

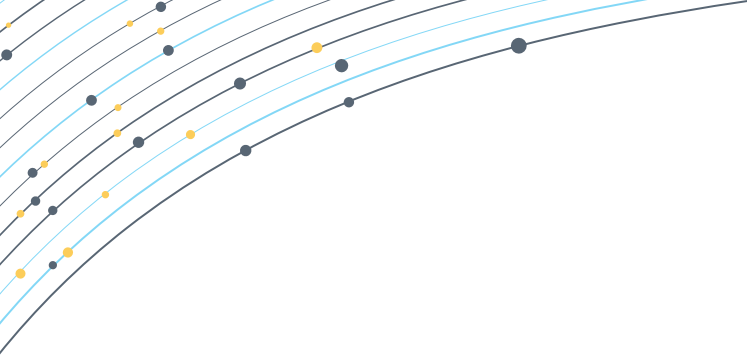


AUSTRALIAN
**CRIMINAL
INTELLIGENCE
COMMISSION**

Corporate Plan 2026–27

Covering reporting period 2026–27 to 2029–30





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

© Commonwealth of Australia 2026



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/.

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.

The document must be attributed
as the *Australian Criminal Intelligence Commission Corporate Plan 2026–27*.

ISSN: 2652-5844 (online)

CEO introduction



The Australian Criminal Intelligence Commission (ACIC) has a legislated mandate to combat serious and organised crime. We play a central role in protecting Australia from criminal exploitation by providing high-quality criminal intelligence that informs operational decision-making, shapes policy, and enables coordinated national responses across jurisdictions and sectors.

The serious and organised crime threat environment continues to evolve at pace. Criminal actors are increasingly transnational, technologically enabled and adaptive, exploiting vulnerabilities across borders, markets and communities. These threats do not respect jurisdictional or sectoral boundaries. Australia's response must therefore be intelligence-led, integrated and agile, underpinned by trusted partnerships and timely intelligence sharing.

This Corporate Plan sets out the ACIC's strategic direction over the next 4 years, reflecting a period of significant reform and organisational transformation. Building on the implementation of recommendations made by the Independent Review of the Australian Criminal Intelligence Commission and associated Commonwealth law enforcement arrangements (ACIC Review), the ACIC is strengthening its legislative foundation and maturing as a modern intelligence organisation. Our focus is on ensuring the agency is fit-for-purpose and positioned to deliver impact for government in a complex and dynamic operating environment, shaped by increasingly sophisticated organised crime networks.

Central to this effort is our role as a national integrator of criminal intelligence. The ACIC connects intelligence holdings across Commonwealth, state and territory agencies, the National Intelligence Community, law enforcement agencies, regulators and international partners, translating complex intelligence into actionable insight.

As agencies continue to be challenged by serious and organised criminals moving between jurisdictions and diversifying their criminal activities, we also have an important role in brokering access to policing and criminal information and intelligence holdings across Australia. The ACIC does this through its national policing information systems and services. In parallel, we are also strengthening engagement with the private sector, recognising the critical role industry plays in identifying and preventing serious and organised crime exploitation across key sectors of the economy.

Our people are fundamental to the ACIC's effectiveness. We are committed to building a skilled, diverse and professional workforce, supported by strong leadership, a values-based culture and a continued focus on wellbeing. By investing in capability and culture, we aim to be an employer of choice and a trusted partner across the National Intelligence Community and law enforcement.

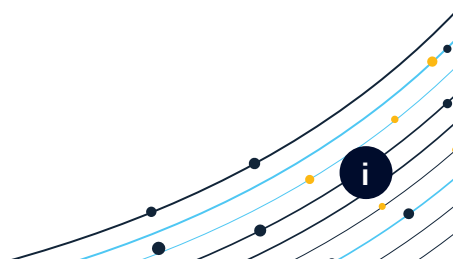
As the accountable authority of the ACIC, I am pleased to present the ACIC's Corporate Plan, prepared in accordance with paragraph 35(1)(b) of the *Public Governance, Performance and Accountability Act 2013*. This plan has been prepared for the 2026–27 reporting year and covers the 4-year period from 1 July 2026 to 30 June 2030.

