Australian Government
Australian Security Intelligence Organisation

ASIO 70TH 1949 2019

Corporate Plan
2019–20



D I G I

T A L

© Commonwealth of Australia 2019

All material presented in this publication is provided under a Creative Commons BY Attribution 3.0 Australia licence (http://creativecommons.org/licenses/by/3.0/au/deed.en).



The details of the relevant licence conditions are available on the Creative Commons website (accessible using the link provided) as is the full legal code for the Creative Commons BY Attribution 3.0 Australia licence (http://creativecommons.org/licenses/by/3.0/legalcode).

Use of the Coat of Arms

The Commonwealth Coat of Arms is used in accordance with the April 2014 *Commonwealth Coat of Arms: Information and Guidelines*, published by the Department of the Prime Minister and Cabinet and available online (http://www.itsanhonour.gov.au/coat-arms/index.cfm).

Contact us

Phone

General inquiries	02 6249 6299 or 1800 020 648
Business inquiries	02 6234 1668
Media inquiries	02 6249 8381

Email

media@asio.gov.au

Post

GPO Box 2176, Canberra ACT 2601

Contents

DIRECTOR-GENERAL'S INTRODUCTION 1

ASIO'S PURPOSE 4

OPERATING ENVIRONMENT 5

PERFORMANCE 7

KEY ENABLERS 9

RISK OVERSIGHT AND MANAGEMENT 18



Heather Cook

Deputy Director-General
Operations and Assessments Group

Duncan Lewis
AO DSC CSC

Director-General of Security

Peter Vickery

Deputy Director-General
Operational Support and Capability Group

Wendy Southern
PSM

Deputy Director-General
Strategic Enterprise Management Group

Director-General's introduction

I am pleased to present the *Australian Security Intelligence Organisation (ASIO) Corporate Plan 2019–20*, which covers the period 2019–20 to 2022–23, as required under paragraph 35(1)(b) of the *Public Governance, Performance and Accountability Act 2013*.

As we enter our 70th year, ASIO has much to be proud of. For seven decades, our Organisation has worked, albeit quietly, to protect Australia from violent, clandestine and deceptive efforts to harm its people and undermine its sovereignty.

Our work today is as vital as it was throughout the 20th century. While our adversaries have changed over the course of our history, the challenges posed by entities wishing to do harm to, or gain advantage over, Australia have not.

We are entering a new phase in our Organisation's history—one characterised by significant shifts in government and community expectations, advancements in technology and data, and evolving views on the balance between privacy and security.

We need to continue to transform how we do our work to take full advantage of the rapid technological advances disrupting our operating environment. We need to ingest and make sense of rapidly increasing volumes of data, and we need to establish a strong, digitally enabled culture in ASIO.

We must continue to partner closely across the public and private sectors to deliver effective security outcomes for Australia and Australians. We must also continue to do our work with integrity and propriety—and be seen to be doing so—to reinforce our position as a highly trusted public institution.

In recognition of these significant challenges, in 2018 we prepared the *ASIO Strategy 2018–23*. The strategy reframed our vision and purpose, and set out the steps we will take over the coming years to ensure we continue to evolve as a modern, sophisticated security intelligence organisation.

Our corporate plan for 2019–20 to 2022–23 adopts the vision, purpose and plans set out in the *ASIO Strategy 2018–23*. The plan:

- outlines ASIO's vision and purpose;
- describes the environment we will be operating in over the period of the plan;
- outlines our performance objectives and the ways we will assess our performance against those objectives;
- describes the key enablers required to achieve our purpose; and
- describes our approach to the management and oversight of risk.

Duncan Lewis AO DSC CSC
Director-General of Security

ASIO headquarters 1949–2019



Ben Chifley Building, Canberra (2013 to present)



Potts Point, Sydney (1949–51)



Queens Road, South Melbourne (1951–68)



469 St Kilda Rd, Melbourne (1968–86)



Russell Offices, Canberra (1986–2014)

