Ministerial Advisory Group on
Transnational, Serious and Organised Crime

JULY REPORT

6 August 2025 TSOC-MAG 25/05

Hon. Casey Costello, Minister of Customs and Associate Minister of Police

INFORMATION SHARING

Executive summary

- The organised crime threat is evolving rapidly. Organised crime groups operate across borders at the pace of digital technology. They are taking advantage of current gaps (both real and perceived) in our ability to share information effectively.
- We need to even things up. We need to have a mature conversation about our privacy settings as an enabler rather than a barrier. The time for bold, system-wide transformation is now.
- This does not mean compromising privacy safeguards—but it does mean creating space to prevent the daily harms caused by organised crime in ways that are safe, ethical, and proportionate.
- We recommend taking urgent action to strengthen the capacity of the system to enhance early detection, enable proactive disruption, foster coordinated responses and build long-term resilience against organised crime.
- We have found:
    - Fragmentation across agencies and inconsistent application of tools such as the information privacy principles, Approved Information Sharing Agreements, and Memorandums of Understanding between agencies.
    - Limited proactive sharing, especially in prevention and early detection of organised crime.
    - Insufficient engagement with the private sector, despite its potential as a strategic partner.
    - Gaps in transnational information sharing, particularly with Pacific neighbours.
    - Technological limitations, including lack of a unified data platform and standardised case management tools.
- To address these challenges, we recommend development of a National Information Sharing Framework to standardise processes, clarify application of legal tools and embed a culture of proactive sharing.

- This Framework should be supported by a national information sharing platform, in the form of a data lake, which will enable effective and transparent access to and use of information.
- It is also critical to mobilise the private sector as a key partner in the response to organised crime through formalised public-private partnerships and legislative tools to incentivise joint action.
- We need to improve international information sharing, especially with the Pacific, building on examples such as the New Zealand Transnational Crime Unit (NZTCU).
- Finally, we need to ensure the system is positioned for the future by:
  - Ensuring there is a clear legal framework in place.
  - Setting clear accountabilities.
  - Investing in future technologies.

Steve Symon
Chair, Ministerial Advisory Group

The response to organised crime relies on effective data and information sharing

1. In our March report we identified information sharing as one of the critical problems inhibiting an effective, unified response to transnational serious organised crime.

2. Organised crime networks operate with high levels of sophistication, exploiting legal business structures, global logistics chains, digital technologies and community vulnerabilities. As we have said before - organised crime can move at the speed of digital technology, but enforcement agencies can only move at the speed of the law. We need to be able to respond effectively and efficiently by ensuring that the right information is shared with the right enforcement agencies so they have the fullest picture possible - to investigate organised crime.

3. In the past, information sharing has focused on person-to-person exchanges, but we are increasingly moving towards the sharing of data which enables analysis, modelling and further processing to detect patterns of offending. While data sharing provides the foundational material, information sharing adds meaning and relevance, making it more useful for operational or strategic purposes.

4. Data sharing can enhance the law enforcement responses. We recognise that it must be managed carefully to ensure protection of individual privacy rights.

5. Information sharing can be done well within the current settings. An example, set out in the table below, is the New Zealand Transnational Crime Unit (NZTCU). But this is unfortunately the exception rather than the norm.

New Zealand Transnational Crime Unit – Targeting deportees to the Pacific

The NZTCU is part of a multi-agency partnership between the Police, Customs, MBIE (Immigration), and Corrections. They share investigative and intelligence capability to combat transnational crime in the Pacific.

The NZTCU shares information with Pacific Island authorities about criminal deportees being relocated from New Zealand. This allows those countries to prepare for their arrival and provide support for reintegration.

It also means that authorities are able to monitor the activities of these deportees to check if they are establishing new criminal networks, based on their connections to organised crime groups in New Zealand and beyond.

6. But we have heard repeatedly that the resulting constraints on information sharing are the most common problem encountered by government agencies in responding to organised crime.

7. While it has some strengths, New Zealand’s current information-sharing approach is insufficiently integrated to respond to the increasing threat of organised crime. Our systems within government are fragmented. Information is held in silos. There is limited co-ordination between law enforcement and other agencies. Inconsistent legal interpretations and a lack of modern technological capacity inhibit our response.

Critically, there are significant gaps in real time information flow. We are not keeping pace with the rapidly evolving world of organised crime.

8. The public reasonably expects government agencies to use information that it has collected to lawfully target organised crime, both domestically and transnationally. That requires the information to be proactively shared. That is not happening. There is a lack of understanding amongst agencies about how information that they hold might help other agencies to combat organised crime, and about the legal mechanisms available to share information. There also appears to be a deeply rooted culture of a risk-averse approach toward proactive sharing of information.

9. This problem flows into the public private sector relationship. The private sector, which holds a wealth of useful information, should be a key partner in the fight against organised crime. Many businesses want to help. But if government agencies are unable to share information consistently and proactively, it is unrealistic to expect that information sharing occurs effectively between the public and private sectors.

Financial Crime Prevention Network (FCPN)

The FCPN is a partnership between public and private entities to enhance information sharing and ultimately facilitate informed decision-making and a swift response to financial crime activities within New Zealand.