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

13 July 2026



Contents

AGENCY OVERVIEW	2
Our role.....	2
Our organisation	2
OPERATING CONTEXT	4
Environment	4
Capability	5
Risk management	8
Cooperation	9
Performance.....	11
Performance framework.....	11
Key activities and performance measures	13
Appendix A – PGPA Act requirements.....	18

ACIC Corporate Plan 2026–27 to 2029–30

Our purpose

Our purpose is 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, which is annually updated and approved by the ACIC Board (see Figure 1).

Our key activities and intended results

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

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

To ensure that there are systems and services that enable criminal intelligence and policing information to be shared across jurisdictions, including the provision of nationally coordinated criminal history checks.

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

Our operating context



Enterprise capabilities



Agency overview

The Australian Criminal Intelligence Commission (ACIC) is Australia's national criminal intelligence agency. The ACIC provides intelligence to combat the threats Australia faces from serious and organised crime.

Our role

Our unique, actionable and insightful intelligence on serious and organised crime threats impacting Australia plays a critical role in bringing together intelligence, law enforcement, 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.

We play a crucial role in facilitating access to policing information and criminal intelligence holdings across Australia, through our delivery of 16 national policing information systems. This enables more than 72,000 police officers and other accredited users to undertake operational policing and intelligence activities that ensure community safety.

To help ensure the safety of the Australian community, we work with Australian police agencies and accredited bodies to deliver the National Police Checking Service. The service enables members of the community 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. Further information is in the Performance section.

Our organisation

The ACIC 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 the establishment and functions of the ACIC Board.

The ACIC Board is composed of agency heads from the Department of Home Affairs; Commonwealth, state and territory law enforcement bodies; and key regulatory and national security agencies. Its functions include providing strategic direction (see Figure 1), authorising special ACIC operations and special ACIC investigations, and determining priorities for the ACIC.

The Australian Criminal Intelligence Commission Bill 2026 (the Bill) was introduced into the House of Representatives on 25 March 2026 and is being considered by Parliament. Subject to its successful passage, the Bill will position the ACIC more effectively as an intelligence agency focused on serious and organised crime. It will support the ACIC to analyse and evaluate intelligence relating to serious and organised crime, share it faster, and maximise the use of this intelligence information enabling police partners to build operational strategies and coordinate disruption activities.

Figure 1: Strategic direction



Operating context

Environment

Serious and organised crime costs the Australian economy over \$82 billion per year¹, 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.

Serious and organised crime is a global, technology-enabled threat that undermines Australia's security, prosperity and community safety.

Developments in the serious and organised crime environment directly shape our intelligence collection priorities, strategies and challenges. 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 amplify their criminal capabilities and 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. This intelligence-led approach creates a significantly 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 and 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 grants criminals easier access to illicit commodities, digital currencies, specialist tools and expertise. Tools and methodologies are also commoditised by criminals across online forums and marketplaces.

1 Voce A & Morgan A 2025. The costs of serious and organised crime in Australia, 2023–24. Statistical Report no.55. Canberra: Australian Institute of Criminology. <https://doi.org/10.52922/78113>

- **Serious and organised criminals are operating and targeting Australia from offshore and online.** Operating offshore and in cyberspace, they are even harder to detect and disrupt. Many of Australia's highest threat criminal networks reside offshore, coordinating their activities remotely and at a distance from the hands of Australian law enforcement.
- **Criminal groups are enabled by insiders and professional facilitators.** Serious and 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 in masking and facilitating complex criminal activities.

Capability

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

Modern, integrated capability is essential to staying ahead of increasingly agile and sophisticated criminal networks.

Operating model

Our operating model defines how the agency will undertake its intelligence activities into the future and enhance our ability to:

- **target serious and organised crime and its enablers** – we have built dedicated intelligence mission management capabilities and commenced uplifting and enhancing our collection, analytics and assessment capabilities
- **harden the environment to serious and organised crime threats** – we have built an outreach program to engage industry, academia and the public to assist in hardening Australia's defences and building resilience against serious and organised crime
- **integrate data, technology and capabilities** – we are enhancing our enterprise-wide data capabilities to enable more efficient exploitation of agency and national data, and maturing our capabilities to combat threats, protect information and support frontline service delivery.

Our operating model sharpens mission focus, integrates capability and strengthens delivery against serious and organised crime.

