

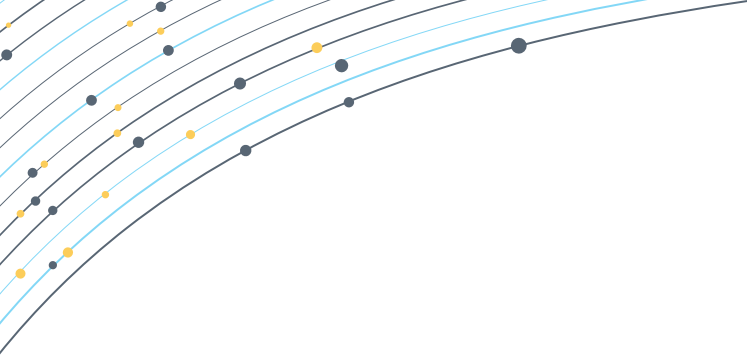


AUSTRALIAN  
**CRIMINAL  
INTELLIGENCE  
COMMISSION**

# Corporate Plan 2025–26

Covering reporting period 2025–26 to 2028–29





The Australian Criminal Intelligence Commission acknowledges the traditional owners and custodians of country throughout Australia and acknowledges their continuing connection to land, sea and community. We pay our respects to the people, the cultures and the elders past, present and emerging.

© Commonwealth of Australia 2025



Except for the Commonwealth Coat of Arms, all material in this publication is provided under a Creative Commons Attribution 4.0 International (CC BY 4.0) licence. This licence applies only to material as set out in this document. To view a copy of this licence, visit [creativecommons.org/licenses/by/4.0/](https://creativecommons.org/licenses/by/4.0/).

The guidelines for using the Coat of Arms are available on the website of the Department of the Prime Minister and Cabinet at [pmc.gov.au/honours-and-symbols](https://pmc.gov.au/honours-and-symbols).

The document must be attributed as the  
*Australian Criminal Intelligence Commission Corporate Plan 2025–26.*

ISSN: 2652-5844 (online)

# CEO introduction



The Australian Criminal Intelligence Commission (ACIC) protects Australia from serious criminal threats by collecting, assessing and disseminating intelligence and policing information.

We are at the forefront of combating the threats Australia faces from serious and organised crime. Our unique, actionable and insightful intelligence is used to make Australia hostile to criminals who harm our communities and our national interests.

The *Independent Review of the Australian Criminal Intelligence Commission and associated Commonwealth law enforcement arrangements* (ACIC Review) released last year has provided valuable insights and recommendations that are positively shaping the future of the ACIC and the significant value we provide. Implementing these recommendations and our

new intelligence operating model are a major focus for the agency over the coming year and will ensure our functions, powers and legislation are fit for purpose.

We are focused on building strong partnerships. Working collaboratively with law enforcement partners, the National Intelligence Community, regulators and policy agencies, the ACIC delivers a diverse suite of criminal intelligence products, services, analysis and advice. The agency has an integrated view of crime, made possible through its connected systems and the capabilities that it uses to cooperate and collaborate with domestic and international partners to confront the threat posed by serious and organised crime impacting Australia.

The ACIC's criminal intelligence insights build awareness and influence strategies to harden the environment and create new opportunities to combat serious criminal threats.

We have updated our performance framework to further mature our approach and to align with ACIC Review recommendations and to further mature our approach. Established in accordance with legislative requirements, our framework captures our key activities, intended results and how we will assess our delivery.

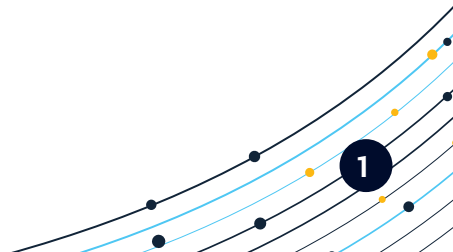
As the accountable authority of the ACIC, I am pleased to present the ACIC's Corporate Plan as required under paragraph 35(1)(b) of the *Public Governance, Performance and Accountability Act 2013*. This Corporate Plan has been prepared for the 2025–26 reporting year and covers the 4-year period from 1 July 2025 to 30 June 2029.

A handwritten signature in black ink, appearing to read 'H Cook', written over a light blue grid background.

**Heather Cook**

Chief Executive Officer  
Australian Criminal Intelligence Commission

6 August 2025



# ACIC Corporate Plan 2025–26 to 2028–29

## Our purpose

To protect Australia from serious criminal threats by collecting, assessing and disseminating intelligence and policing information.

## Our strategic direction

Our purpose is guided and operationalised through our 4-year strategic direction, annually updated and approved by the ACIC Board. See Figure 1.

## Our key activities and intended results

**We collect, analyse and communicate intelligence relating to serious and organised crime impacting Australia, including where it has a transnational dimension.**

- We coordinate, collect, analyse and share valuable criminal intelligence on transnational serious and organised crime threats to inform ACIC and partner operational and strategic policy responses, and regulatory and legislative reforms.