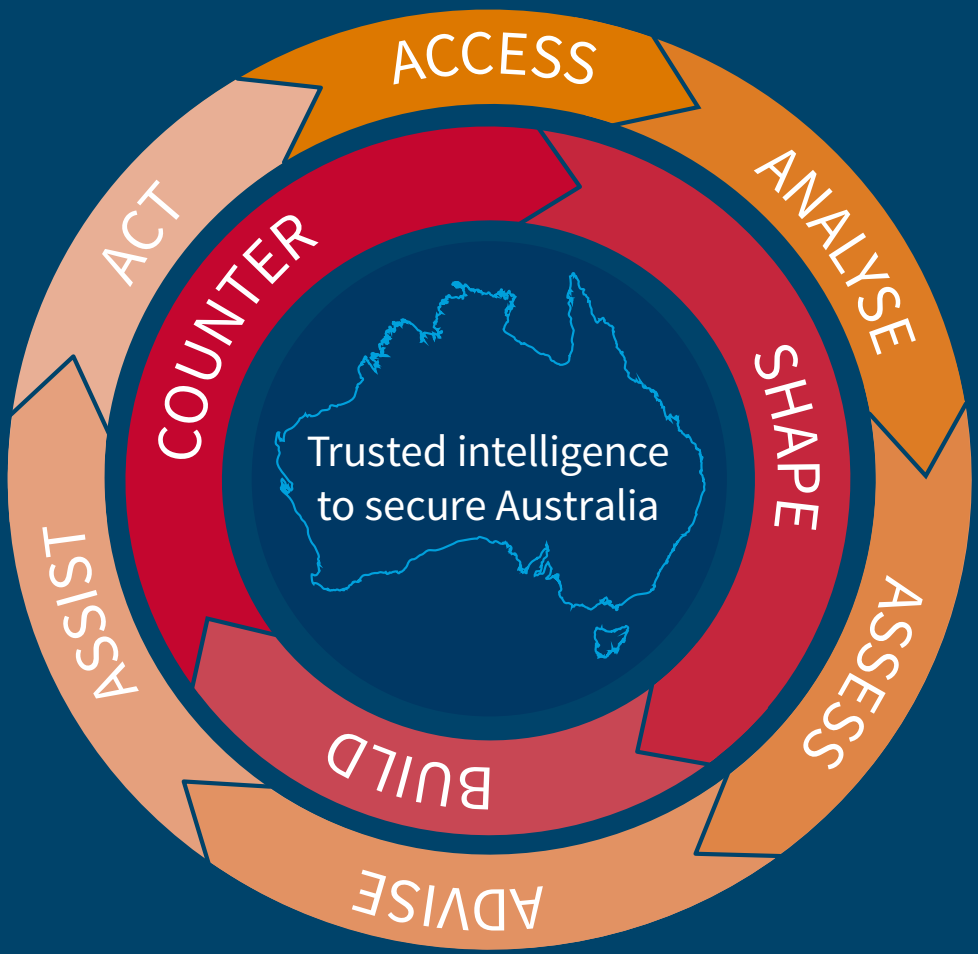
ASIO's purpose

Vision

Trusted intelligence to secure Australia

Purpose

As the nation's security service, ASIO protects Australia from violent, clandestine and deceptive efforts to harm its people and undermine its sovereignty.



Operating environment

ASIO operates in a challenging, rapidly evolving and somewhat uncertain security environment. Significant global shifts offer both challenges and opportunities.



Australia and its interests continue to be targeted by multiple sources at home and globally. This challenge is more complex and faster moving than ever before. The threat from terrorism continues at a high level. Furthermore, espionage and foreign interference—where foreign actors are seeking access to privileged and classified information, resources and innovation, and attempting to covertly influence the opinions of Australian communities, media representatives and government officials—is now occurring on an unprecedented scale.

Technological advancement—and the adoption and use of such advances by those intent on causing harm to Australia—is occurring at an extraordinary pace, and will continue into the future. We live in a data-rich world; and sophisticated, ubiquitous encryption renders traditional collection methodologies less productive. We must explore new ways to acquire, access and exploit data; employ the new tools and techniques that emerging technologies provide to us; and be ready to innovate and respond rapidly, to continue to address the security challenges Australia faces.



The increasing number of agencies involved in national security work has shifted expectations of how we operate. With the establishment of the Department of Home Affairs and the Office of National Intelligence (ONI), it is incumbent on us to better coordinate our efforts with our Home Affairs portfolio and National Intelligence Community partners. This presents us with new opportunities to strengthen our relationships to counter threats, develop security and intelligence capabilities across the Australian community, and make more direct contributions to advance the Australian Government's security-related policy objectives.

The current fiscal environment is placing significant constraints on our ability to sustain the level of security assurance previously provided to government. Costs, in all aspects of our work—people, infrastructure and operating expenses—continue to escalate, while the volume and complexity of our work also increases.