People and culture

A capable, skilled and resilient workforce is central to achieving our purpose. Over the life of this Corporate Plan, we will focus on addressing critical skills gaps, strengthening our leadership talent, and improving recruitment and retention strategies. This remains essential as organised crime becomes more agile, technologically enabled and globally networked, placing increasing pressure on intelligence agencies to detect, analyse and respond to complex threats at speed.

Criminal groups continue to adopt emerging technologies, such as artificial intelligence, that accelerate the demand for advanced analytical, technical and investigative capability. In response, our workforce strategy remains sharply focused on targeted attraction, retention and development of skilled people.

Strategic workforce planning underpins this approach, which is informed by what our people are telling us, including feedback from employee surveys and exit interviews. Divisional people plans use these insights to focus on the capabilities the business needs now and, in the future, and to guide decisions about recruitment, development, movement of staff, and wellbeing.

Entry-level pathways will continue to improve, with programs that build intelligence capability through in-house assessment, clearer progression pathways, and a more joined-up approach to learning across the agency.

Broader Australian Public Service (APS) reforms continue to influence our capability direction. Embedding the APS Strategic Commissioning Framework remains a priority, and we will continue efforts to bring core work in-house in line with the framework. We expect our targets for 2026–27 to focus on reduced outsourcing of information and communications technology (ICT) solutions and portfolio program and project management.

Insights from the 2026 APS Employee Census will inform our actions to enhance leadership, inclusion and workforce wellbeing, supporting our broader retention and engagement objectives. Combined with secure and modern workplace technology, these initiatives position the agency to attract, develop and retain the skills required to deliver intelligence-led outcomes and stay ahead of increasingly sophisticated organised crime networks.

A skilled, resilient and future-ready workforce is critical to delivering intelligence-led outcomes in a rapidly evolving threat environment.

Intelligence and information

We deliver critical policing information and intelligence that keeps police officers and the community safe.

Timely, trusted intelligence and information sharing underpin effective policing and community safety.

Intelligence capabilities

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.

Specialist intelligence tradecraft delivers unique, actionable insights that enable targeted disruption of serious and organised crime.

National information sharing capabilities

We provide national policing information-sharing services to Australian police forces, intelligence partners and approved bodies, supported by technical assurance, system integrity and data quality controls. These services enable policing and investigative activity across jurisdictions.

The National Criminal Intelligence System (NCIS) connects data from Australian law enforcement agencies to provide a secure, national view of criminal intelligence and policing information. NCIS supports informed decision-making and enhances safety for frontline officers and the community.

Planned enhancements in 2026–27 will expand datasets and ensure NCIS continues to meet future national information-sharing requirements.

Checking service capabilities

Through the National Police Checking Service, we facilitate nationally coordinated criminal history checks in partnership with police agencies. This service supports community safety by enabling informed decisions about suitability for positions of trust and entitlements.

Accredited bodies access the service under strict contractual arrangements, supported by compliance, audit and education activities to maintain high integrity and reliability standards.

In November 2025, the Australian Government funded the delivery of the National Continuous Checking Capability. This capability will enable near real-time monitoring across jurisdictions of changes to the criminal history information of Working with Children Check and National Disability Insurance Scheme check holders, strengthening safeguards for children and vulnerable people.

Data and technology

Rapid technological change is creating new opportunities for the ACIC to harness diverse data sources and apply advanced analytical tools to generate timely, high-quality intelligence. For example, artificial intelligence tools enhance our intelligence, national policing information and police checking functions, supported by appropriate governance and oversight. These opportunities must be seized to ensure that we stay ahead of criminal organisations, which rapidly adopt and innovate with new technologies to support their criminal activity.

Strategic approach to data

The scale, diversity and complexity of the data underpinning our mission continue to grow, while serious and organised crime becomes more adaptive, networked and technologically enabled. This environment demands greater specialisation, agility and robust governance to ensure that we can responsibly leverage technology and convert data into actionable insights to respond to sophisticated criminal activities.

We will continue to invest in data management and analytics capabilities, supported by a skilled workforce, strong data governance foundations, high standards of data quality, strategic partnerships, and advanced technology.

Our data strategy provides the blueprint for this transformation. Aligned with our strategic direction, it sets the agency's priorities for building strong foundations, enhancing collaboration, maturing our data management practices and delivering sustainable, future-ready capability. These improvements will enhance the speed, reliability and impact of our intelligence, strengthening our ability to stay ahead of serious and organised crime.