Members include Police (chair), Customs, MBIE (Immigration), Inland Revenue and major banks such as ANZ, ASB, BNZ, Kiwibank, TSB and Westpac.

The FCPN Operations Board meets every month to discuss current financial crime trends. This forum is used to share operational priorities in order to develop intelligence that draws upon the knowledge base of all its members. In addition, joint strategic products are developed to provide guidance for members and other financial institutions.[1]

10. We said in March that a significant transformation is necessary, and it is time for a mature conversation about our privacy settings as an enabler, rather than a barrier. We need to work together. Vital intelligence on organised crime needs to be identified and exchanged amongst government entities, and between government and key private sector partners such as banks, ports and airports. This needs to start occurring in a proactive, rather than reactive, way.

11. A cohesive transnational, serious and organised crime (TSOC) information-sharing framework integrating government, private sector and community stakeholders, accompanied by a well-designed standardised information sharing platform (in the form of a data lake) will improve both the operational effectiveness and enduring strategic resilience of our country to the threat of organised crime.

[1] NZ Police (2025) Financial Crime Prevention Network (FCPN) | New Zealand Police. See also: FCPN (2024) Threat assessment: Transnational Organised Crime Financial Sector Vulnerabilities.

ORGANISED CRIME THRIVES IN THE GAPS

12. The problem of a lack of effective, proactive information sharing amongst agencies is not new: it is a problem that has inhibited both government and the public/private sector relationship for many years. Nor are we the only country facing these types of barriers.

13. The reason for the siloed approach and the culture of aversion to proactive information sharing has been repeatedly cited to us as the Privacy Act. The Privacy Act is designed to ensure protection of an individual's right to privacy, but that is not all that it was intended to do. Its primary purpose is:

> *To promote and protect individual privacy by providing a framework for protecting an individual's right to privacy of personal information, including the right of an individual to access their personal information,* ***while recognising that other rights and interests may at times also need to be taken into account.***[2]

14. That is, the Privacy Act was designed not only to protect privacy, but also to legislate how agencies can share information safely.

15. The sentence in bold above is embedded within the core Information Privacy Principles under in section 22 of the Privacy Act. The principles governing disclosure (i.e. sharing) of personal information are set out in Information Privacy Principle 11 (**IPP11**). This states that an agency that holds personal information must not share the information unless the agency that holds the information believes on reasonable grounds that sharing of the information is necessary to avoid prejudice to maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution, and punishment of offences. This is a limitation in relation to targeting organised crime, as it is the requesting agency rather than the holding agency that knows why the information is necessary, but the onus is on the holding agency to satisfy itself of the need for the information to be shared. We return to this below.

16. The clear exception is that sharing of information for law enforcement purposes is not confined to sharing information reactively to crime that has occurred. Provided there are reasonable grounds for a belief that sharing is necessary for law enforcement purposes, information can and should be proactively shared in relation to organised crime. This is not happening at the moment. It needs to, if we are serious about preventing the harms that flow from organised crime.

17. Unlike comparable legislation overseas, the Privacy Act is not consent-driven. It is purpose and content driven. That is, purpose out-trumps consent.[3] It enables sharing of information without consent, where the legislative criteria for doing so are met: i.e. there is a strong compelling purpose for doing so.

18. An individual's right to privacy of personal information must be protected. But this should not inhibit sharing of information to proactively target and prevent the harms that arise from organised crime. We need to achieve this while still protecting national security and trust and confidence. It can be done. But change is required.

---

[2] Section 3 of the Privacy Act 1993.
[3] Meeting with Privacy Commissioner Michael Webster on 16 April 2025.

19. The culture of fear about proactive sharing of information appears to have arisen, at least in part, from instances of criticism levelled at government agencies for data privacy breaches. For example, in 2019 the Office of the Privacy Commissioner released findings following an enquiry that the Ministry of Social Development had systematically misused its investigatory powers while pursuing benefit fraud, unjustifiably intruding on the privacy of many persons.[4] In 2022, the Privacy Commissioner criticised the Data and Statistics Bill for overriding restrictions in the information privacy principles in the Privacy Act. These examples involved systems failures. We do not understand why they have created the evident culture of fear around sharing of information.

20. The mindset seems to be: if I share information, I might get into trouble; if I do not share information, I won't. So the seemingly obvious choice (and the advice that is often given to organisations by their advisors, including legal advisors) is to not share. To take the safe approach.

"Nine times out of ten, it's organisational culture or systems issues that stop effective and needed information sharing from taking place, not the law."

"We won't ever achieve important objectives and outcomes that rely on effective and lawful information sharing until we start asking "what's possible?", rather than deciding it's all too hard, and giving up."

Privacy Commissioner Michael Webster

---

21. Even when proactive information sharing is done well, it seems to be seasonal. People who come and go at agencies steer the culture – some are more proactive than others. But the approach should not depend solely on the personnel involved or the relationships that they have individually built. It should be consistent and deeply embedded within organisations.

