Australian Government

Office of the Australian Information Commissioner

Office of the Australian
Information Commissioner

# Corporate plan 2024–25

OAIC

# Contact

Mail: Director, Strategic Communications
Office of the Australian Information Commissioner
GPO Box 5288
Sydney NSW 2001

Email: corporate@oaic.gov.au

Website: www.oaic.gov.au

Phone: 1300 363 992

# Non-English speakers

If you speak a language other than English and need help, please call the Translating and Interpreting Service on 131 450 and ask the operator to contact the Office of the Australian Information Commissioner on 1300 363 992.

# Accessible formats

Our publications can be made available in a range of accessible formats. If you would like this document in an accessible format, please contact us.

# Creative Commons

© Commonwealth of Australia 2024

The content of this document is licensed under the Creative Commons Attribution 4.0 International Licence, with the exception of the Commonwealth Coat of Arms, logos, any third-party material and any images and photographs.

Please attribute the content of this publication as: Office of the Australian Information Commissioner *Corporate plan 2024–25.*

# Contents


**Acknowledgment of Country** ..... 4

**Australian Information Commissioner's foreword** ..... 5

Future priorities ..... 5

**Part 1 Our vision, purpose and key activities** ..... 7

Key activity 1: Influence and uphold privacy and information access rights frameworks ..... 9

Key activity 2: Advance online privacy protections for Australians ..... 12

Key activity 3: Encourage and support proactive release of government information ..... 14

Key activity 4: Take a contemporary, harms-based approach to regulation ..... 16

**Part 2 Operating context** ..... 19

Our environment ..... 20

Our capability ..... 24

Our cooperation and collaboration ..... 26

Governance, risk and integrity ..... 29

**Part 3 Performance measurement framework** ..... 37

Key activity 1: Influence and uphold privacy and information access rights frameworks ..... 39

Key activity 2: Advance online privacy protections for Australians ..... 41

Key activity 3: Encourage and support proactive release of government information ..... 42

Key activity 4: Take a contemporary, harms-based approach to regulation ..... 43

Alignment with our PBS ..... 44

Performance measures and performance indicators overview ..... 45

# Acknowledgment of Country

The OAIC acknowledges the Traditional Custodians of Country across Australia and their continuing connection to land, waters and communities. We pay our respect to First Nations people, cultures and Elders past and present.

# Australian Information Commissioner's foreword

As the accountable authority, I am pleased to present the 2024–25 Office of the Australian Information Commissioner (OAIC) corporate plan for the 2024–25 to 2027–28 reporting periods, as required under paragraph 35(1)(b) of the *Public Governance, Performance and Accountability Act 2013*.

As an independent statutory agency, our office regulates privacy and freedom of information (FOI) under the Commonwealth *Privacy Act 1988* and the *Freedom of Information Act 1982* (FOI Act) and has information policy functions under the *Australian Information Commissioner Act 2010.* This corporate plan sets out our key activities and how we measure our performance.

So far, 2024 has been a year of significant changes at the OAIC. Among them was the return to the OAIC having 3 commissioners in February, when I commenced as FOI Commissioner and Ms Carly Kind as Privacy Commissioner. It was then my great honour to be appointed as Australian Information Commissioner from 16 August 2024 for a 5-year term. Following a merit-based selection process, Ms Toni Pirani was appointed as FOI Commissioner commencing 16 August. Commissioner Pirani brings a wealth of experience and expertise in FOI and the promotion of information access rights, as well as a strong record of service on behalf of the Australian public.

I would also like to acknowledge the contribution of my predecessor Angelene Falk who led the office over many years as both Information Commissioner and Privacy Commissioner. Commissioner Falk expertly steered the office through a time of growth, technological development, heightened community expectations and great change in the regulatory landscape. It brings me great pleasure and gratitude to build on Commissioner Falk's work and lead the OAIC at this critical juncture with Commissioner Pirani and Commissioner Kind.

This enhancement to our leadership structure coincided with a strategic review of the OAIC. The review was designed to ensure the office is best positioned to deliver our functions and respond to future challenges. The review made 9 recommendations to the OAIC, including around our regulatory posture, governance, structure, culture and values, and process change. The OAIC has accepted all recommendations directed to the office and has begun implementing them to ensure our future success.