Sustainable digital solutions

As a custodian of systems of government significance and national policing information holdings, the ACIC applies disciplined sustainment practices to ensure its digital products and services remain current and fit for purpose. These systems enable the timely delivery of criminal intelligence to domestic and international partners, as well as to public and private sector institutions.

Rising demand for intelligence and information services requires a clearer understanding of partner and end-user needs. That understanding informs targeted system enhancements as operational and policy requirements evolve. The agency's shift to user-centred, agile delivery and an integrated development–operations model strengthens responsiveness while improving cost control and resource allocation across the ICT portfolio. This approach supports productivity gains and more predictable delivery.

Stronger stakeholder engagement, ICT planning and release management are improving efficiency and accountability. These practices build confidence with stakeholders, support more deliberate prioritisation across workloads, and provide a clearer basis for seeking additional ICT resources where justified.

Digital roadmaps underpin the ACIC's multi-year ICT investment plan by linking agreed priorities to funding decisions and ongoing commitments. This approach supports a digital estate that both leverages existing government capabilities and delivers solutions built on reusable foundations. It positions the agency to meet emerging business needs, sustain existing investments, and retire end-of-life systems in line with the ICT Strategy.

Risk management

We foster a positive risk culture where staff confidently handle uncertainties and realise the benefits arising from opportunities. We engage with risk by applying sound risk assessment and management principles to empower managers and staff to make informed decisions which enable timely and appropriate action.

Our risk management policy and framework support the agency's accountable authority, the CEO, to meet her obligations under section 16 of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) in line with the Commonwealth Risk Management Policy. 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 2 of the agency's governance committees – the Commission Executive Committee and the Compliance and Risk Committee – and by the independent Audit and Risk Committee, which has specific responsibilities under the PGPA Act to review, and provide advice to the CEO on, the appropriateness of our systems of internal control, risk oversight and management.

In 2025–26, we matured our enterprise risk management reporting processes and prepared the agency's first enterprise-wide climate risk and opportunity assessment under the Commonwealth Climate Risk and Opportunity Management Program.

In 2026–27, we will continue to uplift the maturity of our control environment and further embed risk-based decision-making and practices in our day-to-day operations and governance arrangements, in line with our risk management framework.

Risk appetite and tolerance

We have a high-risk appetite in 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 to ensure that when risks are taken, they are understood, accounted for, and integrated into our plans and the way we operate. 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. Our internal governance arrangements allow for regular and active management and oversight of our policy settings and mitigations in critical areas of operation. There are 7 enterprise risks, as shown in Figure 2.

Figure 2: Enterprise risks and tolerances

	Legal and ethical Failure to adequately and ethically consider and treat legal risk and/or failure to comply with policy and statutory requirements.	Tolerance for legal and ethical risk is low. 
	Health and safety Failure to support the safety and wellbeing of workers and manage health and safety hazards presented by our varied operating environments.	Tolerance for health and safety risk ranges from low to high. 
	Security and integrity 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.	Tolerance for security and integrity risk is low. 
	Stakeholder Failure to plan for, establish and effectively manage and prioritise stakeholder relations, meet their requirements, and protect their interests and equities.	Tolerance for stakeholder risk ranges from low to high. 
	Technology and data Failure to implement, manage or secure the ACIC's data/services/systems/tools, including staying on top of emerging technology.	Tolerance for technology and data risk ranges from low to medium. 
	People and culture 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.	Tolerance for people and culture risk ranges from low to medium. 
	Finance and resources Failure to adequately manage financial requirements, contracts and procurement and prevent and detect financial fraud.	Tolerance for finance and resources risk is low. 