22. We recognise that appropriate protection of personal information is a cornerstone of a free and democratic society. But it is not clear to us why these instances have led to the extreme level of risk aversion that has pervaded government and the private sector in the ways described above. In our view, significant course correction is needed.

23. That view is shared by Privacy Commissioner Michael Webster:

[4] Privacy Commissioner (16 May 2019) MSD fraud investigations "intrusive, excessive and inconsistent with legal requirements" - Privacy Commissioner

"We need to reframe how privacy is discussed in New Zealand, moving away from the false narrative that privacy must be sacrificed for goals like public safety, law enforcement, or innovation. Instead, we should aim for policies that recognise privacy can coexist with technological progress and effective public service delivery."

Privacy Commissioner Michael Webster

24. In our May report, we discussed the challenges created by organised crime in the Pacific. We said in that report that New Zealand has not only a moral obligation to assist its Pacific neighbours, but also a very practical reason to do so, as the Pacific is the front door for the physical trade in illegal goods in New Zealand. We need to think of our border as starting overseas, and prevention methods need to start there. Timely and targeted sharing of information with our Pacific neighbours is one of the key components to providing assistance and protecting our borders.

25. With those things in mind, our recommendations in this report are designed to:

    a. improve information-sharing frameworks and culture across government to ensure agencies have access to and are proactively sharing relevant and accurate information in a timely way;

    b. position the private sector, particularly in high-risk industries, as trusted partners in a co-ordinated information sharing strategy to detect and disrupt organised crime;

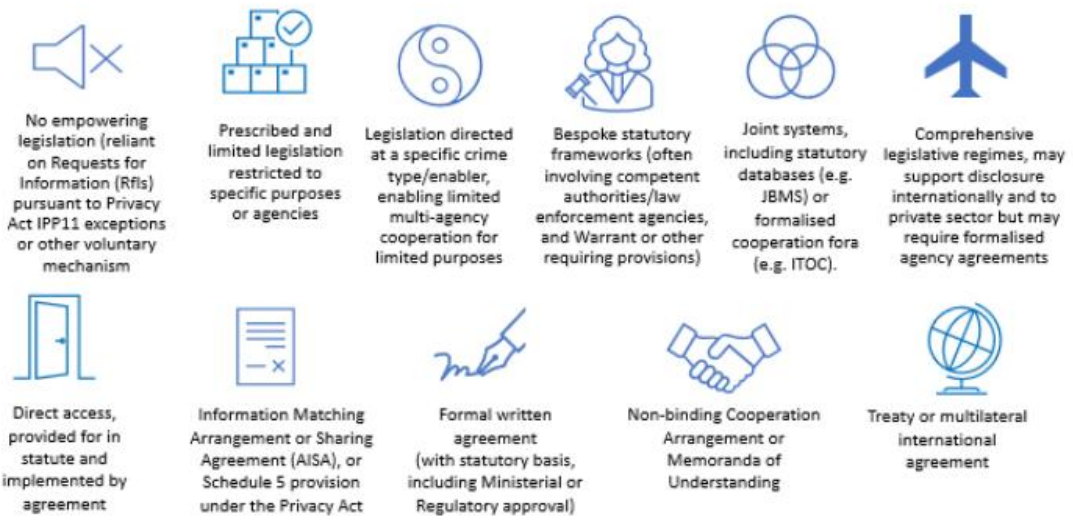
    c. develop transnational information sharing to protect our borders by preventing organised crime before it even arrives in New Zealand; and

    d. invest in technology and innovation to build future resilience and maintain an intelligence edge over increasingly adaptive organised crime networks.

ORGANISED CRIME IS ORGANISED. WE ARE NOT.

26. There are a range of information sharing frameworks in place across the TSOC system, outlined in the diagram below. These frameworks take various forms and are often supported by non-statutory mechanisms.

Figure 1: The variety of agency legal frameworks enabling information sharing across the TSOC system



27. In many cases, bespoke statutory frameworks are in place that allow the collection, use and disclosure of information for defined purposes that go beyond what the Privacy Act enables, including for example, sharing with international partners.[5] It is vital to recognise the important roles that these tools play within the wider information sharing system – and to have confidence that these are also being used to their full potential.

28. In addition to the legislative tools specific to individual agencies, three general tools are relevant to combatting organised crime:

    a. **IPP11.** This enables sharing of information where the holder of the information believes that it is necessary to share to avoid prejudice to the maintenance of the law by any public sector agency, including prejudice to the prevention, detection, investigation, prosecution and punishment of offences.

    b. **Approved Information Sharing Agreements (AISAs)**. An AISA is a legal mechanism that authorises the sharing of information between or within agencies for the purpose of delivering public services. AISAs as a legislative mechanism were introduced via a 2013 amendment to the Privacy Act. This amendment was intended to create a streamlined legal framework, without the need for a full legislative amendment, to share personal information in a controlled and transparent way to improve public service efficiency and effectiveness.[6]

    c. **Memoranda of Understanding (MOUs)**. A memorandum of understanding is a formal, non-binding mutual agreement between two or more parties that outlines the terms and details of an understanding reached between the parties. They do not create a legal entitlement to share information, but are used to clarify things such as the approach that will be taken to sharing information between two agencies.

