

Australian Government

Australian Security Intelligence Organisation

CORPORATE PLAN

2022–26

ASIO

Securing Australia—protecting its people

© Commonwealth of Australia 2022

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

Director-General's introduction

I am pleased to present the ASIO 2022–23 Corporate Plan, which covers the period 2022–23 to 2025–26, as required under section 35(1)(b) of the *Public Governance, Performance and Accountability Act 2013*.

ASIO protects Australia and Australians from threats to their security. Our corporate plan sets out how ASIO will fulfil this purpose and how we will measure our performance.

The security environment remains complex, challenging and changing.

Threats to our way of life

Espionage and foreign interference has supplanted terrorism as our principal security concern. The scale, scope and persistence of espionage and foreign interference threats is outpacing terrorism threats, demanding more attention and resources.

The threat is pervasive and multifaceted, and has the potential to seriously damage our sovereignty, values and national interest.

Multiple countries are seeking to conduct espionage against us, seeking information about Australia's strategic capabilities, economic and policy priorities, research and development, and defence technologies.

Looking ahead, we expect hostile foreign powers and their proxies to aggressively seek information on AUKUS, the Quad and their associated initiatives.

Foreign governments remain determined to interfere in Australia's democracy and undermine our sovereignty.

We see this primarily manifesting in the harassment of diaspora communities, and attempts to shape political and business decision-making to the foreign government's advantage.

These attempts are occurring in all states and territories, at all levels of government, on all sides of politics and in the private sector.

While attempts to interfere in our democratic processes are common, successful interference is not.

Threat to life

Threat to life will always remain a priority for ASIO. This threat is enduring.

Australia's national terrorism threat level is **PROBABLE**, indicating that individuals and groups have the intent and capability to conduct a terrorist attack in Australia.

The most likely terrorist attack scenario in Australia continues to be a lone-actor attack without warning and using a rudimentary weapon such as a knife or vehicle.

Ideologically motivated extremists are now a permanent feature of our security environment.

ASIO's purpose

ASIO protects Australia and Australians from threats to their security.



Nationalist and racist violent extremists continue to radicalise and recruit new members, and we are seeing a distinct increase in specific-issue grievances. Specific-issue violent extremists are being motivated by a cocktail of grievances, including anti-vaccination agendas, conspiracy theories and anti-government sovereign citizen beliefs.

It is important to reiterate that ASIO does not investigate peaceful protest or dissent—we are focused on a small number of angry and alienated Australians, those who advocate acts of violence or the promotion of violence.

In 2021, there were two domestic terrorist attacks and two major disruptions of violent extremist attacks. Globally, violent extremist attacks remain a frequent occurrence and the transnational nature of terrorism means that events across the globe can reverberate close to home.

Unfortunately and alarmingly, increasing numbers of young Australians are being radicalised. Children as young as 13 are now embracing extremism, and this is happening with religiously motivated violent extremism and ideologically motivated violent extremism. A majority of this radicalisation occurs online. At the end of last year, on average, minors represented more than half of our highest priority counter-terrorism investigations each week.

ASIO's response

ASIO is managing these threats by investing in our people, partnerships and capabilities.

Our people are our most important asset. ASIO's continued success relies on the ingenuity and agility of our team. We are actively seeking to recruit and retain talented individuals, and we encourage and foster innovation and leadership at all levels. I want ASIO to reflect the diversity of the community we protect and am committed to taking practical steps to achieve it.

Security is a shared responsibility. ASIO's mission is enabled by our strong partnerships with the National Intelligence Community, law enforcement, state, territory and federal governments, industry, academia and our international counterparts.

The scale and sophistication of the threats facing Australia requires ASIO to be proactive in our advice to our partners. We will leverage our capabilities, insights and expertise to help stakeholders better understand, identify and manage threats.