Cooperation

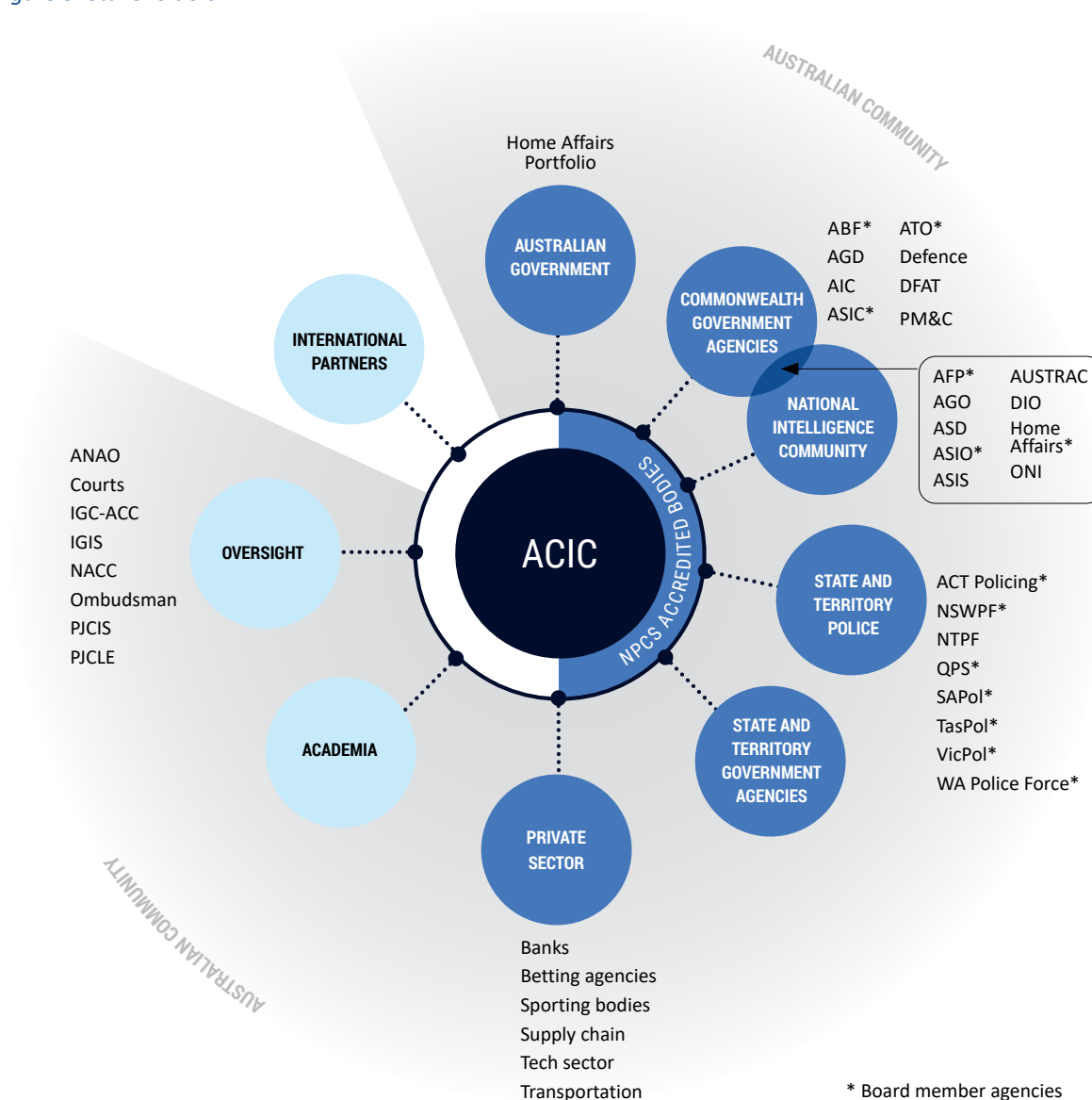
Reducing the impact of serious and organised crime involves cooperation across many government departments, intelligence, law enforcement and regulatory agencies and other entities, in Australia and overseas. Effective engagement is critical.

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.

Outside of the apparatus of government, we also engage with the community, academia and the private sector to foster strong working relationships to combat serious and organised crime and minimise harm to the community.

Figure 3 illustrates the connections between our key stakeholder groups.

Figure 3: 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 for our performance framework, presenting the complete suite of measures. We review our performance measures and their methodologies annually to ensure that they are robust and operationally relevant to our current practices, and they fulfil the requirements of section 16EA of the Public Governance, Performance and Accountability Rule 2014.

In this Corporate Plan we have further refined our suite of performance measures by removing last year's measure 1: Percentage of stakeholders that requested an additional intelligence product disclosure. The intent of this measure, showing the usefulness of ACIC intelligence, is part of, and more effectively reported through, the intelligence survey measure, previously measure 2 and now measure 1 for 2026–27.