29. However, while each of these tools has an important role, there are significant challenges with building an effective and functioning information sharing mechanism.

IPP11

30. IPP11 is used almost exclusively in a reactive rather than proactive way. It is rarely used for prevention or detection purposes, usually being used to obtain or verify information that is already known to exist. It is also interpreted and applied inconsistently within agencies and between agencies and the private sector. We are concerned that it is often used not only as a reason for not sharing, but as an excuse to avoid sharing.

31. There seems to be a lack of understanding within agencies about how information that they hold might be useful to another agency in performing its function in relation to detecting or disrupting organised crime.

32. As noted above, it can be problematic that it is the requestor of the information who knows of the relevance of that information, yet IPP11(1)(e) places the onus on the

[5] MPI (2023) TNOC-related information sharing barriers, opportunities, and proposed solutions - Paper 2: Barriers and Opportunities Analysis, p. 16.
[6] Ministry of Justice (2011) Regulatory Impact Statement: Information sharing amendments to the Privacy Act 1993.

holder of the information to be satisfied that the statutory criteria are met before the information can be shared. We recommend considering an amendment to this specific information privacy principle to reverse this onus in relation to requests by agencies for information in the organised crime space. That is, the amendment would shift the requirement for a belief on reasonable grounds onto the requestor rather than the holder of information.[7] This would simplify the process, ensure that the relevant belief is held by a person who holds sufficient information to make that belief properly informed and it would transfer the privacy risk from the provider to the requestor (usually an enforcement agency), providing assurance to providers that they will not be criticised for sharing information.[8] It could be done, for example, by an amendment to IPP11(e), the introduction of a new subsection or through the use of an AISA.[9] An amendment such as this would be required to implement the data lake discussed further below.

33. In a foreword to the March 2015 "A to Z" guide to AISAs, then Privacy Commissioner John Edwards said:[10]

> *The Privacy Act is, at its core, a flexible and enabling piece of legislation. However sometimes it has been perceived as getting in the way of agencies working together. Sometimes those perceptions have been true, particularly when personal information gathered for a narrowly defined purpose is to be used in a new way, by more agencies, as part of a proposed service delivery innovation.*
>
> *The AISA mechanism was proposed by the Law Commission, and enacted by Parliament in February 2013 to provide an answer to the "Because of the Privacy Act" objection to innovation in service delivery.*

34. The fact that 10 years on from this comment, the "Because of the Privacy Act" objection remains acute and unresolved illustrates that bold change is required.

AISAs

35. Development of AISAs, in practice, take considerable time, resource and investment. There are mixed views on whether AISAs are even effective in relation to organised crime – some agencies that we spoke to expressed concern about the utility of the current AISAs to support detection, deterrence, and dismantling of TNOC activities.[11] AISAs also tend to be relatively rigid, without flexibility to adapt to evolving situations. It is evident from our discussions with agencies that in the decade since being introduced, AISAs have not resolved the "Because of the Privacy Act" objection cited by the Privacy Commissioner in the extract above. Simplifying the development process, building in greater accountability, and including a planned review process would sharpen the AISA tool. But that will not fix the problems relating to organisational culture.

---

[7] For an example of legislation where the onus can rest with the requestor rather than the holder of the information, see the Tax Administration Act 1994, Schedule 7, clause 36.
[8] This may also provide potential witnesses who share information with a degree of comfort that they will not be subject to retribution for sharing information.
[9] Work will be required to determine the exact parameters of this proposed amendment.
[10] Privacy Commissioner (2015) A to Z of Approved Information Sharing Agreements (AISAs).
[11] MPI (2023) TNOC-related information sharing barriers, opportunities, and proposed solutions, p. 9.

MOUs

36. MOUs can be useful for clarifying the operational process for sharing information, but an MOU cannot create a legal right or obligation to share information. MOUs are therefore not of themselves a solution to the information sharing gaps. In any event, overreliance on MOUs would result in inconsistencies in interpretation and application across agencies, agreements that become out of date or are not fit for purpose and duplication of effort.

37. We have also encountered issues with conflicting legislative provisions. For example, there is a practical conflict between section 18 of the Tax Administration Act 1994 and section 98 of the Criminal Proceeds (Recovery) Act 2009. Section 98(2)(b) of the Criminal Proceeds Recovery Act provides that no secrecy restrictions imposed by any other enactment prevents Inland Revenue (IR) from disclosing information to the Commissioner of Police for the "purpose of establishing whether a prima facie case exists for taking civil recovery action under this Act". This is intended to override the confidentiality provisions in s 18 of the Tax Administration Act. However, in practice it does so only until a prima facie case has been established, at which point section 98 of the Criminal Proceeds (Recovery) Act ceases to apply, illogically preventing the Commissioner from sharing information that would support the actual case (as opposed to establishing a prima facie case). The effect of this conflict is that the Commissioner of Police is hindered in attempts to obtain highly relevant information from IR to fulfil his statutory functions.

38. The application of these frameworks has tended to constrain the ability to share information effectively, because they have been built around a limited set of datasets or functions, rather than authorising wider sharing of information for a common purpose.[12] However, there is scope to explicitly design AISAs to allow for sharing for a common public interest purpose – across both public and private sector agencies.