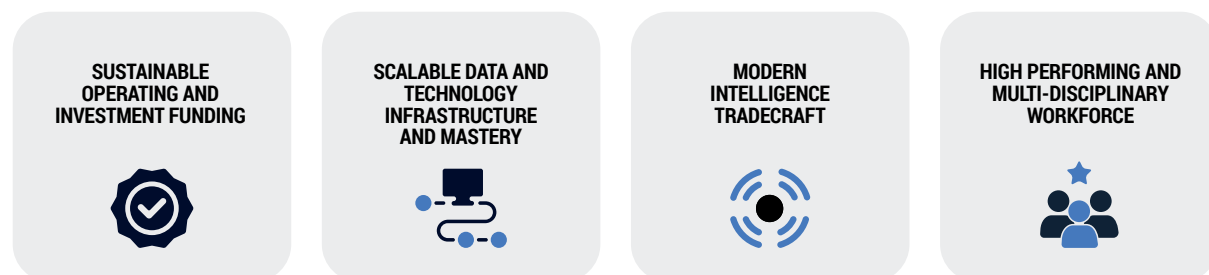
**We have systems and services that enable criminal intelligence and policing information to be shared across jurisdictions, including the provision of nationally coordinated criminal history checks.**

- We ensure there are systems and services that enable criminal and policing information to be shared across jurisdictions.
- We coordinate the delivery of a risk-based, reliable and timely National Police Checking Service that adheres to regulatory requirements.

## Our operating context



## Enterprise capabilities



# Purpose

Our purpose is to protect Australia from serious criminal threats by collecting, assessing and disseminating intelligence and policing information. The agency is part of the Home Affairs portfolio and a member of the National Intelligence Community.

We operate under the *Australian Crime Commission Act 2002* (ACC Act) and our role and functions are underpinned by supporting legislation in each state and territory.

The ACC Act directs aspects of our governance and accountability arrangements, including establishing and outlining the role of the ACIC Board. The ACIC Board is composed of agency heads from Commonwealth, state and territory law enforcement bodies, and key regulatory and national security agencies.

Each year, the ACIC Board provides a statement of strategic direction as shown in Figure 1.

Figure 1 Strategic direction





# Our role

We have two distinct roles:

- To collect, analyse and communicate intelligence relating to serious and organised crime impacting Australia, including where it has a transnational dimension.
- To ensure that there are systems and services that enable criminal intelligence and police information to be shared across jurisdictions, including the provision of nationally coordinated criminal history checks.

## Intelligence

Our unique, actionable and insightful intelligence on serious and organised crime threats impacting Australia plays a critical role in bringing together law enforcement, intelligence, regulatory and policy partners to build coordinated strategies to counter the threat. We use a range of specialist capabilities to collect and analyse information to discover new criminal threats and to develop new insights about the criminal environment. Our criminal intelligence insights build awareness and influence strategies to harden the environment and create new opportunities to combat serious and organised crime.

## Criminal intelligence and police information sharing

### National policing information systems

We have an important role in brokering access to policing and criminal information and intelligence holdings across Australia through its national policing information systems and services. We have a crucial role in facilitating access to policing and criminal information and intelligence holdings across Australia through delivery of 17 national policing information systems. This enables more than 71,000 police officers and other accredited users to undertake operational policing and intelligence activities and ensure community safety.

### National Police Checking Service

To help ensure the safety of the Australian community, the ACIC works with Australian police agencies and accredited bodies to deliver the National Police Checking Service. Through the National Police Checking Service, members of the community are able to apply for a nationally coordinated criminal history check, commonly known as a 'police check'. Police checks assist decision-makers in assessing the suitability of applicants applying for a range of employment and volunteer roles, registration or entitlement schemes, and national immigration and citizenship programs.

We fulfil our role as the regulator of National Police Checking Service accredited bodies in line with the principles of regulator best practice and the direction set out for the agency in a statement of expectations by the Portfolio Minister and a corresponding statement of intent by our CEO. The current statements are available at [www.acic.gov.au/publications/corporate-documents](http://www.acic.gov.au/publications/corporate-documents).

# Operating context

## Environment

Serious and organised crime costs the Australian economy over \$68 billion per year, diverting funds that could otherwise be used to support important government services and initiatives. It encompasses a proliferation of illicit activities that target and harm Australian citizens and undermine Australian interests such as our border integrity, economic prosperity, social cohesion, government revenue and services, geopolitical interests and health. Developments in the serious and organised crime environment shape our intelligence collection priorities, strategies and challenges.

*Our work exposes the complex and ever-shifting nature of serious and organised crime impacting Australia, including where it has a transnational dimension*

Serious and organised crime actors are profit driven and increasingly globalised, collaborative and technically enabled. They are agile and seek opportunities to monitor and exploit technical developments in order to counter law enforcement and intelligence agencies' effort to disrupt their criminal activities.

Understanding criminal networks and how they operate, and identifying emerging threats, allows us to inform and support prevention and disruption actions, which creates a much more hostile operating environment for serious and organised crime actors.