Regulator performance

We are accountable to the government for our performance as the regulator of National Police Checking Service accredited bodies. As part of our regulatory approach, we adhere to the 3 principles of regulator best practice outlined in the Department of Finance **RMG128**:

1. Continuous improvement and building trust – Regulators adopt a whole-of-system perspective, continuously improving their performance, capability and culture to build trust and confidence in Australia's regulatory settings.
2. Risk-based and data-driven – Regulators manage risks proportionately and maintain essential safeguards while minimising regulatory burden, and leverage data and digital technology to support those they regulate to comply and grow.
3. Collaboration and engagement – Regulators are transparent and responsive communicators, implementing regulations in a modern and collaborative way.

Consistent with these principles, we continuously strive to enhance service delivery and build public trust, working transparently and responsively with our stakeholders accessing the National Police Checking Service to ensure that our approach to regulation is intelligence-led and proportionate to risk.

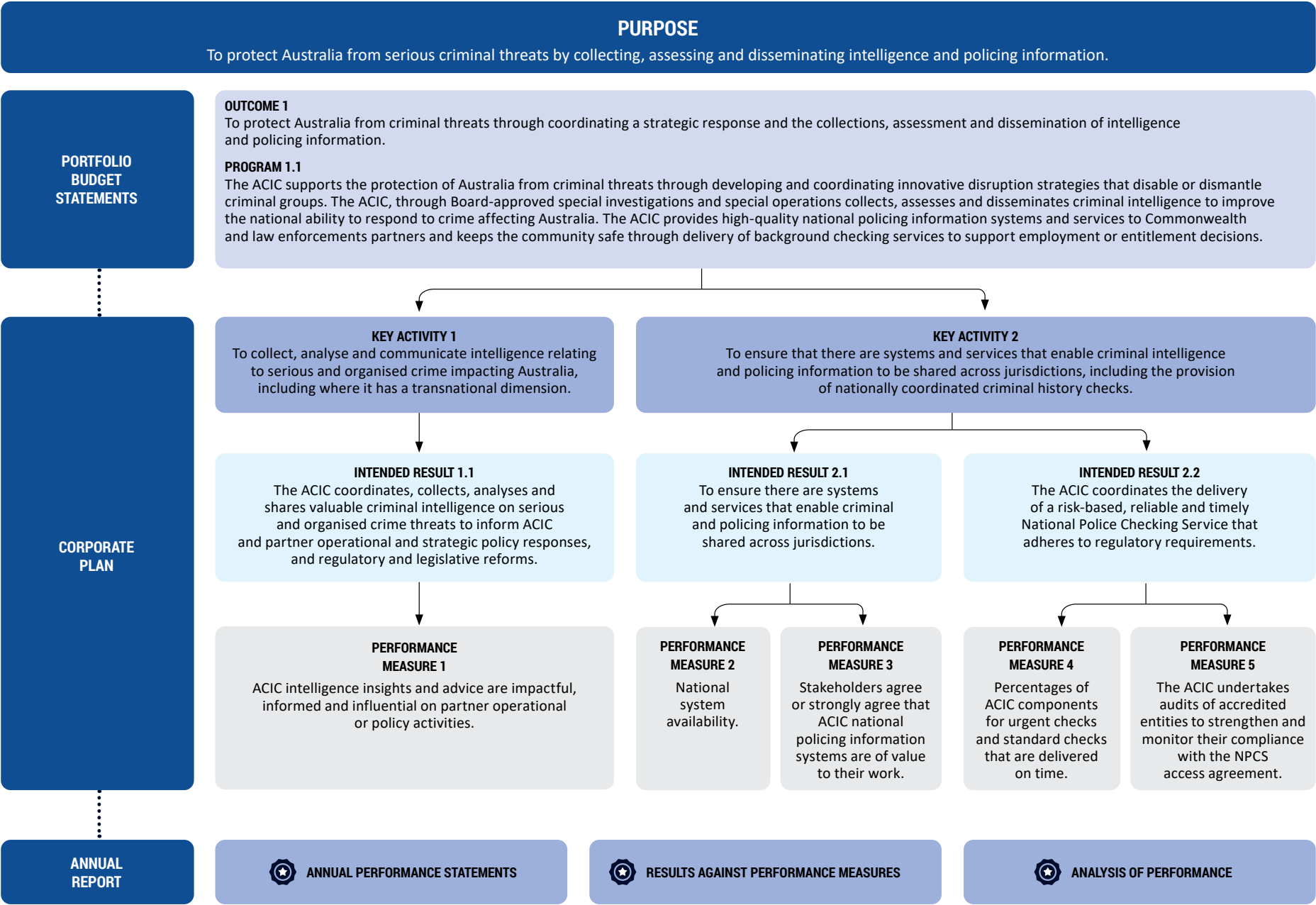
Best practice principles include:

Our current Ministerial Statement of Expectations sets the Australian Government's expectations for the National Police Checking Service and our alignment with the Government's productivity-oriented regulatory reform agenda. The ACIC Regulator Statement of Intent outlines how we plan to meet these expectations. Both documents are available at www.acic.gov.au/publications/corporate-documents.

Performance measure 5 is related to our regulatory function and aligns with the reporting requirements issued by the Department of Finance on **Regulator Performance**.

Figure 4 shows our performance framework for 2026–27, 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 4: Performance framework



Key activities and performance measures

In 2026–27, we will achieve our purpose and deliver our outcome through 2 key activities with 3 intended results. We will assess our achievement of the intended results through 5 measures, addressing targets as shown in the tables in this section.

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 1.1: THE ACIC COORDINATES, COLLECTS, ANALYSES AND SHARES VALUABLE CRIMINAL INTELLIGENCE ON SERIOUS AND ORGANISED CRIME THREATS TO INFORM ACIC AND PARTNER 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.

Intelligence is often an input to inform the actions of other agencies, for this reason this measure emphasises the value delivered for our partners and stakeholders.

Table 1: Performance measure 1

Measure				
ACIC intelligence insights and advice are impactful, informed and influential on partner operational or policy activities				
Target	2026–27	2027–28	2028–29	2029–30
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 better understand the usefulness of intelligence insights and advice.

Methodology

An annual survey is used to seek stakeholder views about the impact and value of ACIC products, analysis and advice on informing operational activity and policy.

The survey is sent to stakeholders who have dealt with the ACIC in a substantial way in the previous 12 months. The survey is conducted by an external consultant and the process is managed to ensure that responses are representative and that results are objective, independent and unbiased. The percentage of stakeholder satisfaction is determined by comparing the number of positive responses against the total number of responses.

Changes to measure

Measure 1 2025–26 was removed from the 2026–27 suite as this stakeholder survey measure includes an assessment of the usefulness of ACIC intelligence.

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

INTENDED RESULT 2.1: TO ENSURE THAT THERE ARE SYSTEMS AND SERVICES THAT ENABLE CRIMINAL INTELLIGENCE AND POLICING INFORMATION TO BE SHARED ACROSS JURISDICTIONS.

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.

Table 2: Performance measure 2

Measure				
National system availability				
Target	2026–27	2027–28	2028–29	2029–30
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 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 unscheduled national 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. Current benchmarks are:

Table 3: System availability benchmarks

System	Benchmark (%)
Australian Ballistic Information Network	95.00
Australian Firearms Information Network	98.50
Australian Law Enforcement Intelligence Network / Australian Criminal Intelligence Database: Desk	98.50
National Automated Fingerprint Identification System	99.50
National Child Offender System	99.50
National Criminal Intelligence System	99.90
National Criminal Investigation DNA Database	99.00
National Firearms Identification Database	96.00
National Missing Persons and Victim System	96.00
National Police Checking System Support System	99.00
National Police Reference System	99.50
National Vehicles of Interest System	99.00
Working With Children Checks National Reference System	98.70

Each system's individual result is calculated against its benchmark using the following matrix:

- met – the benchmark figure is reached or exceeded
- substantially met – 75%–99% of the benchmark figure is met
- partially met – 25%–74% of the benchmark figure is met
- not met – less than 25% of the benchmark figure is met.

The sum of all the individual system results is then calculated and assessed against the collective target of 'substantially met'.

Changes to measure

Nil.

Table 4: Performance measure 3

Measure				
Stakeholders agree or strongly agree that ACIC national policing information systems are of value to their work				
Target	2026–27	2027–28	2028–29	2029–30
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 NCIS 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

An annual survey is used to seek stakeholder views about the value gained from using the national policing information systems.