Other examples

Financial Crime Prevention Network

39. The Financial Crime Prevention Network, outlined on page 4, is a good example of effective information sharing to target organised financial crime. This network facilitates collaboration between public and private entities to enhance information sharing that will combat organised crime groups from operating in New Zealand. It is exactly the type of information sharing that should be occurring to target organised crime. But to be effectively utilised to target all types of organised crime, it needs a national strategy to inform clarity and consistency.

Inland Revenue holds substantial tax information

40. Another example is the collaboration between the Serious Fraud Office (SFO), IR and the NZ Police Financial Intelligence Unit (FIU), with the establishment of a dedicated detection and intelligence unit. Information sharing between IR, Police, Customs, and

[12] There are some exceptions. For example, the Joint Border Management System (JBMS) enables shared access to **border information** gathered by both Customs and the Ministry of Primary Industries.

the SFO is conducted through an AISA agreed in 2020 specifically for the purposes of prevention, detection, investigation or providing evidence of serious crime.[13] IR has however told us that it recognises the approach it has traditionally taken to information sharing may have been too conservative, and there is scope to be more pragmatic.[14] This mirrors feedback we received from a number of other government agencies. We are told that IR has engaged in constructive dialogue with Customs, Police and the SFO and their reactive approach has improved, but there is room for improvement in their proactive approach to information sharing. Again, we emphasise that there should be a national plan: these types of information sharing arrangements should occur at a national level, guided by clear strategy, rather than bespoke efforts by agencies. There also needs to be oversight to ensure accountability (discussed further below).

Strengthening information sharing with supply chain partners

41. Under current settings, there is no clear and transparent framework that authorises the sharing of sensitive information with private sector partners. For example, in the border security space, there is no clear and transparent framework that enables the two-way sharing of sensitive information between Customs and private sector partners such as operators of Customs Controlled Areas and other supply chain partners.[15] This is essential to build a shared understanding of risks to the integrity of the supply chain. Without a clear legal framework, operators (especially those based offshore) may be reluctant to share where there is a risk of conflict with the laws of the other jurisdiction and/or the information may lead to prejudicial outcomes such as prosecution or an increased level of inspection. Similarly, Customs may want to minimise the risk of a privacy breach due to organisational or reputational harm. We understand that this issue is to be considered as part of the upcoming Customs and Excise (Border Security) Amendment Bill.

Progress under the TNOC Strategy

42. Since the inception of the TNOC Strategy, addressing the barriers imposed by information sharing have been a feature of successive TNOC action plans. For example, MPI led a multi-year strategic review to identify and address barriers to information sharing. Commenting on the need for timely, effective information sharing, and the systemic nature of the barriers to information sharing, they recommended a system-wide approach to information sharing practices, identifying the situation as a threat to national security (p. 3). The key actions in response to this work have been to build a shared toolkit to facilitate effective sharing based on consistent definitions.

43. Agencies have recently reviewed the operation of the two AISAs in the TSOC space[16] to determine their suitability for broader application for preventing and combating organised crime. The conclusion of this review, which we endorse, is that more work is

[13] The *Additional Information* section includes similar details for MSD and DIA, which mainly relate to student loan debt and child support debt. IR appears to engage in more proactive information sharing with these agencies compared to Customs, Police and SFO.
[14] Meeting notes, MAG meeting with IR officials, March 2025
[15] Section 317 of the Customs and Excise Act 2018 provides for information disclosures with the private sector – but it does not allow for two-way sharing, nor disclosures with offshore organisations.
[16] New Zealand Gang Intelligence Centre Approved Information Sharing Agreement and Serious Crime AISA between IR, Police, Customs and SFO.

needed to consider the optimum legislation to support relevant information sharing, and the extent to which the law and our systems enables both law enforcement action and prevention of organised crime, including for lesser-known crime types and enablers.

FROM FRAGMENTED TO UNIFIED: A NATIONAL RESET

44. We are operating in an increasingly volatile environment, where the threat from organised crime is rapidly evolving. These groups are highly skilled at leveraging technology against us, and we must strengthen our ability to respond. This does not mean compromising the safeguards that protect privacy rights—but it does mean creating space to prevent the daily harms caused by organised crime, in ways that are safe, ethical, and proportionate.

45. To fix the problems that are prevalent within the system, we need to:

    a. standardise the processes

    b. change the culture

    c. ensure accountability

    d. mobilise the private sector

    e. improve transnational information sharing

    f. future proof the solutions.

46. Implementing the recommendations set out below will achieve the following outcomes:

    a. **Improved detection**: Early detection of organised crime will become possible through integrated insights and awareness and increased visibility across agencies.

    b. **Proactive disruption**: Faster access to patterns, actors and behaviours that can be discerned from the data and other information will enable targeted and pre-emptive enforcement and disruption activity.

    c. **Co-ordinated responses**: Shared situational awareness will support joint operational responses.

    d. **Increased trust**: Public sector, businesses and communities will be empowered to contribute in an effective and meaningful way. That trust can be fostered through development of clear and accessible rules regarding the use of data and information.

    e. **Systematic resilience**: Legal, cultural, technical and operational maturity will increase the system's ability to evolve and adapt to emerging risks.