Image (left to right)

Ewan Mcmillan	Deputy Director-General Vetting Service Delivery Group
Chris Teal	Deputy Director-General Intelligence Service Delivery Group
Hazel Bennett	Deputy Director-General Enterprise Service Delivery Group
Mike Burgess	Director-General of Security



ASIO continues to invest in cutting-edge technical capabilities. The allocation of $1.25 billion over 10 years announced in the 2021–22 Budget will ensure we remain well equipped to defeat hostile nation states that are effectively unconstrained by resources, ethics and laws, and violent extremists who are embracing encryption and other technologies to avoid detection. We will partner with the Australian tech industry to advance this capability uplift, adopting a human-led, data-driven, technology-enabled approach.

Conclusion

ASIO does not just do what is legal, we do what is right. Our mission depends on the continued trust, confidence and understanding of government, our partners, and the Australian people. This is why, as Director-General, I embrace rigorous oversight, transparency and compliance.

The corporate plan and its performance measures are critical components of this accountability agenda.



Mike Burgess
Director-General of Security

ASIO Corporate Plan 2022–26

PURPOSE

ASIO protects Australia and Australians from threats to their security.

KEY PRIORITIES

COUNTER–ESPIONAGE AND FOREIGN INTERFERENCE

Protecting Australia from espionage and foreign interference



COUNTER–TERRORISM

Protecting Australians from violent extremism



INFLUENCE AND IMPACT

Leveraging our capabilities and insights to help stakeholders better understand, identify and manage sophisticated threats



ENABLERS

PEOPLE AND LEADERSHIP

ASIO's people are fundamental to our business, and our culture enables their success. Given the complexity of our work, we emphasise the value of leadership at all levels. We recognise the importance of attracting, developing and retaining our diverse and talented workforce, and empowering and supporting our staff to achieve their full potential.



SECURITY

ASIO outcomes are enabled by the importance we place on security—protecting our people, our partners and our capabilities. As Australia's security service, we adapt and lead in developing security practices and by building a security vetting capability to provide assurance in a complex, challenging and changing security environment.



TRUST

Our ability to deliver our purpose requires us to maintain the confidence and trust of our stakeholders, including the Australian people. This trust is fostered through good practices and by delivering demonstrated effects and outcomes. Transparency is a precursor for trust. ASIO recognises it has a responsibility to be as open as possible about what we do and why we do it.



CONTEXT AND EXTERNAL DRIVERS

Evolving threat environment



Geopolitical shifts



Technology advancement



CAPABILITY

Accelerating and sustaining our ability to achieve our purpose, deliver against priorities, and be positioned to meet future challenges through a human-led, data-driven and technology-enabled approach to capability

RISK AND COMPLIANCE

Delivering outcomes by responsibly engaging with risk while operating with integrity and in compliance with the law

TECHNOLOGY AND DATA

ASIO delivers value by making sense of complex data and information. We will navigate developments in the threat environment by embracing new technology and seizing opportunities to innovate, including working with Australian technology partners. Our imaginative and curious workforce are essential to our success.

GOVERNANCE

ASIO's governance practices allow us to act with authority, establish disciplined business processes and demonstrate accountability. Our governance enables informed planning, operational decision-making and prioritisation, strong oversight, and assessment and adjustment, while also ensuring the effective and efficient use of resources.

Partnerships

Community expectations

Labour market conditions



ASIO's context and external drivers

ASIO continues to operate in a complex, challenging and changing security environment. ASIO's success relies on our ability to understand the environment, identify and understand the threats it presents, and convert this understanding into actionable insights and impactful advice.

Evolving threat environment

Foreign interference and espionage activities within Australia, and against Australian interests, remain pervasive and enduring. We continue to observe attempts at foreign interference across all levels of government, and in every state and territory. Foreign powers and their intelligence agencies continue to target government, defence, academia and industry to steal classified information, military capabilities, policy plans and sensitive research. Clandestine, deceptive and threatening activities of foreign states can undermine Australia's national security and sovereignty by interfering in our democratic institutions, inflicting economic damage, degrading and compromising assets and infrastructure, and threatening the safety of Australians. In the years ahead, we expect to see a greater confluence of these threats, impacting how we investigate and respond to an increasingly complex security environment.