- **Serious and organised crime threatens Australia's security and prosperity.** Criminal networks are global, technology-enabled and resilient. Serious and organised crime actors exploit growing uncertainty in the realms of the economy, geopolitics, instability and global conflict, focusing firmly on opportunities to derive profit at the expense of the security and wellbeing of the Australian community.
- **Serious criminal threats impact everyone.** Serious and organised crime actors are highly adept at using everyday systems and services to enable destructive, pervasive and complex illicit ventures. They make our communities less safe, create unfair competition for legitimate businesses and industries, exploit our most vulnerable people and increase pressure on the economy and vital health and welfare services.
- **Criminals prioritise personal gain above all else.** The heads of criminal networks lead global organisations with all elements of their illicit business focused on maximising profits. These high-level criminals will go to great lengths to achieve their goals, regardless of traditional allegiances, geographic boundaries, or the harm they cause.
- **Serious and organised criminal enterprises are globalised and collaborative.** Even the highest-threat criminal enterprises have limitations to their reach and rely on the services, access and expertise of other criminals to succeed in their illicit ventures. More than ever, serious organised crime groups are prioritising collaboration over competition.
- **Technology is expanding opportunities for criminals across every category of crime.** Criminals quickly adopt emerging and advanced technologies to enable and expand their end-to-end business models. As Australians rely more heavily on online services and platforms, global opportunities for cybercrime, serious financial crime and victim-based crime expand. Our increasingly digital world also grants criminals easier access to illicit commodities, digital currencies, specialist tools and technologists. These tools and methodologies are also commoditised by criminals across online forums and marketplaces.
- **Criminal groups are enabled by insiders and professional facilitators.** Serious organised crime networks rely on a range of skills to help conceal their activity and manage the profits of crime. Criminals exploit insiders in Australian supply chains, leveraging their access and knowledge to evade detection by law enforcement and border security. Professionals such as lawyers, accountants and real estate agents are also engaged (both wittingly and unwittingly) for their skills to assist in masking and facilitating complex criminal activities.



*We are building an organisation that is data driven, technologically enabled and globally focused*

## Capability

Ongoing development and modernisation of our capability ensures that we can continue to achieve and deliver on our purpose.

During the period of this Corporate Plan, we will continue internal reforms and improvements, implementing a new operating model that will enable us to deliver more timely and relevant intelligence and national policing information systems to partners, using existing and better aligned resources.

### New operating model

We have developed an operating model that defines the high-level intent of how the agency will operate in the future. Implementation of the new model iteratively dependent upon available funding and will seek to enhance our ability and capacity to:

- **target serious and organised crime and its enablers** – by building dedicated intelligence mission management capabilities and uplifting and enhancing analytic and assessment capabilities. We will focus on serious and organised crime sources by expanding our international footprint including deployments and secondments, enhancing and extending our collection capabilities, and leveraging advanced technology to enhance efficiency and reduce operational risk.
- **harden the environment to serious and organised crime threats** – by developing an outreach program to engage industry, academia and the public to harden Australia's defences and build resilience against serious and organised crime. We will uplift and enhance our external services for sharing and collaborating with our partners and customers on national data, information, intelligence and criminal history checks.
- **integrate data, technology and capabilities** – enhancing enterprise-wide data capabilities; including data governance, tooling and data fluency, to enable more efficient exploitation of agency and national data. We will mature enabling capabilities within the agency to combat threats, improve information protection and support frontline service delivery. We will enhance our cyber security posture, replace legacy technology and implement new solutions to support operating at pace and scale and in compliance with government policies.

### People and culture

Attracting, retaining and developing people will be essential as we adapt to evolving workforce challenges. National talent shortages, increased competition for skilled professionals and shifting workforce expectations will require us to position the agency as an employer of choice.

Over the next 4 years, we will address critical skills gaps, enhance leadership talent pipelines, and improve recruitment processes and retention strategies. With digital transformation accelerating, we will need to upskill existing employees in data analytics, artificial intelligence and cyber security to remain at the forefront of intelligence capability. Targeted recruitment training, leadership development and knowledge sharing will support this skills uplift, especially in specialist analytical roles.

These priorities will support the adaptation of our 2024–25 interim strategic workforce plan, which aligns with the ACIC Enterprise Agreement 2024–2027, and support the development of a 5-year strategic people plan that will continue our reform agenda to enhance our operational efficiency. Having adopted the Australian Public Service Strategic Commissioning Framework in our workforce planning approach in 2024–25, we will continue to embed the principles of the framework in our workforce strategies.

In 2025–26 we will continue efforts to bring core work in-house in line with the APS Strategic Commissioning Framework. We expect our targets for 2025–26 to focus on reduced outsourcing of ICT Digital Solutions and Portfolio Program and Project Management.

Continuing investments in leadership, employee wellbeing, integrity and enhancing inclusive culture strategies reinforce our commitment to retaining and developing talent. We understand that fostering an engaged workforce is crucial for delivering intelligence-led solutions that protect Australia's national security.

## Intelligence and information capabilities

### Intelligence capabilities

*We share our intelligence, information and work with a range of partners to make Australia hostile to criminals who harm our communities and our national interests*

Our intelligence capabilities and infrastructure include the tradecraft and tools through which we identify criminal activity through covert methods, including technical and human intelligence, and through coercive collection, using our legislated powers.

We continue to invest in these capabilities to deliver unique and actionable intelligence that supports our stakeholders and partners in targeting and disrupting serious and organised crime. Our strategic assessments and insights also inform policy and government responses, while our operational intelligence directly supports targeted partner-led interventions.

### National information sharing capabilities

*We provide front line with critical policing information to improve officer and community safety*

We provide intelligence and national police information-sharing services to Australian police forces, intelligence partners, and other approved bodies. This includes providing associated technical support and assurance on system integrity and data quality. These national policing information services enable our partners to better combat current and evolving criminal and national security threats.