Standardising the process: A National TSOC Information Sharing Framework

47. Standardising the information-sharing landscape will require strategic leadership and national co-ordination.

48. We recommend developing and implementing a National TSOC Information Sharing Framework (**Framework**) for the purpose of combatting organised crime. This Framework will provide the key building blocks for implementing and embedding an effective and efficient information sharing ecosystem amongst agencies and removing the culture of fear that currently persists about information sharing. It should be aligned to the TSOC Strategy.

49. The Framework should include a Common Information Sharing Standard (**CISS**) across all relevant agencies. This is essential to reduce the current inconsistencies and fragmentation. The CISS should:

    a. Confirm the general principles and legal frameworks that apply to information sharing amongst government agencies. This will necessarily be built around the Privacy Act and the relevant Information Privacy Principles.

    b. Identify the specific information sharing principles that are applicable to each particular agency (including aspects of the unique legislative framework that each agency operates under[17]) and how those principles will be applied by the agency. This will ensure that there is a consistent understanding within each agency of what their own information sharing powers and limitations are, as well as an understanding within each agency of the powers and limitations of each other agency within government.

    c. Where appropriate, establish protocols for the development (or amendment) of AISAs under the Privacy Act. While we have noted the limitations with AISAs above, they remain important tools to prevent agencies from regressing into previous practices, to ensure that the processes are transparent and are approved by the Privacy Commissioner and enable development of a consistent, coherent and future proofed national framework.

    d. Embed an expectation of proactive, as well as reactive, information sharing between agencies where information may be of assistance to another agency in relation to organised crime. This could be supported by a provision similar to section 92 of the Anti-Money Laundering and Countering Financing of Terrorism Act 2009, which makes it an offence for a reporting entity to fail to report certain suspicious activities to the Commissioner of Police.

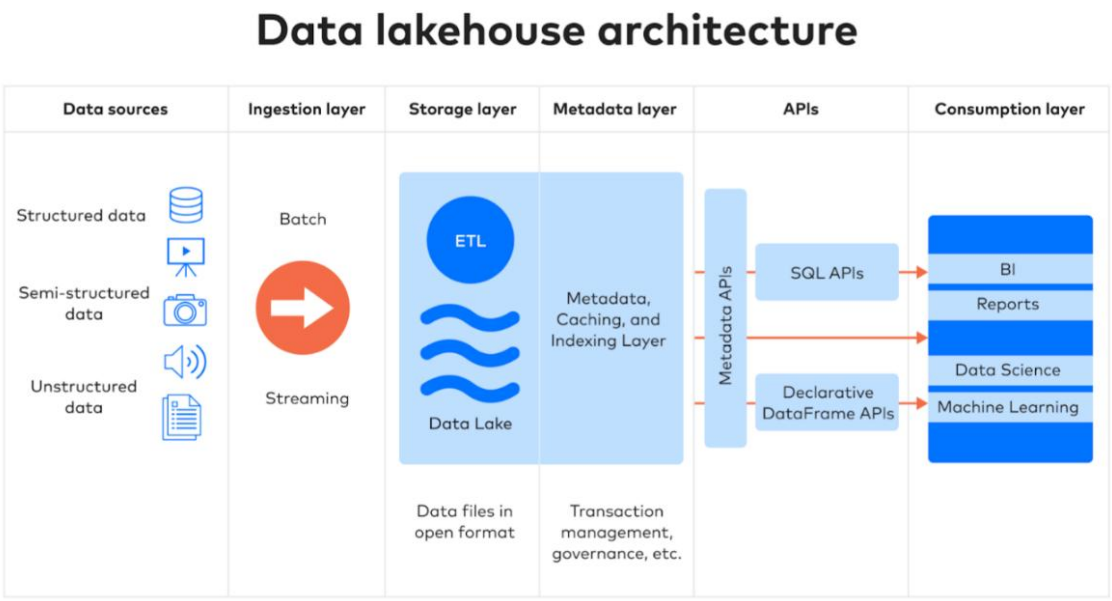
50. Development of the Framework should standardise, as much as practicable, the data formats, classification and systems protocols to ensure consistency of storage and handling of information across agencies. Sharing of data is of little practical use if it is stored in disparate ways across agencies that it is not readily accessible and useable once shared. A national information-sharing platform**,** in the form of a **data lake,** will enable effective sharing and use of information that can be shared within the new Framework.

51. A data lakehouse (which for simplicity we refer to as a data lake) is a centralised repository that stores large amounts of datasets, supported by the necessary

[17] For example, the specific information sharing provisions in the Customs and Excise Act 2018 or the Tax Administration Act 1994.

architecture to make that data useable and accessible for its intended purpose. We set out some information about the implementation of a data lake in **Appendix 1**.

52. The following image describes the data lake architecture.



53. There should be a standardised case management system that would sit alongside the data lake as an investigative tool. This should draw in particular on the design of the Police Information Management Tool (IMT), an investigative tool that integrates with the Police National Intelligence Application to enable traceable access to relevant information held by Police.[18] We have heard from several government agencies that their investigative capabilities would be improved by standardised access to IMT.