The nature of violent extremism continues to evolve and present new challenges. The threat of religiously motivated violent extremism persists, with individuals and groups espousing violent narratives and inspiring attacks around the world, including in Australia. Ideologically motivated violent extremism—inspired by a range of grievances—is increasingly present in Australia. Adding further complexity to this threat environment, increasing numbers of young people are being radicalised toward extreme ideologies. This radicalisation predominantly occurs online. This trend will continue to shape the need for nuanced and appropriate policy and responses from government, law enforcement, and the community more broadly.

Australia's border security is likely to be impacted by global factors including economic, security and health conditions. The relaxing of international border restrictions and resumption of international travel following the height of the COVID-19 pandemic will impact Australia's border security environment.

Geopolitical shifts

Geopolitical strategic shifts will continue to be a significant driver of Australia's security environment. Global power dynamics and the impacts of foreign conflicts, health and economic crises—as well as political polarisation and nationalism—will continue to shape and challenge Australia in complex ways.

Major power competition has intensified and will continue to impact the security environment. This competition, and any resulting challenges and changes to the international order, will produce a more uncertain security environment for Australia. Broader Australian Government efforts to promote and build a resilient Indo-Pacific—in particular, the development of the Quad and a nuclear-powered submarine program through the AUKUS trilateral security pact—will present a range of security opportunities and challenges.

In addition to these challenges, we can expect to see evolving and varied security challenges as a result of climate change and global competition for resources over the next decade.

Technology advancement

Rapid technological changes and ever-increasing volumes of data will continue to be a feature of our operating environment. These changes increase the complexity of the threats to security and the scope of our vulnerabilities. We have observed our adversaries using encryption and secure communications platforms to hide their capability, intent and motivations. These challenges will only increase in coming years.

Responding to these challenges by building and maintaining our underlying capabilities is critical for ASIO. In 2021, ASIO received an unprecedented ten-year investment of $1.25 billion to advance our technology capabilities. Leveraging opportunities in technology-enablement and automation will allow ASIO to operate at the speed and scale necessary to detect and respond to threats as they emerge. The successful delivery of this program is critical for ASIO to deliver on its purpose and to be ready for the challenges of the future.

Notably, the AUKUS agreement will provide future opportunity to shape and progress the technology landscape in Australia in relation to artificial intelligence, research and innovation, and other advanced technologies such as quantum and cyber capabilities.

Partnerships

Australia's security is a shared responsibility. Strong partnerships are instrumental for ASIO to deliver its mission. These relationships span across government, including the National Intelligence Community, our state and territory law enforcement partners, international counterparts, industry, academia, and the Australian public.

ASIO's partners are mission enablers who are vital for ASIO to identify and resolve threats to security. They provide insights that inform and enhance our advice and decision-making. In turn, we share our unique expertise to advance our collective goals. This teamwork is critical, and we perform better collectively when we draw on each other's capabilities and strengths.

To respond flexibly to changes in our security environment, we will continue to deepen our relationships across industry and academia. This engagement helps us to innovate and adapt by providing unique perspectives and insights into new and emerging threats and capabilities.

The importance of ASIO's partnerships will only increase as Australia's security environment evolves.

Community expectations

As Australia's security service, ASIO relies on the continued trust of Australians. We are as transparent about our activities as possible—while protecting our sensitive capabilities—and we are committed to strong, independent oversight.

ASIO's accountability framework includes oversight by the Inspector-General of Intelligence and Security, who has powers akin to a Royal Commission. This is something we welcome, because independent and rigorous oversight is critical to maintaining the trust of our stakeholders, including the Australian public.

We act in a targeted, proportionate and ethical way. Wherever possible we use the least intrusive method available to collect security intelligence. We do not just do what is legal, we do what is right.

Labour market conditions

Attracting, developing and retaining talent will be a key focus for ASIO in the coming years. We continue to compete with government and industry and will need to explore new ways to demonstrate we are an employer of choice. In an already highly contested labour market, we operate in an environment with additional complexities and unique requirements to protect our people, information and capabilities.