As part of our commitment to evolve these systems to meet current and future needs, we have developed the National Criminal Intelligence System, which connects data from Australian law enforcement agencies and provides secure access to a national view of policing and criminal information and intelligence. As a core information sharing platform, the National Criminal Intelligence System provides law enforcement and intelligence agencies with a comprehensive, unified picture of criminal activity that enables better informed decision-making to help keep frontline officers and the Australian community safe.

Capability enhancements planned for the National Criminal Intelligence System in 2025–26 focus on adding datasets, improving criminal intelligence exploitation functionality and ensuring the National Criminal Intelligence System meets future national criminal information and intelligence-sharing needs.

### Checking service capabilities

Through the National Police Checking Service we facilitate nationally coordinated criminal history checks. While all Australian police agencies participate in delivering criminal history checks, as the overarching Commonwealth agency with legislative responsibility for delivering nationally co-ordinated criminal history checks, is committed to ensuring a nationally consistent approach to ensure the delivery of timely and accurate information.

Our role involves regulating the external bodies that are accredited by us to access the National Police Checking Service. To strengthen our position as a regulator, we have entered into a new access agreement with all accredited bodies, which came into effect on 1 January 2025. The new agreement introduces stronger controls governing the management of ACIC accredited bodies, reinforcing our commitment to ensuring the safety of the Australian community by holding accredited bodies to a high standard of accountability and responsibility.

## Data and technology

Advances in technology create significant opportunities for us, including the ability to rapidly harness new and evolving data sources and apply sophisticated digital analysis tools to extract insights and generate the insightful intelligence needed to effectively respond to the criminal threat.

### Strategic approach to data

The scale and diversity of data critical to our functions is expanding, as the serious and organised crime threat landscape also rapidly evolves. While advances in technology present great opportunities, there are also serious risks. In response, we need increased specialisation, agility and robust governance practices to stay informed and aware of emerging challenge, and to effectively harness new technology to respond to sophisticated criminal activities.

To meet these challenges, we will continue to invest in its analytics and data management capabilities, supported by key enablers such as a skilled workforce, a strong data governance foundation, high standards of data quality, strategic partnerships through collaboration and advanced technology.

Our ICT and Data strategies prioritise and guide our digital and data capability development. The strategies are informed by, and align with, the **Strategic Direction 2025–29**, outlining key priorities that position us for the future, including: foundation building, collaboration, mature management, and sustainability.

The strategies are underpinned by detailed digital roadmaps and business initiatives to ensure stewardship of data and systems. The roadmaps, combined with enterprise architecture oversight, equip us to minimise duplication and fragmentation in the ICT environment while ensuring that opportunities to leverage data and new technologies are considered.

### Sustainable digital solutions

We adopt sustainment practices that ensure our digital products and services are contemporary. As the primary custodian of national criminal intelligence and police information, we reiterate our commitment to enhancing the systems that deliver effective data-sharing services and intelligence insights to enable cross-jurisdictional identification of criminal threats.

Our progressive shift to agile work practices and a combined development–operations delivery model is leading to better cost management and resource balancing across our ICT portfolio, improving our responsiveness and delivering productivity gains.

Our strategic architecture roadmaps directly inform the ACIC’s multi-year ICT investment plan, providing the basis to forecast and allocate funding based on agreed priorities and ongoing commitments. This is key to successfully deploying new digital solutions and building foundational data capabilities that meet emerging business requirements, while enhancing and sustaining our existing technology investments, and retiring end-of-life systems in a timely manner.

## Risk management

We strive to foster a positive risk culture where staff confidently handle uncertainties and opportunities. We engage with risk by applying sound risk assessment and management principles to empower managers and staff to make informed decisions, which enable action.

In 2024–25, we updated our risk management framework, policy and procedures. These documents facilitate our compliance with the Commonwealth Risk Management Policy, the *Public Governance, Performance and Accountability Act 2013* (PGPA Act), and the international standards set out in ISO 31000:2018 Risk Management – Guidelines.

In 2025–26, we will focus on embedding our new risk management framework; maturing our risk culture to more effectively integrate risk management into agency planning, reviewing and monitoring processes and supporting proactive risk management as part of our daily responsibilities.

Our CEO has overall responsibility for risk management in the agency. The CEO is supported by the Chief Risk Officer and members of the executive who have defined accountabilities for enterprise and divisional risks.

Risk governance oversight is provided by the agency's Commission Executive Committee, the Compliance and Risk Committee, and by the Audit and Risk Committee which has specific responsibilities under the PGPA Act to review and provide advice as to the appropriateness of our risk management framework.

### Risk appetite and tolerance








We have a high-risk appetite for the pursuit and collection of criminal intelligence, the nature of this work is intrinsically higher risk and requires a more forward leaning posture to meet the required objectives. This posture necessarily requires more oversight and active risk management. However, the agency has a low-risk appetite in relation to legal, compliance and integrity matters.

To support the agency's risk appetite, individual tolerances have been applied to each of the enterprise risk categories. This is defined in our risk management framework. Risks that are outside of tolerance will be escalated to the appropriate executive or committee for action.

### Enterprise risks

Our enterprise-level risk domains encompass the areas of most significant exposure and ensure our internal governance arrangements allow for regular and active management and oversight of our policy settings and mitigations in these critical areas of operation. There are 7 enterprise risks as shown in Table 1.