54. We recognise that the establishment of a data lake will involve the storage and use of large amounts of personal data. There are however in our view two key points to appreciate:

    a. First, this is not about obtaining new information. Rather, it is about the effective use of information that has already been obtained and is currently being stored by agencies.

    b. Second, a well designed and implemented data lake would provide greater traceability and transparency about who is accessing what data, and when, than the current system because all access would be digitally recorded. That is, it would be very easy to tell who has accessed what data and when, so accountability mechanisms can ensure that data is only being accessed and used lawfully for proper purposes by those who should be entitled to access it. Access

[18] Another example is the Joint International Crime Centre in the United Kingdom, a specialist unit established to improve the UK's policing of transnational, serious an organised crime. Establishment of the centre is accompanied by a new case management system that automates administrative processes, enabling officers to spend less time on admin and more time investigating and catching criminals. See National Crime Agency annual report and accounts: 2023 to 2024 (accessible) - GOV.UK

to certain types of information could also be effectively restricted through the security classification of each individual user.

Changing the culture: Moving from need to know to need to share

55. To move away from the risk-averse culture in relation to information sharing, the Framework should include measures designed to incentivise proactive sharing of information amongst agencies. This might include:

    a. A benchmarking tool to assess proactiveness, relevance of information shared, frequency and responsiveness.

    b. Transparency on overall system health and participation across the sectors.

    c. Implementation of key performance indicators relating to information sharing within senior leadership across the relevant agencies. For example, Chief Executives across government departments could have, as part of their KPIs, a certain threshold for compliance with the scorecard discussed above. Senior leaders steer the direction of their agencies – if they are motivated to improve the culture, that motivation should filter down through the organisation.

Ensuring effective implementation

56. The Privacy Commissioner has a mandate to monitor and enforce compliance with the Privacy Act. But there is currently no accountability mechanism for ensuring proactive information sharing to combat organised crime.

57. We recommend implementing governance and accountability mechanisms by a body that is solely focused on organised crime to provide unified oversight of systems-based issues following implementation of our recommendations. We will elaborate on how this can be achieved in our September report.

Mobilising the private sector as a key partner

58. The private sector is a key partner in the fight against organised crime. But there are two issues with the current settings within which those partnerships operate:

    a. First, current information sharing strategies tend to involve one-way traffic, with some information being collected by government from the private sector but insufficient outward sharing of information to the private sector. Information that would assist businesses in high-risk industries such as ports and airports to disrupt and prevent organised crime, such as key trends, emerging threats and features of organised crime, are not being provided. Businesses want this information. Sector leaders that we spoke to told us that they want a seat at the table. They want to help to design the solution. But they are being overlooked.

    b. Second, there needs to be an understanding amongst private sector entities of the threats of organised crime and the incentives for them to proactively respond. An important incentive is an understanding of the financial cost of not responding – the reputational and branding damage of crime impacts, the unplanned expenditure of responding to crime, and the commercial impacts that flow from this. That is the carrot. A co-ordinated, targeted messaging campaign to educate

the private sector about this is important. But there also needs to be a stick – a legislative mechanism for requiring the less than willing segment of the private sector to come to the table. This is where a legislative provision akin to the offence provision in section 92 of the Anti-Money Laundering and Countering Financing of Terrorism Act as noted above would be particularly useful.

59. There are a number of tools that can be utilised to achieve this:

    a. Formalising public-private partnerships with high-risk sectors through tools such as AISAs or data sharing agreements. These can be implemented in the first instance through pilot programmes, which can be utilised to refine effective legal, technical and operational frameworks.

    b. Strengthening the focus of the enforcement network in high-risk regions and sectors, through dedicated liaison roles within Customs, Police and other relevant agencies. Local presence of law enforcement can aid in building trust and information flows. This should occur in areas most vulnerable to organised crime, such as ports and border towns.

    c. Encourage establishment of organised crime prevention roles within private sector entities. These would be designated roles within organisations operating in critical private sector industries who would provide contact points, streamline information exchange and lift standards. This could involve, for example, adaptation of the existing roles within some businesses of Chief Risk Officer, who is responsible for establishing and maintaining enterprise vision, strategy, and work programs to ensure information assets and technologies are adequately protected.

    d. A targeted work program of sharing information with private sector in high-risk industries to ensure they understand their risk environment associated with organised crime.[19]

    e. An organised crime supply chain rating system. This would involve rating and accrediting businesses based on organised crime resilience and information sharing maturity. Ratings could be linked to things such as procurement eligibility in relation to government contracts.

Transnational information sharing

60. As explained in our May report, protecting our borders needs to start offshore, before the trade in illicit goods even reaches New Zealand. This can only be achieved through timely and targeted transnational information sharing with foreign agency counterparts.

61. Police Liaison Officers and similar roles in other agencies provide an important mechanism by which relationships can be developed between agencies in New Zealand and overseas. We encourage continued investment in developing and embedding these roles.