Attracting individuals with the right skill sets will see us recruiting more creatively and leveraging circumstances presented by people looking for new or different career opportunities. Developing and retaining our talent will see us thinking more flexibly about our workforce model, people management policies and operating environment.

Key priorities and performance objectives

ASIO will advance its purpose for the period 2022–26 through five priorities.

Two of these priorities—counter–espionage and foreign interference, and counter-terrorism—form ASIO's key activities. Border security will continue to be delivered through the provision of analysis and security advice that supports whole-of-government efforts to protect Australia's border integrity—through the lens of our counter-espionage and foreign interference and counter-terrorism activities.

This mission focus is enabled and bolstered by three further priorities—influence and impact, our capability program, and our attention to engaging with risk and ensuring compliance. The introduction of influence and impact as a key priority demonstrates the strategic importance we place on maximising the effect of our advice and insights.

ASIO's performance against these five priorities will be measured through a combination of quantitative and qualitative methods, including defined targets, case studies, stakeholder feedback, and identified milestones. ASIO will continue to progressively refine our performance measures to ensure we demonstrate our effectiveness in a transparent way, while safeguarding our sensitive capabilities and tradecraft.

Counter–espionage and foreign interference

ASIO will protect Australia by countering espionage and foreign interference from foreign intelligence services. We will collect intelligence and investigate to uncover and understand threats to Australian government, defence, political and other national interests. Over the period of this corporate plan our intelligence will shape government decisions and inform tactical operations to thwart espionage and foreign interference. Our impactful and trusted advice to government and industry will raise awareness of the threat and establish a less permissive environment for covert actors. We will work with partners to disrupt and deter those attempting to undermine our national interests.

Counter-terrorism

ASIO will counter terrorism by protecting Australians from religiously motivated and ideologically motivated violent extremism. Prioritising our resources against the greatest threats, the Organisation will continue to collect intelligence within Australia and overseas, analyse and investigate terrorist threats, and work with partners to strengthen public safety and intervene to disrupt attacks.

Our intelligence collection, investigation and assessment efforts enable ASIO to identify and understand the threats we face, and to provide impactful advice that hardens the environment against, and informs government policy and responses to, violent extremism. Over the period of this corporate plan, we will continue to deliver impactful, relevant and practical advice to assist stakeholders in their counter-terrorism decision-making. Our advice will enable our stakeholders and partners to harden the environment and disrupt violent extremist activities.

Influence and impact

The scale and sophistication of the threats facing Australia requires ASIO to be proactive in its advice to government and industry. ASIO will leverage our capabilities and insights to help stakeholders better understand, identify and manage security threats. We will promote security awareness and strengthen security maturity by providing expert insights and impactful advice.

Capability program

Our human-led, data-driven and technology-enabled approach to capability will help us to accelerate and sustain our ability to achieve our purpose, deliver against priorities, and position us to meet future challenges. Our capability delivery program will keep ASIO ahead of technological change and maintain our ability to identify and respond to threats. ASIO will continue to invest in, and sustainably adopt new technology, commercial platforms and tradecraft practices to deliver security outcomes for Australia and Australians. We will continue to partner with the Australian technology sector in the development of sovereign capabilities in key areas of national security, and engage with international partners to share and leverage benefit from collective innovation and action.

Risk and compliance

Maintaining an appropriate system of risk oversight and management and accepting and engaging with risk is inherent to our role to protect Australia and Australians from threats to their security. In a complex security environment, our risk and compliance frameworks ensure we are applying sophisticated risk management practices to identify, evaluate and respond to risks and opportunities. The shared understanding of risk leads to well-informed decision-making and effective prioritisation.

ASIO acts to the letter, and in the spirit, of the law. ASIO officers act with integrity. We are impartial, committed to our purpose, and operate ethically and with propriety. Our frameworks support our compliance with the law and enable dynamic responses to an evolving threat environment.

Performance measures

Impact definitions*—the definitions to be shared with key stakeholders when determining what level of impact our advice has had on their decision-making.