With multiple agencies working in an increasingly congested space, the demand for finite resources, including critical skills, exceeds supply. Our security clearance requirements, and inability to always compete with other employers' remuneration and conditions, create unique challenges in our recruitment.

Despite the various challenges and opportunities we face, the level of security assurance we are expected to provide to the people of Australia and their representatives—the federal parliament—remains as high as ever.

We will continue to rigorously prioritise our efforts in relation to those threats representing the greatest potential harm to Australians and Australian interests.

Performance

Throughout the period of this corporate plan, we will assess our performance in achieving our 'Counter, Shape and Build' strategic objectives in four 'key mission' areas: counter-terrorism; counter-espionage and foreign interference; border integrity, including people smuggling; and protective security advice.

Strategic performance objectives 2019–20 to 2022–23



COUNTER

We identify and mitigate violent, clandestine or deceptive efforts to harm Australians and compromise Australian sovereignty, economic well-being and national security.



SHAPE

We provide Australian governments, law enforcement and industry with intelligence and advice to enable better decision-making in relation to security responses, policies and priorities, including warning of emerging and imminent threats.



BUILD

We work with our Australian and international partners to build security and intelligence capabilities.

Key missions

Counter-terrorism

Counter-espionage and foreign interference

Border integrity, including people smuggling

Protective security advice

Performance assessment and reporting

Assessment method	When
Impact of our Counter, Shape and Build activities, including security outcomes and stakeholder feedback	Triannually by internal review
Performance against service-level agreements for security assessments	Triannually by internal review
Survey of stakeholders in federal, state and territory governments; national security and law enforcement agencies; and industry	Annually by independent senior reviewer
ONI evaluations	Annually by ONI
Assessment of overall performance against strategic objectives reported in annual performance statement contained in ASIO annual report to parliament.	

Performance reporting cycle

Corporate plan 2019—20	Triannual performance reporting	PBS 2020–21: performance forecast	Annual performance statement 2019–20	Annual report 2019–20
Set performance objectives	**Monitor performance**	**Forecast performance**	**Report on performance**	**Publish report on performance**
Corporate plan performance objectives approved by Director-General.	Intelligence Committee monitors performance throughout year, reporting triannually to the Executive Board.	Portfolio Budget Statement (PBS) performance forecast drawn from triannual reports for November 2019 and March 2020.	Annual performance statement drawn from triannual reports for November 2019, March 2020 and June 2020, and annual stakeholder survey.	Annual performance statement published in ASIO annual report to parliament 2019–20.
Performance objectives incorporated into divisional business plans.	Triannual performance reports provided to Executive Board in November 2019, March 2020 and June 2020.	Forecast approved by Director-General.	Approved by Director-General.	Annual report to be provided to Minister by 15 October 2020 for tabling in parliament.
Corporate plan commences operation on 1 July 2019.		PBS published with Budget (early May 2020).	Produced as soon as practicable at the end of 2019–20 reporting period.	
The Audit and Risk Committee reviews and provides independent advice to the Director-General on the appropriateness of ASIO's corporate plan performance objectives, triannual performance reports and annual performance statement.				

Key enablers

Eight key enablers provide the foundation for the continued delivery of our purpose and underpin our 'Counter, Shape and Build' services. We will progress a range of initiatives throughout the period of this plan to further develop and strengthen these enablers.

People and culture

Authorising environment and assurance

Security

Management of risk

Technology, capabilities and infrastructure

Information, data and systems

Governance

Strategic partnerships

People and culture



Our people have been, and will always be, the most important element of our success. To develop our people and culture we will:

- foster a collegiate and innovative workplace with agile, diverse, inclusive and expert staff, by embedding an approach which identifies future workforce skills and capability requirements, optimises our recruitment pipeline, and modernises our workforce planning practices;
- institute a unifying Organisational culture that centres on a commitment to our mission, builds on shared values, and recognises the contribution each employee makes to advancing our purpose;
- build leadership excellence within ASIO—and become a recognised source of national security leaders—by building on our comprehensive leadership program and consolidating the ASIO Leadership Charter in our policies, procedures and governance settings;
- cement adaptive leadership principles as keystones of our leadership culture; and
- in the context of our job family model, introduce Organisation-wide competencies and adopt a systematised approach to designing and delivering training programs to support staff in developing essential skills.