Table 1 ACIC enterprise risks

Enterprise risks and risk categories	
	<b>Legal and ethical</b> Failure to adequately and ethically consider and treat legal risk and/or failure to comply with policy and statutory requirements.
	<b>Health and safety</b> Failure to support the safety and wellbeing of workers and manage health and safety hazards presented by our varied operating environments.
	<b>Security and integrity</b> Failure to protect against external and internal threats to tradecraft and sensitive capabilities, compromise of employees, information security, integrity/corruption, unlawful access to premises, and physical protection measures.
	<b>Stakeholder</b> Failure to plan for, establish and effectively manage and prioritise stakeholder relations, meet their requirements, and protect their interests and equities.
	<b>Technology and data</b> Failure to implement, manage or secure ACIC's data/services/systems/tools, including staying on top of emerging technology.
	<b>People and culture</b> Failure to plan for, attract, develop, retain and maintain a workforce with the skills and capabilities which are aligned to the ACIC's organisational needs.
	<b>Finance and resources</b> Failure to adequately manage financial requirements, contracts, procurement and prevent and detect financial fraud.

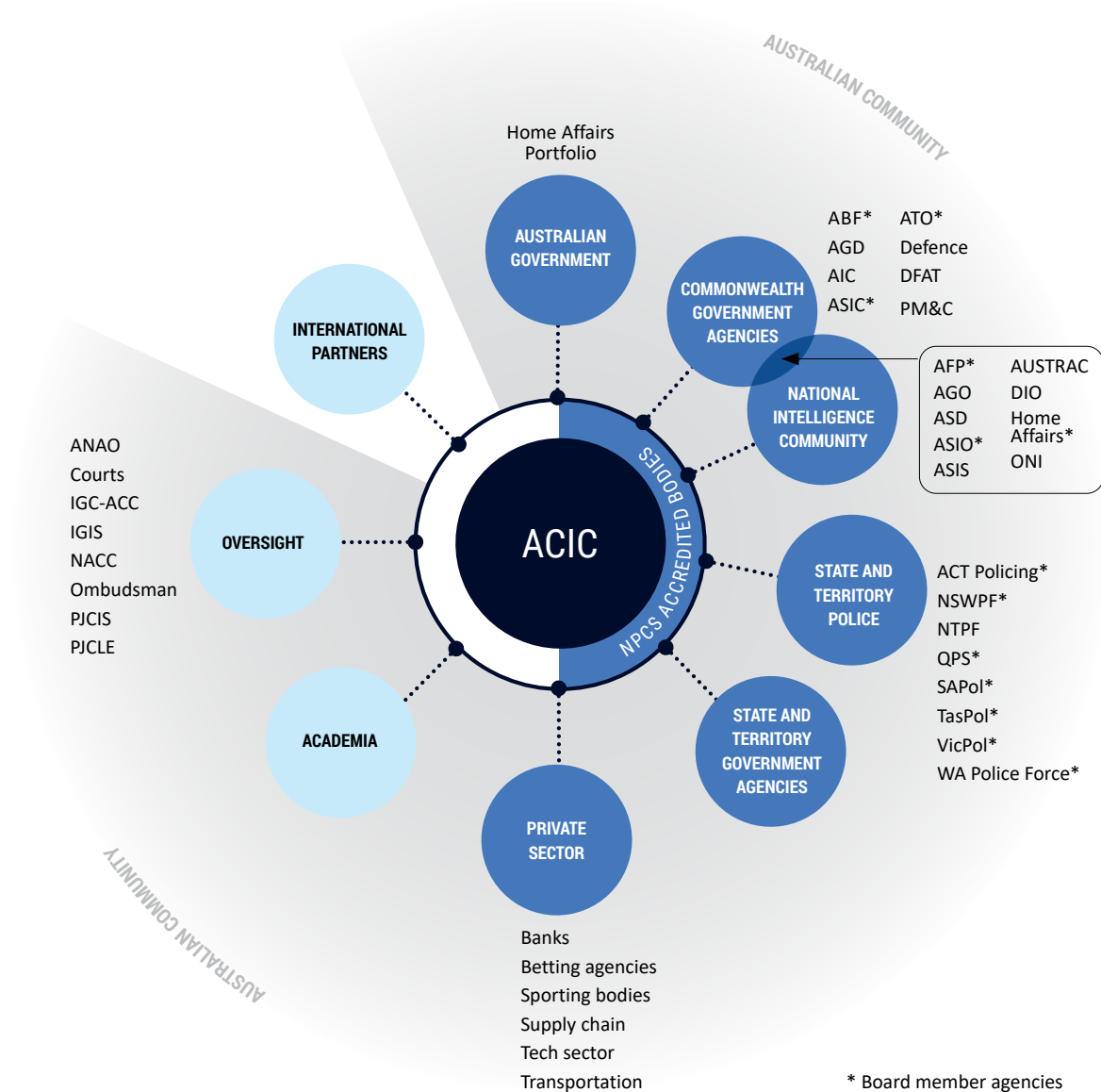
## Cooperation

Reducing the impact of transnational serious and organised crime involves cooperation across many government departments, intelligence, law enforcement and regulatory agencies and other entities, in Australia and overseas. Effective engagement is critical.

We engage in a variety of forums, taskforces and multi-agency teams and chair a variety of standing working groups and committees to build stronger national networks for cooperation and information exchange.

Figure 2 illustrates the connections between our key stakeholder groups.