LOW	MEDIUM	HIGH
Our advice provided little or no context, and did not influence your decision-making.	Our advice provided context; was relevant and practical; and influenced your decision-making.	Our advice was timely and relevant; practical, focused and provided or enabled exercisable options; and directly informed and shaped your decision-making.

Advice—for the purposes of this performance framework, 'advice' encompasses all forms of communication—to the Australian Government, government agencies, and industry and community sector stakeholders—that conveys ASIO's expertise, intelligence, assessments, priorities and recommendations on security matters.

**Impact definitions relate to counter–espionage and foreign interference and counter-terrorism measures.*

Counter–espionage and foreign interference

1. Impact of operational activities advice

Measure	The percentage of key stakeholders who confirm our counter-espionage and foreign interference advice had a HIGH impact on their decision-making in informing counter-espionage and foreign interference operational activities, managing security risks and disrupting activities that threatened Australia's security.			
Targets (% and impact level)	2022–23 80% HIGH	2023–24 80% HIGH	2024–25 80% HIGH	2025–26 80% HIGH
Rationale	ASIO's advice to partners within government, the national security community, industry and community sectors provides the knowledge and understanding that enables them to respond appropriately to security threats.			
Methodology	Assessment of the impact is drawn from stakeholder feedback throughout the year, including the annual survey of key stakeholders. Stakeholders are: ■ drawn from relevant federal, state and territory governments, and private enterprise; ■ ongoing, frequent recipients of ASIO counter–espionage and foreign interference advice; and ■ engaged in counter-espionage and foreign interference operational activities, managing security risks, and/or disrupting espionage and foreign interference activities that threaten Australia's security.			

2. Impact of policy development advice

Measure	The percentage of key stakeholders who confirm our counter–espionage and foreign interference advice had a HIGH impact on their decision-making in relation to specific and relevant espionage and foreign interference policy development and responses to this threat.			
Targets (% and impact level)	2022–23 80% HIGH	2023–24 80% HIGH	2024–25 80% HIGH	2025–26 80% HIGH
Rationale	ASIO's advice to partners within government, the national security community, industry and community sectors provides the knowledge and understanding that enables them to respond appropriately to security threats.			
Methodology	Assessment of the impact is drawn from stakeholder feedback throughout the year, including the annual survey of key stakeholders. Stakeholders are: ■ drawn from relevant federal, state and territory governments, and private enterprise; ■ ongoing, frequent recipients of ASIO counter–espionage and foreign interference advice; and ■ engaged in developing relevant policy responses to the espionage and foreign interference threat.			

Counter-terrorism

3. Impact of operational activities advice

Measure	The percentage of key stakeholders who confirm our counter-terrorism advice had a HIGH impact on their decision-making in relation to informing counter-terrorism operational activities, managing security risks and disrupting activities that threatened Australia's security.			
Targets (% and impact level)	2022–23 80% HIGH	2023–24 80% HIGH	2024–25 80% HIGH	2025–26 80% HIGH
Rationale	ASIO's advice to partners within government, the national security community, industry and community sectors provides the knowledge and understanding that enables them to respond appropriately to security threats.			
Methodology	Assessment of the impact is drawn from stakeholder feedback throughout the year, including the annual survey of key stakeholders. Stakeholders are: ■ drawn from relevant federal, state and territory governments, and private enterprise; ■ ongoing, frequent recipients of ASIO counter–terrorism advice; and ■ engaged in counter-terrorism-related operational activities, managing security risks, and/or disrupting terrorism-related activities that threaten Australia's security.			

4. Impact of policy development advice

Measure	The percentage of key stakeholders who confirm our counter-terrorism advice had a HIGH impact on their decision-making in relation to specific and relevant policy development and responses to terrorism.			
Targets (% and impact level)	2022–23	2023–24	2024–25	2025–26
	80% HIGH	80% HIGH	80% HIGH	80% HIGH
Rationale	ASIO's advice to partners within government, the national security community, industry and community sectors provides the knowledge and understanding that enables them to respond appropriately to security threats.			
Methodology	Assessment of the impact is drawn from stakeholder feedback throughout the year, including the annual survey of key stakeholders. Stakeholders are: ■ drawn from relevant federal, state and territory governments, and private enterprise; ■ ongoing, frequent recipients of ASIO counter–terrorism advice; and ■ engaged in developing relevant policy responses to terrorism.			