A key recommendation was for the office to accelerate our shift to a more risk-based and education and enforcement-focused posture. Our stakeholders and the community can expect to see this reflected in a greater focus on directing our regulatory effort towards where it has the greatest impact, including areas where there is a high risk of harm to the community. Our focus on harm and outcomes will be driven by evidence and data, and we will make the best use of our resources, maximising opportunities for our people.

The shift in our regulatory posture is underway and changes to our strategic plan, governance, structure, processes, capability, culture and leadership will all ensure our success. These seminal changes, many of which are detailed in this plan, are designed to deliver our future priorities and maximise our impact as Australia's information access and privacy regulator. Our implementation of these changes and a revised regulatory action plan has only just commenced, but already we are achieving a significant impact.

## Future priorities

We are advancing our effectiveness in privacy regulation by taking a strategic approach. We are committed to clearly defining and effectively communicating our regulatory expectations to provide the community with the safeguards they are entitled to expect.

We are focused on identifying the unseen harms that curtail privacy rights in the digital environment. This means implementing a program of targeted, proactive investigations that will not only uncover latent harms and provide avenues for remediation, but will also set the standard for industry practice.

The proposed reforms to the Privacy Act will provide a greater range of enforcement powers to the OAIC, establish stronger privacy protections for children and enhance requirements in relation to the security of personal information and its destruction when information is no longer needed. The OAIC is well prepared and committed to lending our expertise to the next phase of this much anticipated reform. These reforms are urgent, particularly in an environment where we continue to see large data breaches and technology advance at a rapid pace. We stand ready to assist the regulated community with the transition.

Even ahead of reforms, the regulated community should be alert that the OAIC will ensure compliance with the law, and where there are egregious privacy breaches, we will hold organisations to account. An example of this is our civil penalty proceedings on foot against Medibank Private Limited, Australian Clinical Labs Limited and Meta Platforms Inc and Meta Platforms Ireland Ltd.

We also use guidance and education to effect behaviour change. A particular focus for the OAIC in this regard will be our new role as privacy regulator for the Digital ID system as it is expanded across the Australian economy.

Access to information underpins open government and is essential to a participative democracy. Our aim is to promote open government to better serve the Australian community. We aim to increase public participation in government decision making and ensure information held by government is managed for public purposes and is a national resource.

A key focus in 2023–24 was the 5-yearly Information Publication Scheme review. We look forward to applying the results of this review, to promote proactive publication of government-held information and ease of compliance with FOI obligations.

We will build on the substantial progress we made in 2023–24 in effective case management to eradicate the backlog that has developed over many years and ensure our regulatory currency and therefore effectiveness.

The OAIC's sharpened intelligence-led approach will also inform our information access priorities; we will apply our intelligence to identify and target areas of non-compliance. We are committed to identifying and uplifting capability gaps within agencies and ministers' offices in exercising their functions under the FOI Act. Timeliness in their decision making is a key risk to the right to access information, and we will focus our regulatory action towards halting the decline in timeliness that has occurred over past years.

We remain energised in our work monitoring the FOI framework as a measure of the health of our democracy, by analysing agency and OAIC statistics. In harnessing this information and through examining optimal features for FOI legislation, we will also advocate to ensure the FOI Act is responsive to the digital environment and secures community expectations.

We continue to navigate work of increasing volume and complexity across our regulatory functions. Our collaborative work – with peers both on home soil and abroad – is an important channel for sharing information, cooperating on mutual issues and opportunities, and ensuring our regulatory efforts are efficient. This work is particularly impactful in our region, and our collaboration with our neighbouring sovereign states well serves human rights and our democratic and economic stability.

The commonality of information access and privacy as fundamental human rights is deeper and more powerful than their origins. Transparency and trust are enlivened and preserved by our effective regulation of these rights, and so we are committed to meeting the expectations of the Australian community as a credible and effective regulator.

Never before have we seen such focus on the importance of privacy protection and information access – from individuals, businesses and government alike. This is a pivotal moment for the OAIC and our country, and it is an honour to lead the agency in promoting and upholding these critical rights for the Australian community at this time.