Figure 2 Stakeholders



\* Board member agencies

ABF	Australian Border Force
ACT Policing	Australian Capital Territory Policing
AFP	Australian Federal Police
AGD	Attorney-General's Department
AGO	Australian Geospatial-Intelligence Organisation
AIC	Australian Institute of Criminology
ANAO	Australian National Audit Office
ASD	Australian Signals Directorate
ASIC	Australian Securities and Investments Commission
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service

ATO	Australian Taxation Office
AUSTRAC	Australian Transaction Reports and Analysis Centre
Defence	Department of Defence
DFAT	Department of Foreign Affairs and Trade
DIO	Defence Intelligence Organisation
Home Affairs	Department of Home Affairs
IGC-ACC	Inter-Governmental Committee on the Australian Crime Commission
IGIS	Inspector-General of Intelligence and Security
NACC	National Anti-Corruption Commission

NPCS	National Police Checking Service
NSWPF	New South Wales Police Force
NTPF	Northern Territory Police Force
ONI	Office of National Intelligence
PJCIS	Parliamentary Joint Committee on Intelligence and Security
PJCLE	Parliamentary Joint Committee on Law Enforcement
PM&C	Department of the Prime Minister and Cabinet
QPS	Queensland Police Service
SAPol	South Australia Police
TasPol	Tasmania Police
VicPol	Victoria Police
WA Police Force	Western Australia Police Force



# Performance

As a statutory agency within the Home Affairs portfolio, we deliver one outcome, as set out in the portfolio budget statements:

*To protect Australia from criminal threats through coordinating a strategic response and the collection, assessment and dissemination of intelligence and policing information.*

We assess our results in delivering our outcome, and achieving our purpose, through the measures set out in our performance framework.

## Performance framework

The Corporate Plan is our primary planning document.

We continue to mature and improve our performance framework ensuring our performance measures and targets are aligned to our key activities and demonstrate how we will deliver against our purpose.

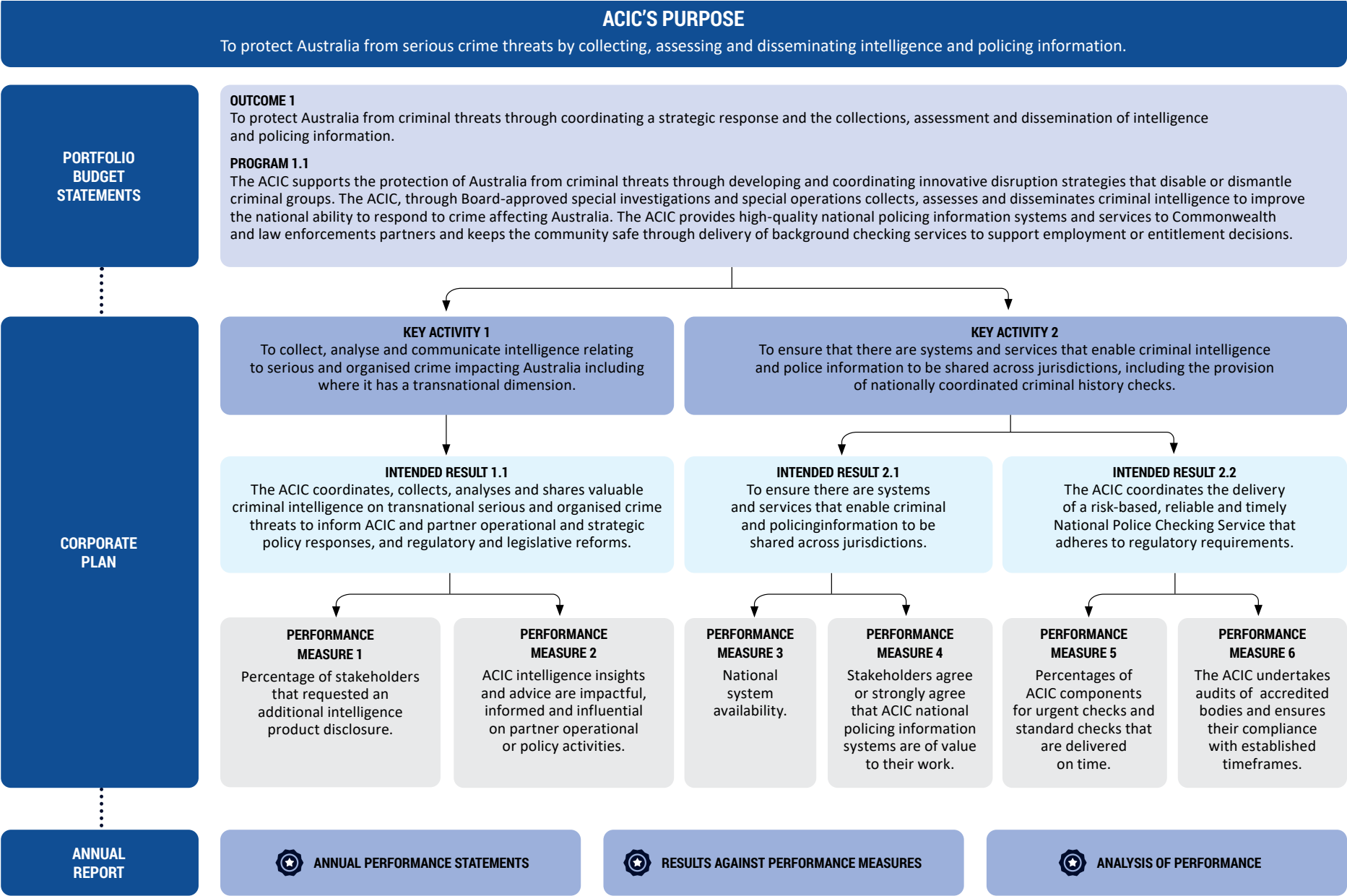
The number of measures has been reduced from 11 in 2024–25 to 6 in 2025–26, driven by ongoing internal changes influenced by the *Independent Review of the Australian Criminal Intelligence Commission and associated Commonwealth law enforcement arrangements*.

