into irregularities... As such, we have no way of commenting or influencing the process, if this is not being handled in accordance with our expectations. (*Official from DANIDA, the Danish development cooperation agency*)

Donors often demand greater transparency, but the UN officer we interviewed cites limited capacity and reputational risk as reasons for caution. One senior official noted that investigative teams spend increasing time managing donor expectations. Moreover, unfiltered transparency can be risky, especially in cases involving whistleblowers or sensitive political dynamics. To manage this, the UN restricts disclosure until investigations are verified. But this approach has costs: delayed reporting weakens oversight, makes coordination harder, and allows governance gaps to persist.

Moreover, donor–UN relations are shaped by political sensitivities. Many donors face internal pressures and may hesitate to challenge UN partners publicly, even when disclosure is lacking. This mutual caution can entrench information asymmetries, reinforcing a system where strategic ignorance remains unchallenged.

Ultimately, the tension between transparency and controlled disclosure reflects competing institutional priorities. Donors seek timely data to manage risk, while the UN often prioritises control to protect staff or maintain independence.

The next section examines how these tensions manifest in asymmetries of information distribution – and the broader implications for risk governance in multilateral organisations.

Power asymmetries in information distribution: How unequal access to information hinders accountability

Both transparency and confidentiality contribute to information asymmetry, as the manufacture and control of information remain in the hands of certain actors. For donors, relying solely on official reports may provide a false sense of security. Requiring multi-source reporting or triangulation with field feedback can mitigate this risk.

'Overflowing information' occurs when reports or communications become overly detailed, burying key insights under excessive data. This happens when too much irrelevant or minor information is included, making it difficult for the reader to identify the main points. Reports may lack structure, prioritise data over clarity, or include unnecessary visuals, leading to confusion and disengagement. As a result, the essential message is lost, causing decision paralysis and reduced effectiveness in communication.

This challenge is particularly relevant in multilateral organisations, where donors, oversight bodies, and internal stakeholders struggle to extract meaningful insights from dense documentation. As one official observed:

> Information received is not enough to reflect field reality in multilateral organisations. UN agencies have all the structures in place to manage risks, from codes of conduct to whistleblowing processes. Yet, it is possible to circumvent those processes and act differently than what is presented on paper. (*Senior officer, Finnish Ministry of Foreign Affairs*)

This quote highlights how voluminous reporting can create an illusion of oversight while failing to capture concrete risks and internal control weaknesses, ensuring that critical gaps remain unnoticed and limiting the effectiveness of external scrutiny.

On the other side of the balance, confidentiality can be used to reinforce power hierarchies, evade accountability, or manipulate narratives. As illustrated in the UNOPS case, the concentration of information at the executive level meant that external stakeholders, including donors and oversight bodies, were dependent on what UNOPS leadership chose to disclose.

One of our interviewees is critical of the overuse of confidentiality in the multilateral sector. To them, confidentiality sometimes prevents the needed information from flowing and the risks from being openly discussed:

> Confidential information is difficult to work with and carries risks. If major reforms, such as changes to a cost recovery model, are kept within a small circle, there's a high chance of blind spots. Without broader input, critical aspects may be overlooked, leading to unforeseen issues when the reform is implemented. (*Senior advisor, country donor*)

When decisions are made within small, insulated circles, there is a greater risk that critical weaknesses remain unchallenged, oversight mechanisms are bypassed, and vested interests shape policies without scrutiny. For example, bureaucratic

procedures that classify information as confidential may be used to prevent scrutiny, limit accountability, or delay necessary interventions. In such cases, confidentiality ceases to serve its intended purpose (protecting sensitive information) and instead becomes a mechanism for opacity, keeping evidence away from external accountability.

Beyond policies: The missing 'speak-up' culture

Multilateral organisations can rely on a full ethical infrastructure, including whistleblowing policies and codes of conduct. However, organisational culture shapes what is considered 'knowable' or 'sayable'. Employees learn to stay silent in the absence of protection or organisational appetite for disclosure. This suggests that strategic ignorance can be deeply embedded in governance and decision-making structures. It influences not only what information is shared but also the things employees feel they can or cannot speak about.

The challenge of speaking up is grounded in the conditions for dialogue and communication. According to Hunt-Matthes and Gallo (2017), the UN Ethics Office rejected 96% of applications for whistleblower protection between 2006 and 2016. As highlighted in the BBC documentary *Whistleblowers: Inside the UN*, those who report irregularities often face harsh consequences, including retaliation and reputational damage.[19] Whistleblowers are frequently portrayed as traitors, and for women, the risks are even greater due to limited organisational support.