The survey is sent to stakeholders who have dealt with the ACIC in a substantial way in the previous 12 months. The survey is conducted by an external consultant and the process is managed to ensure that responses are representative and that results are objective, independent and unbiased. The percentage of stakeholder satisfaction is determined by comparing the number of positive responses against the total number of responses.

Changes to measure

Nil.

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.

The ACIC works with Australian police agencies and accredited bodies to deliver the National Police Checking Service, and has a regulatory role for accredited bodies. 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.

Table 5: Performance measure 4

Measure				
Percentages of ACIC components for urgent checks and standard checks that are delivered on time				
Target	2026–27	2027–28	2028–29	2029–30
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 timeliness 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 measure

Nil.

Table 6: Performance measure 5

Measure				
The ACIC undertakes audits of accredited entities to strengthen and monitor their compliance with the NPCS access agreement				
Target	2026–27	2027–28	2028–29	2029–30
Accredited bodies subject to an audit or compliance check per year	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 the Statement of Expectation and Intent and Australian Government Resource Management Guide 128 – Regulator Performance.

Methodology

The percentage is calculated as the number of active accredited bodies subject to audit or compliance checks, divided by the total number of active accredited bodies at 30 June. This is compared against the target of 10% or more accredited bodies being subject to audits or compliance checks each year. An 'active' accredited body is an accredited body that has undertaken a specified minimum number of checks during the financial year.

The 10% or more target adopts a risk-based approach in selecting entities and elements of the Agreement to audit. This allows the ACIC, as a regulator, to properly assess the risks of non-compliance and respond in a proportionate way to the harm being managed. It also supports the efficiency of the ACIC by directing audits or checks to entities of highest concerns. The measure supports the regulatory principle 2: being risk-based and data-driven.

The audit process also involves consultation and engagement with the accredited body during the audit, including meetings, and correspondence outlining the process, initial and final findings, and education to address issues through remedial action. Given this, this measure also supports principle 3: collaboration and engagement.

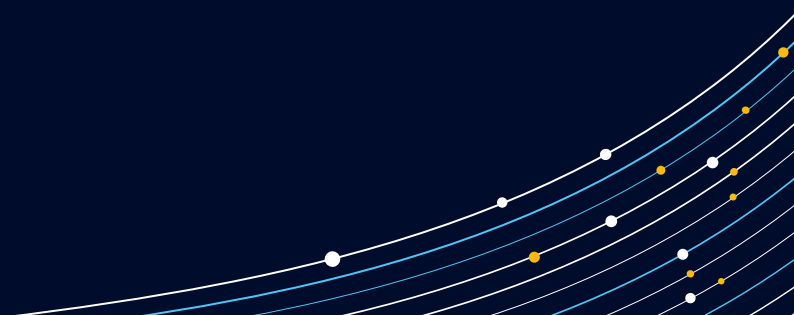
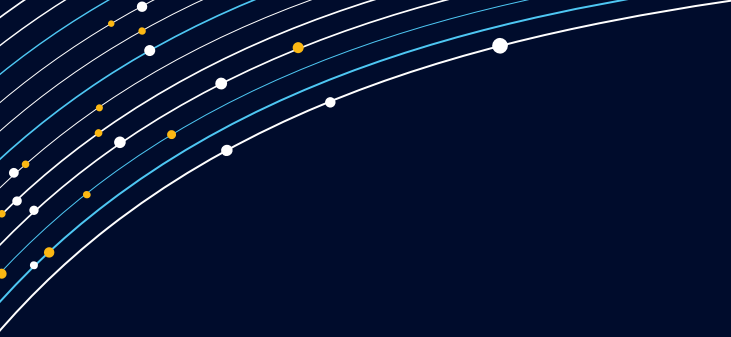
Changes to measure

Minor adjustment to wording from "the ACIC undertakes audits of accredited bodies and ensures their compliance with established timeframes".

Appendix A – PGPA Act requirements

The table below summarises the PGPA Act requirements for corporate plans, including page references for each requirement.

Requirement	Page(s)
Introduction	
• introductory statement	i
• the reporting period for which the plan is prepared	i
• the reporting periods covered by the plan	i
Purpose	1
Key activities	1
Operating context	4
• environment	4
• capability	5
• risk management	8
• cooperation	9
• subsidiaries (if applicable)	Not applicable
Performance	11



acic.gov.au