Influence and impact

5. Delivery of impactful intelligence and advice

Measure	Case studies which demonstrate the delivery of impactful intelligence and advice, resulting in an operational outcome or policy reform.			
Targets	2022–23	2023–24	2024–25	2025–26
	≥ 1	≥ 1	≥ 1	≥ 1
Rationale	The scale and sophistication of the threats facing Australia require ASIO to be proactive in its advice to government and industry. ASIO will leverage our capabilities and insights to help stakeholders better understand, identify and manage security threats. We will promote security awareness and strengthen security maturity by providing expert insights and impactful advice.			
Methodology	Case studies are provided by ASIO's intelligence delivery areas on a triannual basis for internal performance tracking. These case studies demonstrate the impact of ASIO's intelligence and advice for our stakeholders. Case studies will be chosen on the basis of their demonstration of the impact of ASIO assessments and advice with consideration to protecting sensitive tradecraft, capabilities and information.			

ASIO capability program

6. ASIO capability delivery

Measure	The capability program delivers mission effects and outcomes through achieving deliverables consistent with capability program objectives and milestones.
Targets	2022–26 Qualitative and quantitative measures demonstrate delivery of capability program milestones across the period of this corporate plan.
Rationale	ASIO operates in a complex threat environment made more challenging by the rapid pace of technology advancement. The capability program will improve the Organisation's capacity to future-proof its ability to respond to these challenges and help protect Australia and Australians from threats to their security. This will be achieved through enhancing and sustaining capabilities to detect and disrupt adversaries including through analysis and processing of complex data.
Methodology	Qualitative and quantitative analysis of the capability program will be informed via a range of inputs, including internal program governance, assessment of benefits realisation, staff feedback, the development of key enabling partnerships, the onboarding of capability-related resources, and other program delivery metrics such as budget and time frame.

Risk and compliance

7. Risk management framework

Measure	ASIO's risk management framework, culture and practices are consistent with the requirements of the Commonwealth Risk Management Policy.
Targets	2022–26 Adherence to the requirements of the Commonwealth Risk Management Policy in order to identify and manage risk, and drive a compliance culture.
Rationale	Maintaining an appropriate system of risk oversight and management ensures ASIO can fulfil its purpose of protecting Australia and Australians from threats to their security. Our enterprise risk management framework ensures we engage with risk in all aspects of our business, and apply a sophisticated understanding of risk management practices to identify, evaluate and respond to risks and opportunities.
Methodology	The Commonwealth Risk Management Policy seeks to embed risk management as part of the culture of Commonwealth entities—where the shared understanding of risk leads to well-informed decision-making. The Commonwealth Risk Management Policy sets out nine elements that entities must comply with in order to establish an appropriate system of risk oversight and management.

Enablers

ASIO's success depends on our key enablers of people and leadership, security, trust, technology and data, and governance. Our enablers are the foundation of our capability to protect Australia and Australians. Each year we assess and review our enablers and capabilities to ensure we are able to effectively and efficiently deliver on our purpose.

People and leadership



ASIO's people are integral to our success. Our highly skilled workforce responds flexibly to a complex, challenging and changing security environment. As a priority we will invest in attracting talented individuals to contribute their experience, skills and ideas. Equally, to retain our talent we provide a supportive and inclusive workplace that encourages and invests in growth and development of staff. We encourage and foster innovation and leadership at all levels. We seek to reflect the diversity of the community we protect and we are committed to celebrating and promoting diversity through our Diversity and Inclusion Strategy and our staff-led diversity networks. Our leaders are purpose focused, accountable, collaborative, empowering, inclusive—and act in the best interests of the whole Organisation.