**Elizabeth Tydd**
Australian Information Commissioner
29 August 2024

# Part 1

## Our vision, purpose and key activities

### Our purpose

To promote and uphold privacy and information access rights

### Our vision

To increase public trust and confidence in the protection of personal information and access to government-held information

## Guiding principles

**Proactive**
We adopt a risk-based, education and enforcement-focused posture.

**Purpose driven**
We focus on harms and outcomes and are driven by evidence and data.

**Proportionate**
We prioritise our regulatory effort based on risk of harm to the community.

**People focused**
We preserve expertise and talent. We make the best use of our resources and maximise opportunities for our people.

## Key activities

1

Influence and uphold privacy and information access rights frameworks

2

Advance online privacy protections for Australians

3

Encourage and support proactive release of government information

4

Take a contemporary, harms-based approach to regulation

# Key activity 1

## Influence and uphold privacy and information access rights frameworks

The OAIC has a wide range of regulatory functions and powers under the Commonwealth *Australian Information Commissioner Act 2010* (AIC Act), *Freedom of Information Act 1982* (FOI Act), *Privacy Act 1988* and other laws. We regulate the privacy aspects of the Consumer Data Right (CDR), My Health Record system and, from 2024–25, Digital ID, as the system is expanded across the Australian economy.

### Access to information

The OAIC regulates the community's access to government-held information under the FOI Act. Our freedom of information (FOI) functions include conducting independent merit reviews of FOI decisions made by Australian Government agencies and ministers and investigating actions taken by agencies under the FOI Act, in response to complaints and on our own initiative.

We also monitor the FOI framework, including by analysing agency statistics, Information Commissioner review (IC review) applications, complaints, extension of time applications, vexatious applicant declarations and regular reviews of the operation of the Information Publication Scheme (IPS). This activity informs our guidance, education and regulatory activity.

The OAIC promotes and advocates for the timely release of government-held information. The timely release of information is consistent with the objects of the FOI Act and supports participative democracy. We factor the importance of timeliness into decisions about extensions of time and promote its importance to agencies when engaging with senior leaders and practitioners and through more formal guidance.

The delivery of timely IC reviews is a priority for the OAIC. Our focus during 2024–25 is finalising matters received in 2020 and 2021 and expediting cohorts of applications for review of:

- access grants
- matters involving ministers as the respondent
- deemed access refusals
- imposition of a charge
- practical refusal decisions
- adequacy of searches
- secrecy provisions.

In terms of FOI complaints, our priority for the year ahead is reviewing, investigating and monitoring current agency practices and making recommendations that will support agencies to move towards best practice.

We engage with agencies and other stakeholders through multiple channels, including events, meetings, consultations, our Information Contact Officers Network and our annual International Access to Information Day campaign.

## Privacy

The OAIC regulates how agencies and certain organisations handle personal information under the Privacy Act. Our privacy functions include handling complaints, conducting investigations and assessments, and providing advice and guidance.

A variety of other laws confer privacy-related functions, powers, responsibilities, or other obligations that require certain bodies to consult with the Australian Information Commissioner on privacy matters. The OAIC acquits our regulatory functions under these laws and provides privacy guidance and advice to entities when consulted under legislation. We also review and update statutory instruments we are responsible for to ensure they are fit for purpose.

The OAIC also has statutory functions to monitor activities and advise agencies that are developing laws, programs or policies that impact privacy. We do this by making submissions to government consultation processes, reviewing bills and other statutory instruments, and providing advice and guidance to agencies to ensure any adverse effects on privacy are minimised.

We engage with organisations, agencies and other stakeholders through multiple channels, including events, meetings, consultations and our annual Privacy Awareness Week campaign.

### Security and the Notifiable Data Breaches scheme

The OAIC's goal is to make Australian entities more resilient to security threats by:

- providing advice and guidance to individuals and entities about the obligation to secure personal information
- increasing awareness about the causes of data breaches and prevention strategies
- advising entities that experience a breach to notify, contain and remediate
- taking regulatory action.