According to Stoyanova,[20] 'there are elements of the UN system's internal culture that contribute to the UN's apathy in protecting whistleblowers', including a lack of accountability from leadership, an absence of incentives to reward ethical decisions, and a pervasive fear of retaliation.[21] In addition, precarious employment conditions further discourage reporting. As of December 2022, non-staff personnel constituted approximately 43% of the total UN system workforce, reaching as high as 91% at UNOPS. Short-term contracts and job insecurity create disincentives for personnel to challenge authority, reinforcing a culture of silence.

Decision-making within the UN Secretariat ultimately lies in the hands of permanent representatives from member states. However, many delegates are deeply embedded in diplomatic networks and attuned to their own international career trajectories. Their incentives often prioritise maintaining the UN's image over addressing governance weaknesses.[22]

19. British Broadcasting Corporation. 2022. The whistleblowers: Inside the UN.
20. 2024.
21. Stoyanova, 2024.
22. Baturo and Gray 2021.

This may explain the reluctance of executive boards to act when presented with red flags, as seen in the UNOPS case. While the example here concerns the UN, similar dynamics can be found in other intergovernmental organisations, where reputational concerns and career incentives influence institutional responses.

The next section offers recommendations on how information governance and related practices can be structured to foster transparency rather than opacity.

Turning insight into reform: Recognising and reducing strategic ignorance

Strategic ignorance is not a symptom of failure, it is a consequence of how information is governed. It emerges where discretion, power asymmetries, and professional norms interact, shaping what remains unseen.
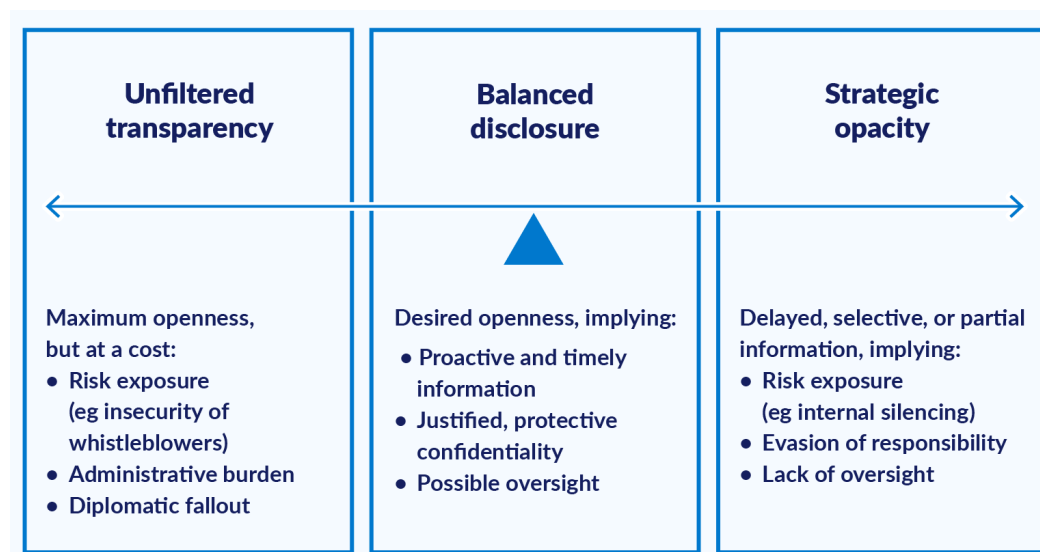
Having examined how strategic ignorance operates through information practices and organisational culture, we can now turn to practical recommendations. The following sections offer concrete strategies to address this challenge, giving insights to recognise strategic ignorance, strengthen oversight, and increase disclosure.

How to recognise strategic ignorance within an organisation

Confidentiality remains vital in protecting sensitive negotiations, safeguarding personnel, and upholding diplomatic discretion. But when misused, it can facilitate opacity, suppress accountability, and conceal misconduct. Likewise, transparency must not be confused with data overload or symbolic disclosure, both of which can obscure more than they reveal.

To illustrate both extremes and the expected middle point for disclosure, the illustration below maps the continuum between unfiltered transparency and strategic opacity. A balanced disclosure implies not just timely information-sharing but also structured transparency that protects sensitive sources while enabling oversight. For instance, according to an interview with a UNICEF staff member, a disclosure model combining semi-annual summaries with alerts for high-risk cases has been developed to balance confidentiality with donor oversight needs.

Figure 1: The information circulation spectrum in multilateral organisations. Strategic opacity emerges when discretion becomes a tool of evasion rather than protection.

Unfiltered transparency	Balanced disclosure	Strategic opacity
Maximum openness, but at a cost: • Risk exposure (eg insecurity of whistleblowers) • Administrative burden • Diplomatic fallout	Desired openness, implying: • Proactive and timely information • Justified, protective confidentiality • Possible oversight	Delayed, selective, or partial information, implying: • Risk exposure (eg internal silencing) • Evasion of responsibility • Lack of oversight

Strategic opacity emerges when discretion becomes a tool of evasion rather than protection. At one end is unfiltered transparency, which prioritises openness but carries risks. In the middle is balanced disclosure, aiming for justified openness with oversight. At the other end is strategic opacity, where information is selectively or partially shared, often limiting accountability.