Security



ASIO's outcomes are critically enabled by our commitment to security. As Australia's security service we are leaders in developing security practices to protect people, information, operations and capabilities. From an internal perspective our security culture promotes resilience, builds trust, and sustains our access to the critical sources of intelligence that enable us to protect Australians from security threats. Our role in promoting a mature security culture across government and with our partners assists others to have a high level of security assurance. With partners we are building a security vetting capability to deliver a consistent vetting standard, stronger assurance and improved transferability of Australia's Top Secret–cleared workforce.

Trust



ASIO's ability to deliver our mission requires us to maintain the confidence and trust of our stakeholders, including the Australian people. Our work with partners in the National Intelligence Community, law enforcement, state, territory and federal governments, industry, academia and our international counterparts underpins our ability to protect Australia and Australians from threats to their security. ASIO recognises we have a responsibility to be as open as possible about what we do and why we do it. We are committed to building public trust through transparency, strict compliance with the law, stringent application of policies and procedures, and cooperation with external oversight and accountability bodies.

Technology and data



Technology and data is at the core of our business. Investing in new technologies will enhance our ability to detect and respond to new and emerging threats. A 10-year investment from government has enabled ASIO to commence a significant capability uplift program, delivering a human-led, data-driven, technology-enabled approach to the delivery of our mission. Our imaginative, curious and highly skilled technology workforce will work together with Australian technology partners to redesign and future-proof the technology that is integral to our work. New technologies will complement our capabilities and our ability to contextualise and synthesise large volumes of complex data into impactful advice.

Governance



ASIO's governance is founded on the principles of performance, transparency and accountability in accordance with Australian law. It enables our planning, resource management and operational decision-making and prioritisation. A strong culture of performance, oversight, continuous assessment and adjustment ensures we are using resources efficiently and effectively to deliver on our purpose. Our compliance and governance practices demonstrate our commitment to integrity in our role to protect Australia and Australians in a complex, challenging and changing security environment.

Risk management and oversight

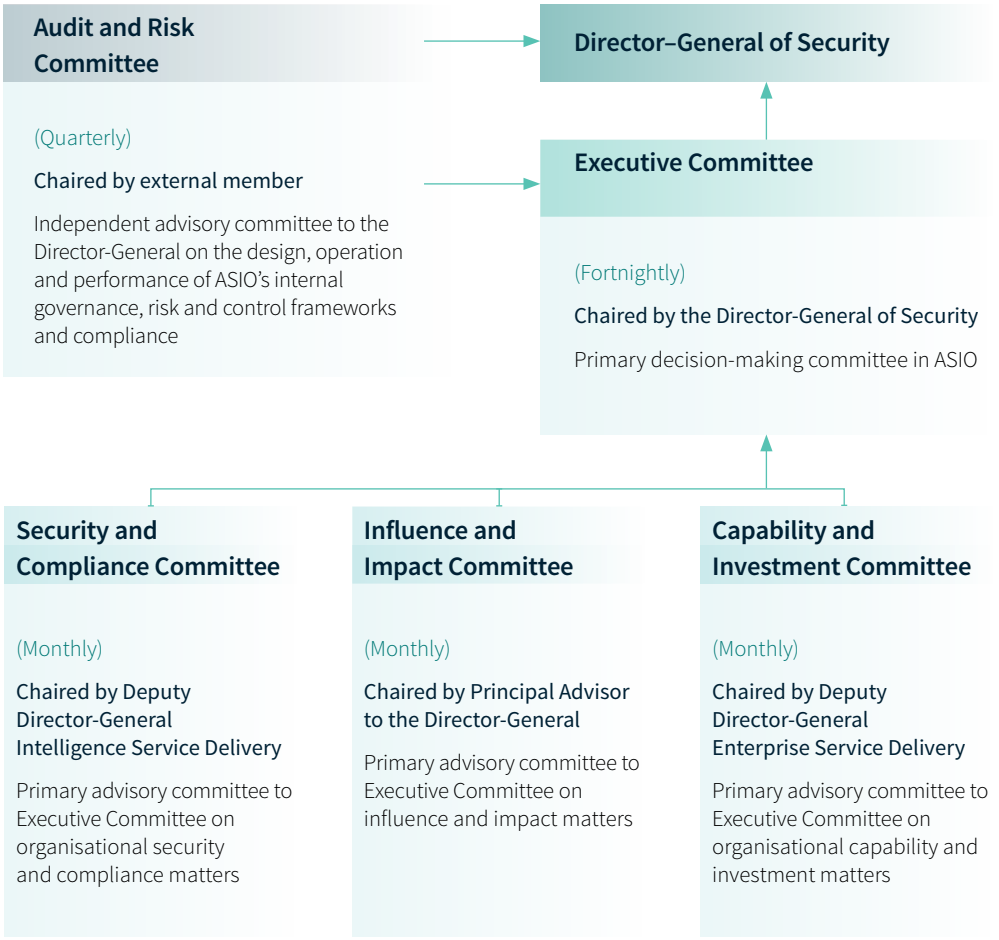
The Director-General is responsible for ensuring that ASIO maintains an appropriate system of risk oversight and management, so we can fulfil our purpose of protecting Australia and Australians from threats to their security. Our enterprise risk management framework ensures we engage with risk in all aspects of our business, and apply a sophisticated understanding of risk management practices to identify, evaluate and respond to risks and opportunities.