Indicators of success

- We have a safe, innovative, diverse and valued workforce, reporting high levels of job satisfaction and commitment to purpose.
- Our workforce is known for its security and intelligence expertise.
- A culture based on shared values—where all staff feel part of the 'ASIO community'—is evident in the Organisation, and modelled and fostered by our leadership.
- Our leaders are future and mission focused, enterprise minded, committed to people, and inclusive.
- We attract, develop and retain the specialist skill sets we need.

Authorising environment and assurance



Our authorising environment—and how we are regarded by the people of Australia, the parliament, the government, and our partners here and overseas—is critical to achieving our purpose.

To foster our reputation and reinforce our status as a trusted Australian institution we will:

- focus our services where they achieve greatest strategic impact, by identifying, mapping and understanding where we deliver public value, and determining where these services best connect to gaps and vulnerabilities across our security ecosystem;
- optimise our contribution to national security policy outcomes by enhancing our strategic engagement with key authorising entities, including ministerial offices, the Department of Home Affairs, ONI, the Department of the Prime Minister and Cabinet, and the Department of Finance;
- develop and communicate a unified and compelling corporate identity to enhance awareness of our function and value by the public and our partners; and
- adopt a coordinated approach to our outreach activities to convey consistent external communications to government agencies, academic and research institutions, influential corporate and community groups, and the media.

Indicators of success

- We enjoy the funding, support, information, collaboration, and/or legislative, policy and procedural amendments necessary to deliver on our purpose.
- Our unique status in Australia's national security architecture, and the value we provide, is accepted and supported.
- Our stakeholders understand who we are and what we do, and support us in undertaking those activities.

Security



Our embedded security culture is a positive for the Organisation—it keeps us safe and responsive in our work, and promotes resilience and integrity. Our commitment to protecting our people, sources and capabilities; our equities and those of our partners; and the sensitive information we hold, engenders trust, sustains our access to critical sources of intelligence, and promotes effective delivery of security intelligence outcomes.

To ensure ASIO is a safe and secure workplace, and protects the equities entrusted to us, we will:

- become a leading voice in promoting a positive security culture among Australian Government agencies and relevant industry sectors by coordinating and providing protective security guidance and expert threat reduction advice;
- enhance officer safety and security assurance, operational effectiveness and agility, and interoperability with key partners, by developing data-enabled technology solutions, including communications platforms and officer safety applications; and
- design and implement the policies, procedures and tools required to successfully operate multi-tiered information technology (IT) systems.

Indicators of success

- Security is not 'traded' for engaging with risk, nor is it used as an excuse for avoiding risk.
- ASIO is considered the expert in protective security matters, and is engaged with and used by government and industry partners.
- Our staff believe their safety is of utmost importance to the Organisation, and trust the measures implemented to provide this security.
- Our partners continue to collaborate and engage with us, and provide us with information, assistance and expertise.
- We have multi-tiered IT systems with minimal security breaches or long-running security concerns.

Management of risk



Risk is inherent to the operation of an intelligence agency. Over time, we have refined our operational risk practices to protect our people and equities and to ensure our resources are allocated to the highest priority threats to security. We need to do more, however, to ensure we apply a similarly mature approach to risk across all decisions in the Organisation.

To develop a sophisticated approach to engaging with and managing risk, we will:

- develop and implement a new enterprise risk framework;
- elevate awareness of our risk protocols and embed consistently high-standard risk management practices across the enterprise by investing in dedicated specialist resources; and
- develop and deliver tools to support staff in understanding and engaging with risk, including toolkits, training and coaching.

Indicators of success

- Our staff are empowered by policies and supported by their managers to make decisions, which they clearly articulate and record.
- Risk is managed at appropriate levels.
- Our staff understand the risk environment they operate in, and where the risk boundaries are for them.
- A culture of learning from ‘failure’ is established across the Organisation.

Technology, capabilities and infrastructure



To achieve our vision and deliver our purpose in a rapidly evolving environment, we must substantially transform to become an Organisation that is more agile and innovative. How we acquire, leverage, manage and govern technology, and how we build capability and infrastructure, will be key to this.

To engage with technology in new ways, and provide our future infrastructure needs, we will:

- identify our technology and infrastructure needs, prioritise our investments, maximise adoption of new technology and sustain our capabilities;
- preference agility and sustainability when acquiring technology; and
- promote the joint development of technical collection, surveillance and communications platforms, including providing support to multi-agency research and development facilities and increasing collaboration with industry partners.