We also annually review our measures and their methodologies to ensure they are robust operationally relevant to our current practices, and fulfil section 16EA of the Public Governance, Performance and Accountability Rule 2014.

The ACIC coordinates the delivery of a risk-based, reliable and timely National Police Checking Service that adheres to regulatory requirements. A performance measure related to this function is included within the Corporate Plan in accordance with the official guidance issued by the Department of Finance on Regulator Performance.

Figure 3 shows our performance framework for 2025–26, and establishes a clear line of sight between the portfolio budget statements, the measures in our Corporate Plan and results to be provided in our annual report.

Figure 3: Performance framework



## Key activities and performance measures

In 2025–26, we will achieve our purpose and deliver our outcome through 2 key activities:

- **Key activity 1:** To collect, analyse and communicate intelligence relating to serious and organised crime impacting Australia, including where it has a transnational dimension.
- **Key activity 2:** To ensure that there are systems and services that enable criminal intelligence and police information to be shared across jurisdictions, including the provision of nationally coordinated criminal history checks.

We will measure our performance against the intended results for those key activities.

## Intelligence

We contribute to protecting Australia from transnational serious and organised crime threats by collecting, analysing and communicating intelligence to inform partners' operational and strategic policy responses, and regulatory and legislative reforms.

Our criminal intelligence efforts are supported by:

- ACIC Board determinations which authorise special ACIC operations or special ACIC investigations and national intelligence priorities
- partner relationships spanning the law enforcement and intelligence sectors
- ACIC tradecraft and collection capabilities including coercive examinations and notices.

Because intelligence is often an input to inform the actions of other agencies, this group of measures emphasises the value delivered for our partners and stakeholders.

**Key activity 1: To collect, analyse and communicate intelligence relating to serious and organised crime impacting Australia, including where it has a transnational dimension.**

### Intended result 1

The ACIC coordinates, collects, analyses and shares valuable criminal intelligence on transnational serious and organised crime threats to inform ACIC and partner operational and strategic policy responses, and regulatory and legislative reforms.

Table 2: Performance measure 1

Measure				
Percentage of stakeholders that requested an additional intelligence product disclosure				
Target	2025–26	2026–27	2027–28	2028–29
Additional disseminations	Equal to or greater than 60%	Equal to or greater than 60%	Equal to or greater than 60%	Equal to or greater than 60%

### Rationale

Additional disseminations of products indicate that partners find ACIC products of interest or valuable to their work and that ACIC intelligence needs to be shared further.

### Methodology

The number of additional requests for disseminations of products is calculated as a percentage of all product disseminations for the financial year (first time issued plus any disseminations of products previously issued). This figure is compared to the target, which has been derived from the average percentage of additional disseminations from 2022–23 to 2024–25.

### Changes to measures

Measure 1 corresponds to measure 1.3 of 2024–25, which was based on a count of total incoming additional dissemination requests. It was modified to use a percentage in 2025–26.

*Table 3: Performance measure 2*

Measure				
ACIC intelligence insights and advice are impactful, informed and influential on partner operational or policy activities				
Target	2025–26	2026–27	2027–28	2028–29
Stakeholder survey respondents deliver 'agree' or 'strongly agree' ratings	Equal to or greater than 80%	Equal to or greater than 80%	Equal to or greater than 80%	Equal to or greater than 80%

### Rationale

Intelligence can be applied to and may inform law, regulation and policy as well as operational strategies adopted by partners. Obtaining feedback from users allows us to know whether our intelligence products are useful and delivering what is required.

### Methodology

An annual survey is used to collect feedback from stakeholders on the quality and usefulness of ACIC products, analysis and advice to inform operational activity and policy. The survey uses a 5-point rating scale or equivalent to assess 'agree' or 'strongly agree' statements. The results for those rating categories are combined to calculate a percentage of the total responses to the 5-point rating scale.

### Changes to measures

Measures 1.4 and 1.5 of 2024–25 have been combined into the new measure 2, which emphasises our products' quality and ability to inform partners' work.

## National policing information systems

National policing information systems allow users to search holdings on diverse topics such as general policing information, vehicles of interest, DNA profiles and unidentified human remains. They provide relevant and timely information to support frontline 24/7 policing responses as well as specialist investigations. The information can help keep police officers and the community safe, and progress investigations supporting criminal justice outcomes.

National policing information systems must be available and reliable, and meet the specific needs of users. These factors are the focus of our measures.

**Key activity 2:** To ensure that there are systems and services that enable criminal intelligence and police information to be shared across jurisdictions, including the provision of nationally coordinated criminal history checks.

### Intended result 2.1:

To ensure there are systems and services that enable criminal and policing information to be shared across jurisdictions.