We influence entities to take a proactive approach to their security obligations, including through our work overseeing the Notifiable Data Breaches (NDB) scheme. We work closely with entities that notify data breaches to ensure the requirements of the scheme are met and promote best practice data breach prevention and response. We also respond to risks identified through the scheme and consider regulatory action in instances of serious non-compliance with the scheme's requirements.

The OAIC has underway several investigations into organisations in relation to data breaches, including Singtel Optus Pty Limited, Latitude group of companies and HWL Ebsworth Lawyers.

The OAIC's civil penalty proceedings against Medibank Private Limited and Australian Clinical Labs Limited will continue in the Federal Court in 2024–25. This enforcement action is an example of how the OAIC is prioritising regulatory action where there is a high risk of harm to the community. It sends a strong message to the regulated community that keeping personal information secure and meeting the requirements of the NDB scheme must be priorities.

### Digital ID

We will be undertaking work to ensure Australians' privacy is protected as the Digital ID system is expanded. Digital ID will allow Australians to verify their identity online in a secure, convenient and voluntary way while reducing the amount of personal information that needs to be shared.

Robust privacy safeguards are fundamental to the effective functioning of the Digital ID system and to ensuring individuals can have confidence when using the system. We will help stakeholders understand the Digital ID privacy safeguards through publishing guidance material and responding to enquiries. We will also provide assurance to the community of the privacy protections in the Digital ID system by using our range of enforcement powers to ensure individuals' privacy is protected.

## Credit reporting

Another key focus area for the OAIC is facilitating an efficient credit reporting system that protects individuals' privacy.

We will continue implementing proposals from the 2021 independent review of the Privacy (Credit Reporting) Code 2014 (CR Code), including considering and publicly consulting on an application from the industry code developer to vary the CR Code. The amendments will include minor adjustments to ensure the smooth functioning of the CR Code, as well as significant changes that will enhance individual rights and the operation of credit reporting.

As part of our work to raise credit reporting issues with government, we will participate in the statutory reviews of Part IIIA of the Privacy Act and the *National Consumer Credit Protections Act 2009,* which are both due to be completed before 1 October 2024.

The OAIC will also remake the Credit Related Research Rule 2014, following public consultation, which is due to sunset in October 2024.

## Digital health

The OAIC aims to increase public trust and confidence in the handling of health information through our regulatory role, including our oversight of the privacy provisions for the My Health Record system and Healthcare Identifiers Service.

We do this through education and guidance activities and engaging collaboratively with health professionals to uplift privacy knowledge and practices relating to digital health. For example, we publish refreshed guidance following policy or legislative reforms to ensure everyone who handles health information does so in accordance with community expectations and legislative requirements.

In addition to these proactive engagement activities, the OAIC may exercise a range of powers as part of our compliance and enforcement role, including making determinations, conducting assessments and investigating any alleged failures to comply with data breach notification requirements. We respond to risks identified through enquiries and complaints, assessments and data breach notifications relating to the My Health Record system.

The OAIC is finalising our review of the National Health (Privacy) Rules 2021 to ensure they remain fit for purpose to regulate how Australian Government agencies use, store, disclose and link Medicare Benefits Schedule and Pharmaceutical Benefits Schedule claims information. In the year ahead, the OAIC will lodge new rules to commence on 1 April 2025.

## Consumer Data Right

We co-regulate the Consumer Data Right (CDR) with the Australian Competition and Consumer Commission (ACCC).

The OAIC regulates and enforces the privacy aspects of the CDR. The objective of our regulatory approach is to ensure consumers can have trust and confidence in the handling of consumer data under the CDR framework.

We collaborate with the Treasury, the ACCC and the Data Standards Body to ensure the fundamental privacy protections in the CDR are maintained. We engage with CDR participants to help them understand their privacy obligations, including by publishing guidance material, investigating complaints and conducting assessments.

We also publish information about the CDR for consumers and contribute to education and awareness strategies regarding the CDR and our role.

We advise on the privacy implications of proposed amendments to and expansions of the CDR framework, including the designation of new sectors and the development of new rules.

## Key activity 2

### Advance online privacy protections for Australians

The OAIC advances online privacy protections for Australians to support the Australian economy by influencing the development of legislation, taking a contemporary and harms-based approach to regulation and raising awareness of online privacy risks and protections.