Indicators of success

- Our project and procurement processes are driven by the principles of the preferencing of market acquisition, data- and risk-based prioritisation, and inception-to-delivery coordination.
- The time between the approval and delivery of new capabilities is reduced.
- We observe an improvement in internal customer satisfaction ratings and an increased rate of technology adoption across the Organisation.
- Our partners recognise our mature approach to technology and capability development, seek to work with us more closely, and observe increased efficacy in sharing data.
- Our engagement with members of the Australian technology industry is increased and enhanced.

Information, data and systems



We provide value to our partners and customers by synthesising and contextualising complex information. However, we bear a latent risk across the current systems we rely on to ingest, organise and make sense of our information. Many of our legacy systems were developed for discrete data sets and remain unintegrated. Increases in the volume, velocity and variety of data is further challenging us.

To improve our ability to ingest, organise and make sense of the information we collect, and communicate our insights to partners, we will:

- empower our chief data officer to develop and implement the strategic management of our information requirements, develop data standards, and optimise the use of our data holdings;
- partner with a commercial supplier to acquire a core data platform;
- invest in augmented decision-making technology, which is supported by training and initiatives to optimise its adoption and continuing use, and governing protocols;
- develop and implement robust, principles-based rules for cross-domain activity; and
- institute a data culture to optimise the value we derive from data.

Indicators of success

- Automation and artificial intelligence technologies have been adopted, where appropriate, to support business activities across the Organisation.
- Staff report increased satisfaction in accessing and organising information in support of decision-making.

Governance



To deliver our 'Counter, Shape and Build' services effectively, we need to be adaptive and flexible, understand and navigate risk in a sophisticated manner, prioritise activities, and rapidly reallocate resources to address emerging challenges and exploit opportunities.

We will reform the Organisation's operating and governance models so we can better respond to change and deliver effective and informed prioritisation, resourcing and investment decisions by:

- designing and implementing a new enterprise-wide operating model to embed agile methods of working and data-driven decision-making, and allow the rapid allocation of assets and resources across the Organisation;
- reforming governance architecture to reinforce accountability practices; promote decision-making effectiveness, legality and propriety; and determine and oversee Organisational capability development and expenditure; and
- ensuring our Portfolio Management Office has the capability to prioritise, coordinate and optimise the delivery of high-value projects and procurement initiatives.

Indicators of success

- Decision-making is structured and robust and keeps us ahead of changes in the security and operating environments.
- We are able to pivot quickly and adopt new technologies with ease.
- We identify ways to better engage partners when significant change occurs in the authorising environment.
- Our governance structure has defined decision points, and committee members act with discipline in all matters.
- Our governance models ask the right questions, and provide the reassurance that staff and our stakeholders require.

Strategic partnerships



We will elevate our engagement with partners beyond transactional 'customer-service' relationships towards more enduring and strategically beneficial partnerships. We will work with our partners to develop a deep understanding of each party's needs and objectives, and identify and work towards common goals.

To elevate our engagement with partners, we will:

- adopt a strategic approach to developing and sustaining our suite of partnerships, which is delivered by investing in systems and practices for managing strategic relationships, and refined by rigorous evaluation and prioritisation; and
- expand the modalities through which we partner, including briefings, secondments, outsourcing and in-sourcing, and increased collaboration and liaison with industry sectors.

Indicators of success

- Our partners have a greater awareness of our niche capabilities, expertise and position in the National Intelligence Community.
- We have an enriched understanding of what we can provide to our partners, and what our partners can provide to us.
- We find means of providing advice to our partners that are suitable for us and practical for our partners.

Risk oversight and management

Our Executive Board is the primary advisory committee that supports the Director-General in the governance of the Organisation. The board oversees our risk management policies, including the identification and treatment of key strategic Organisational risks. The board determines whether our overall level of risk is acceptable and considers whether our risk management structures, systems and processes remain effective and support the achievement of our purpose.

The Director-General established the Audit and Risk Committee (ARC) in compliance with section 45 of the *Public Governance, Performance and Accountability Act 2013*. The ARC's role is to provide independent assurance and advice to the Director-General and the Executive Board on the design, operation and performance of ASIO's internal governance, risk and control framework; performance reporting; and compliance with our internal and external accountabilities and responsibilities. The ARC has four external members, including an external chair.

During the period of this corporate plan, we will implement a new enterprise risk framework and other initiatives to identify, measure and manage risks and opportunities—including through ensuring legal compliance, acquiring and adopting technological capabilities, and prioritising resources.

TRANSFORMATION