This continuum reflects how information circulation operates, not only through deliberate choices, but also through structural constraints and informal norms that shape control and limit scrutiny. For compliance teams, understanding these informal norms is critical. Risk information may not flow through formal channels; audit procedures should be designed to capture off-the-record dynamics.

The following questions can help determine when discretion has shifted from protective caution to evasive silence:

External visibility

▪ Are donors and external auditors granted access to full investigation reports or financial reviews?

▪ How often are joint monitoring missions or site visits conducted?

Disclosure patterns

▪ Is there a formal process to justify delays or non-disclosure of governance risks?

▪ Do decision records show changes in language, risk emphasis, or omissions between internal and external versions?

Board-level engagement

- Are integrity risks meaningfully and regularly discussed in executive board meetings?

- Is there a mechanism to flag and analyse delays in risk disclosure or gaps in information sharing?

Recognising strategic ignorance is the first step. But awareness alone is insufficient. Organisations must act decisively to reinforce oversight mechanisms that resist information capture and institutional silence.

Strengthening oversight and preventing selective information control

Organisational autonomy plays a critical role in the effectiveness of oversight bodies. Internal audit and investigative units perform best when structurally independent from executive leadership, thereby minimising conflicts of interest. At UNOPS, the Internal Audit and Investigation Group (IAIG) reported directly to the executive director, significantly limiting its capacity to investigate misconduct independently. Genuine autonomy requires that internal audit and compliance functions report to independent governance bodies, such as executive boards or audit committees with enforcement powers.

Standard practice can include third-party audits and regular independent evaluations. As evidenced in the UNOPS case, internal reporting processes are vulnerable to manipulation or suppression. The full extent of the case was only uncovered after KPMG's external review, demonstrating the importance of an autonomous, external layer of scrutiny. Independent audits reduce the risk of selective disclosure and enhance credibility in oversight mechanisms.

To pre-empt the emergence of strategic ignorance, oversight systems can monitor early indicators of information control and organizational opacity. These can include:

- Transparency on whistleblower complaints and related follow-up

- Staff survey on the level of trust and integrity in the leadership

- Reporting line of internal audit and investigations

Establishing regular reviews of these indicators would allow oversight bodies to intervene before strategic ignorance becomes institutionalised.

Enabling disclosure through better governance and integrity culture

Strategic ignorance is sustained not only by organisational design but by workplace norms and informal practices.Information is often shared cautiously or informally, shaped by fear of reputational harm, retaliation, or diplomatic fallout. Organisations must therefore build formal and informal systems that normalise disclosure.

A constructive practice would be for multilateral organisations to provide regular, structured updates on governance risks and misconduct cases directly to donors' country offices, even before investigations are finalised. This proactive communication would help build trust, demonstrate a commitment to transparency, and support timely, coordinated responses. Metrics such as the frequency of shared risk assessments and donor satisfaction with the quality of disclosure could be used to monitor performance.

Yet even the best-designed systems fail when silence is rewarded and speaking up is unsafe. Organisational culture determines whether staff trust internal processes and whether risk information circulates freely. Staff surveys and culture diagnostics can help identify barriers to disclosure and highlight where silence is institutionalised. For example:

- Annual staff surveys on willingness to report misconduct and fear of retaliation

- Staff perception of whether misconduct is tolerated when committed by senior personnel

- Gender-disaggregated reporting data, enabling the development of context-specific integrity frameworks

A values-based approach can also complement compliance mechanisms in mitigating corruption risks.[23] In particular, indicators related to employee well-being and job satisfaction can contribute to corruption risk assessments, linking workplace well-being and a safe reporting environment to the development of a stronger integrity culture.

To reduce the incentive to ignore inconvenient information, organisations can normalise disclosure by integrating risk reflection into programme reviews, creating safe spaces for staff to raise concerns, and using internal learning formats to highlight constructive handling of sensitive issues. Rather than sanctioning silence

---

23. Nicaise 2022.

through performance metrics, these softer mechanisms foster a culture in which raising problems is seen as part of good professional judgement.

Finally, robust whistleblower protection is essential.[24] This includes anonymous reporting, safeguards against retaliation, and transparent follow-up. Without such systems, concealment becomes the safer option, and strategic ignorance prevails.

---

24. Nicaise and Worth 2024.

References

Baturo A. and Gray J., 2021. Delegating diplomacy: Rhetoric across agents in the United Nations General Assembly. International Review of Administrative Sciences 87(4): 718– 736.