The Executive Committee is ASIO's peak governing body, advising the Director-General on matters requiring executive decision-making. The Executive Committee's purpose is to provide oversight of all ASIO activities, including the effective management of ASIO's risks. The Executive Committee sets and reviews the Organisation's risk appetite and tolerance, determines whether ASIO's overall level of risk is acceptable, and considers whether the risk management framework remains effective.

The Executive Committee is supported in its consideration of ASIO's risk by the:

- Security and Compliance Committee, which makes recommendations to the Executive Committee on significant security and compliance matters relating to or impacting ASIO, including the successful delivery of ASIO's strategic objectives and management of enterprise risk;
- Capability and Investment Committee, which makes recommendations to the Executive Committee on significant matters related to organisational capability and investment, and ensures their alignment to ASIO's strategic objectives; and
- Influence and Impact Committee, a new committee established in 2021, which makes recommendations to the Executive Committee on significant matters relating to or impacting on ASIO's influence agenda and gives account of performance against ASIO's objectives and endorsed lines of effort.

The Audit and Risk Committee provides independent assurance and advice to the Director-General, including on ASIO's enterprise risk management framework and internal controls for the effective oversight of risks.


Audit and Risk Committee
(Quarterly)
Chaired by external member
Independent advisory committee to the Director-General on the design, operation and performance of ASIO's internal governance, risk and control frameworks and compliance
Director–General of Security
Executive Committee
(Fortnightly)
Chaired by the Director-General of Security
Primary decision-making committee in ASIO
Security and Compliance Committee
(Monthly)
Chaired by Deputy Director-General Intelligence Service Delivery
Primary advisory committee to Executive Committee on organisational security and compliance matters
Influence and Impact Committee
(Monthly)
Chaired by Principal Advisor to the Director-General
Primary advisory committee to Executive Committee on influence and impact matters
Capability and Investment Committee
(Monthly)
Chaired by Deputy Director-General Enterprise Service Delivery
Primary advisory committee to Executive Committee on organisational capability and investment matters

Key risks

ASIO faces a broad range of risks reflecting its responsibilities as Australia's security intelligence service. The risks arising from ASIO's work can be significant, but we are committed to engage with risk to protect Australia and Australians from threats to their security.

Key areas of risk include the following:



Legal and propriety

Risks to compliance with laws, regulations, direction from government, international obligations, internal procedures or standards of propriety.



Financial

Risks to the security of money, assets and resources, including our financial sustainability.



Capability

Risks to the effectiveness and robustness of ASIO's capabilities, including technologies, data, facilities, partnerships, people and operational capabilities.



Health and safety

Risks to the health, safety and wellbeing of staff, partners, affiliates and the public.



Security

Risks to the protection of ASIO's capabilities, information and activities from compromise.



Reputation

Risks to the preservation of trust and confidence that government and the public place in ASIO.



asio.gov.au