[19] As set out in our May report, High-risk industries include public sector agencies with law and regulatory enforcement responsibilities, companies that are involved in import and export supply chains, immigration advisers, professional facilitators, banks and telecommunications providers.

62. The New Zealand Transnational Crime Unit (**NZTCU**) provides an effective example of how information sharing can occur with overseas counterpart agencies. The NZTCU was established as a pilot programme in early 2019 to add New Zealand's resources and expertise to Pacific nations' fight against transnational criminal activity in the Pacific. The NZTCU plays an important role in the gathering and sharing of intelligence on transnational criminal activities in the region. Mechanisms for transnational information sharing to combat organised crime should draw in particular on the lessons learnt by the NZTCU.

Future proofing

63. There are three key components to a future-proofed system:

    a. **A clear legal framework**: Without a clear and consistently applied legal framework, the current roadblocks will return. Agencies will revert to a risk-averse mindset: if in doubt, don't share. Such a reversion will undo all of the gains that will be made by implementing our recommendations above. It cannot occur. The legal framework must be clear, well understood and consistently applied.

    b. **Accountability measures**: Government agencies and private sector businesses must be held accountable for performance of the information sharing expectations that we have recommended. It is not enough to implement them and expect them to be complied with. There must be incentives, including rewards for good compliance, and there must be consequences for poor compliance. Finally, there must be a mechanism for marking the homework, to make sure that compliance is enduring.

    c. **Investment in future technology**: Technology is evolving at a rapid rate. New technology brings new tools and new opportunities. But it also comes with cost. Organised crime will be utilising emerging technologies. If we want to keep pace, we must be prepared to invest and to innovate. We need to invest in AI, automation and advanced analytics tools that can be used to detect patterns, typologies and anomalies in large data sets.

Appendix 1: Data Lake

1. Evolving technology is one of our greatest tools for an effective real-time response to organised crime.

2. New Zealand's government agencies could significantly strengthen their ability to disrupt Organised Crime by adopting a secure, standards-based information sharing framework underpinned by a national data-lake architecture. This would enable agencies to contribute specific, pre-agreed datasets into a centralised, cloud-based repository. Doing so would unlock cross-agency visibility, enable pattern detection, generate a system-wide intelligence view, and support more coordinated led responses to organised crime threats.

3. Participating agencies would transfer data via encrypted application programming interfaces (APIs). This means sending the data from their agency into a secure data lake.

4. Once ingested, data would be automatically standardised and enriched with metadata defining its classification, source, and permitted uses. The centralised data lake, hosted within a secure government-controlled cloud platform, would partition data to ensure appropriate access control and containment of sensitive information. This means the technology can take the data from different agencies and make them useable together.

5. Robust tagging and encryption protocols would safeguard information at the field level, ensuring only authorised personnel can access or decrypt specific records. Access would be governed by both role-based and attribute-based controls, reflecting the user's agency, clearance level, and operational context. That is, if an enforcement officer currently has limited access, they will continue to have limited access.

6. Once inside the platform, approved users would access a secure interface, enabling cross-source queries, link analysis, and surfacing potential connections across diverse data types. This functionality would facilitate joint investigations and create an integrated operational picture that was previously constrained by agency data silos and system access limitations. In practice it means we can do more with the data to find out where organised crime is being committed and to do something about it.

7. Integrating AI into this platform would significantly enhance tactical and strategic value. AI can automatically identify patterns and relationships across large, complex datasets such as financial transactions, travel records, corporate structures, and identity data. It can detect anomalies, reconcile aliases, and map criminal networks, enabling more timely and informed decision-making. Real-time alerts, dynamic risk scoring, and network visualisations would also support operational agility and responsiveness.

8. AI tools also extend analytical reach into unstructured data sources, such as intelligence reports, notes, or interview transcripts. AI can extract meaningful indicators, highlight early signs of criminal activity, and anticipate emerging threats based on historical and behavioural modelling. This improves targeting precision, reduces manual workload, and enhances preventive strategic planning. Ultimately, AI integration strengthens disruption outcomes, unlocks the system view, and dramatically

improves resource efficiency. Work will be required to ensure that AI tools can be utilised in a lawful and responsible way.

9. From an operational standpoint, this model would dramatically improve the efficiency of information discovery and the effectiveness of cross-agency coordination. It reduces duplication, minimises reconciliation delays, and allows for near real-time detection of high-risk individuals or networks. For example, a known person of interest could be rapidly linked across agencies to multiple but otherwise unknown parallel case investigations, suspicious financial activity, cross-border movement, and the use of trust structures, insights that would previously have taken weeks, months to uncover, or worse, not at all.

10. This architecture can be scalable, privacy-conscious, and legally compliant. It creates a future-proof platform for secure and governed information sharing, enabling agencies to act with a unified view of organised crime.

11. Adopting a secure, standards-based data lake model addresses New Zealand's information-sharing system's significant weakness. It positions government agencies to respond to organised crime with the necessary speed, adaptability, scale, and analytical sophistication, unlocking greater cross-agency visibility and enabling more effective, intelligence-led disruption of organised crime.

12. The image below describes the architecture that would underpin a data lake.