Baumann, M. O. 2021. The case for greater project-level transparency of the UN's development work. Briefing Paper 5/2021. German Institute of Development and Sustainability (IDOS).

Bolle, T. A., 2024. UD ble advart om høy risiko i FN-organisasjon – unnlot å gripe inn [The Ministry of Foreign Affairs was warned of high risk in the UN organisation – failed to intervene] Panorama Nyheter, 6 December.

Bowra, A., Saeed, G., Gorodensky, A., and Kohler, J. C. 2022. An exploration of anti-corruption and health in international organizations. Plos One 17(8): e0269203.

Carson A. and Thompson A. 2019.The power in opacity: rethinking information in international organizations. In International organisations and power politics: Bridging the divide, eds Anders Wivel and T. V. Paul, 123–144. Georgetown University Press.

Gordon, J. 2006. The accusations against the oil for food program: the Volcker reports. Arab Studies Quarterly, 28(3/4), 19–26.

Hafner-Burton, E. M. and Schneider, C. J. 2019. The dark side of cooperation: International organizations and member corruption. International Studies Quarterly 63(4): 1108–1121.

Hunt-Matthes, C. and Gallo, P. A. 2017. The UN whistleblowing protection gap: Implications for governance, human rights and risk management. In Selected papers from the International Whistleblowing Research Network conference, eds D. Lewis and W. Vandekerckhove. Oslo, June 2017.

IIC. 2005a.Report of investigation. Vol IV, part II ofThe management of the United Nations Oil-For-Food Programme. The Independent Inquiry Committee into the United Nations Oil-For-Food Programme, 7 September.

IIC. 2005b.Manipulation of the Oil-For-Food Programme by the Iraqi regime. The Independent Inquiry Committee into the United Nations Oil-For-Food Programme, 27 October.

KPMG, 2022a. Third-party review of effectiveness of the UNOPS oversight mechanisms for S3i.

KPMG, 2022b. Third-party review of the internal control systems, risk management and overall governance structures of the United Nations Office for Project Services.

KPMG, 2023. Follow-up of the 2022 Independent Reviews

Kohler, J. C. and Bowra, A. 2020. Exploring anti-corruption, transparency, and accountability in the world Health organization, the United Nations development programme, the world bank group, and the global fund to fight AIDS, tuberculosis and malaria. Globalization and Health 16: 1–10.

McGoey, L. 2012. The logic of strategic ignorance. British Journal of Sociology 63(3): 533–576.

Nicaise, G. 2022. Strengthening the ethics framework within aid organisations. Good practices from the compliance approach and the values-based approach.U4 Issue 2022:8. U4 Anti-Corruption Resource Centre, Chr. Michelsen Institute.

Nicaise, G. and Worth, M. 2024. Whistleblowing in aid organisations: Successful approaches for reporting and protection. U4 Issue 2024:2. U4 Anti-Corruption Resource Centre, Chr. Michelsen Institute.

Seyoum, T. A. and Goisemang, G. 2023. Review of the use of non-staff personnel and related contractual modalities in the United Nations system organizations. Report of the Joint Inspection Unit.

Stoyanova, D. 2024. Whistleblowers of the United Nations. PhD diss., University of Helsinki.

UN. 2018. Personal data protection and privacy principles. High-Level Committee on Management (HLCM), 11 October 2018.

Weaver, C. E. 2019. Open data for development: The World Bank, aid transparency, and the good governance of international financial organisations. In The Asian Infrastructure Investment Bank: China as a Global Actor, 129–153. Brill.

World Bank. 2020. World Bank Group Policy: Personal data privacy. Cat. No. SEC4.05-POL.103, 20 May.

About the authors

Guillaume Nicaise

Guillaume Nicaise is a senior adviser at the U4 Anti-Corruption Resource Centre, Chr. Michelsen Institute. He leads the work on integrity management, organisational integrity, and the private sector. Dr. Nicaise is an anthropologist specialising in norms transfer and implementation, with a focus on good governance mechanisms such as transparency, accountability, and civil participation.

Mahaut Fanchini

Mahaut Fanchini is assistant professor at the University of Paris-Est Créteil. Her research focus is on organisation studies, especially on whistleblowing, strategic ignorance, and the circulation of information in contemporary organisations.

Keywords

strategic ignorance – multilateral organisation – information systems – information circulation – UNOPS – Oil-for-Food Programme – governance

How to cite

Corruption erodes sustainable and inclusive development. It is both a political and technical challenge. The U4 Anti-Corruption Resource Centre (U4) works to understand and counter corruption worldwide.

U4 is part of the Chr. Michelsen Institute (CMI), an independent development research institute in Norway.

U4 ANTI-CORRUPTION
RESOURCE CENTRE