Table 4: Performance measure 3

Measure				
National system availability				
Target	2025–26	2026–27	2027–28	2028–29
Collective attainment of board benchmarks across all systems	A rating equal to or greater than 'substantially met'	A rating equal to or greater than 'substantially met'	A rating equal to or greater than 'substantially met'	A rating equal to or greater than 'substantially met'

#### Rationale

The ACIC's national policing information systems, which currently include 17 individual but interlinked IT systems, provide frontline policing and intelligence information services fundamental to police and community safety. Availability and reliability are core features that ensure that an IT system delivers its services. We measure national availability to ensure that national policing information systems provide reliable access to data.

#### Methodology

This measure uses an internal dashboard which reports on the availability of each system, predominantly based on information from IT outage incident management processes. Unscheduled outages are identified through system monitoring and may also be reported to the ACIC by users. The dashboard automatically calculates national availability, defined as the percentage of time when the system is operating in all jurisdictions.

Availability benchmarks for each individual system are set by the ACIC Board and updated every 3 years. The next updates are scheduled for 2026–27. Each system's individual result is calculated against its benchmark using the following matrix: met (the benchmark figure is reached or exceeded), substantially met (50-99% of the benchmark figure is met), partially met (25-49% of the benchmark figure is met) and not met (less than 25% of the benchmark figure was met). The sum of all the individual results are then calculated and assessed against the collective target of substantially met.

#### Changes to measures

Nil.

Table 5: Performance measure 4

Measure				
Stakeholders agree or strongly agree that ACIC national policing information systems are of value to their work				
Target	2025–26	2026–27	2027–28	2028–29
Stakeholder survey respondents deliver 'agree' or 'strongly agree' ratings	Equal to or greater than 80%	Equal to or greater than 80%	Equal to or greater than 80%	Equal to or greater than 80%

#### Rationale

The national policing information systems are a key deliverable and joint initiative with partners, serving Australian law enforcement and government agencies. Systems such as National Criminal Intelligence System are major investments and government priorities. All systems play a crucial role in supporting partners' operations. The ACIC needs to know that its systems are relevant and deliver value to partners.

### Methodology

Stakeholders are annually surveyed to collect feedback about the value they gain from using the national policing information systems. The survey uses a 5-point rating scale or equivalent to assess 'agree' or 'strongly agree' statements. The results for those rating categories are combined to calculate a percentage of the total responses to the 5-point rating scale.

### Changes to measures

Nil.

## National Police Checking Service

The ACIC works with Australian police agencies and accredited bodies to deliver the National Police Checking Service. The National Police Checking Service allows people to apply for a nationally coordinated criminal history check, or 'police check', which is a point-in-time check often required when applying for employment, Australian citizenship, appointment to positions of trust, or a variety of licensing and registration schemes.

For the National Police Checking Service to be effective, police checks must be delivered on time, and accredited bodies must comply with the agreement that controls their access to the National Police Checking Service Support System. These factors are the focus of our measures.

### Intended result 2.2:

The ACIC coordinates the delivery of a risk-based, reliable and timely National Police Checking Service that adheres to regulatory requirements.

Table 6: Performance measure 5

Measure				
Percentages of ACIC components for urgent checks and standard checks that are delivered on time				
Target	2025–26	2026–27	2027–28	2028–29
Urgent checks completed in 5 business days	Equal to or greater than 95%	Equal to or greater than 95%	Equal to or greater than 95%	Equal to or greater than 95%
Standard checks completed in 10 business days	Equal to or greater than 95%	Equal to or greater than 95%	Equal to or greater than 95%	Equal to or greater than 95%

### Rationale

National Police Checking Service requests require prioritisation and triage, including time frames for completion. Having requests processed based on timeliness requirements supports quick decision-making for employment and community safety where it is needed, especially in sectors involving vulnerable people or national security. Measuring check completion ensures that the ACIC is aware of, and fulfils, timeliness requirements.

### Methodology

The ACIC Board has set the time targets for the completion of urgent and standard checks. The measure calculates the percentage of urgent checks completed in 5 business days and the percentage of standard checks completed in 10 business days during the financial year. The categorisation of the request as either 'urgent' or 'standard' is applied by the organisation requesting the check upon submission to the ACIC. The results are compared against the target of 95% to assess performance.

### Changes to measures

Nil.



Table 7: Performance measure 6

Measure				
The ACIC undertakes audits of accredited bodies and ensures their compliance with established timeframes				
Target	2025–26	2026–27	2027–28	2028–29
Accredited bodies subject to an audit or compliance check	Equal to or greater than 10%	Equal to or greater than 10%	Equal to or greater than 10%	Equal to or greater than 10%

#### Rationale

The ACIC, the Australian Government and members of the community need to be able to have trust in the National Police Checking Service. Trust is supported by the accreditation system and compliance checks. Should the National Police Checking Service operate without integrity, it would potentially have significant security and corruption impacts for the community and economy, and dangerous impacts for children and other vulnerable people.

This performance measure also addresses the ACIC's reporting obligations as the regulator of accredited bodies, as outlined in Australian Government Resource Management Guide 128 – Regulator Performance.

#### Methodology

Data on the numbers of total accredited bodies and ACIC compliance audits is used to calculate the percentage of bodies subject to checks. This is compared against the target of 10% or more accredited bodies being subject to audits or compliance checks.

#### Changes to measures

Nil.



[acic.gov.au](https://acic.gov.au)