The OAIC will foster community trust in and uptake of Digital ID through our new role as privacy regulator for the system. Digital ID reduces a significant source of risk in Australians' digital lives: the current wide sharing and storage of identity documents.

The OAIC continues to support and contribute to law reform processes, including the work to progress the Australian Government's response to the review of the Privacy Act, the 2023–2030 Australian Cyber Security Strategy legislative reforms, the Australian Government's interim response to the safe and responsible AI in Australia consultation, and the review of Part IIIA of the Privacy Act. We advocate for the progression of privacy law reform to advance privacy protections for Australians and build trust and confidence in the digital economy.

In relation to the Australian Cyber Security Strategy, the OAIC supports a consistent and whole-of-government approach to reducing cyber risk to mitigate privacy risk. The OAIC's principal concerns are ensuring our regulatory remit is preserved, particularly in relation to the NDB scheme, and that reforms promote a coherent framework of obligations for entities.

The OAIC will prioritise regulatory action to address the harms arising from the practices of online platforms and services that impact individuals' choice and control, either through opaque information sharing practices or in the terms and conditions of service.

The OAIC's civil penalty proceedings against Meta Platforms Inc and Meta Platforms Ireland Ltd in relation to Cambridge Analytica will continue in 2024–25. This follows a successful application to the High Court of Australia in March 2023 for Meta Platforms Inc's grant of special leave to appeal to be revoked due to a change in the Federal Court Rules regarding overseas service, which cleared the way for the substantive case to be heard in the Federal Court. In June 2023, the Federal Court ordered the Information Commissioner and Meta to engage in mediation.

We are continuing work to respond to the privacy risks arising from artificial intelligence (AI), including the effects of powerful generative AI capabilities being increasingly accessible across the economy. The release of these technologies publicly and their distribution at no cost to the user amplifies the scale of potential privacy impacts and reinforces the importance of the OAIC building awareness of privacy risks and regulated entities' obligations. Robust privacy governance and safeguards are an important foundation for using this technology in a way that builds trust and confidence in the community and enables entities to take advantage of the opportunities of AI.

We provide information, resources and support to entities to help them understand and mitigate privacy risks and uplift their practices. The most visible demonstration of this is Privacy Awareness Week (PAW), an annual campaign that raises awareness of privacy issues and the importance of protecting personal information among agencies, businesses and individuals. We run PAW with state and territory privacy regulators and the Asia Pacific Privacy Authorities (APPA).

It is important for regulators to work together as much as possible to ensure consistency and avoid unintentional or unnecessary overlap. The OAIC collaborates and engages with domestic and international regulators in performing our regulatory functions and to enhance our effectiveness in addressing new and emerging threats to privacy.

The OAIC is a founding member of the Digital Platform Regulators Forum (DP-REG). In 2023–24, DP-REG's strategic priorities included assessing the impact of algorithms, and understanding and assessing the benefits, risks and harms of generative AI. The impact of these technologies continues to be an area of focus for the OAIC as their prevalence increases.

As a founding member and co-chair of the Cyber Security Regulator Network, we collaborate with other Australian regulators to improve the effectiveness of regulatory activity and work together to understand, respond to and share information about cyber risks impacting privacy.

Our membership of the Global Privacy Assembly, APPA and the Global Privacy Enforcement Network gives us a platform to influence the development of interoperability between international privacy laws and consistent high standards of privacy regulation. Through these bodies, we share knowledge, exchange ideas and identify solutions to emerging issues, including the use of AI and other technologies that pose a high privacy risk.

The OAIC also monitors ongoing developments in the international regulatory landscape, including overseas data protection and AI regulation, to inform our domestic policy activities.

## Key activity 3

### Encourage and support proactive release of government information

The OAIC promotes a proactive approach to the publication of government-held information. We focus on supporting efficient access to information and facilitating innovation and engagement. Our regulatory and educative approach will be informed by the results of the 2023 review of the IPS.

The OAIC promotes proactive release of government-held information through the IPS and informal release of information as part of administrative access processes.

A key focus in 2023–24 was the 5-yearly IPS review, conducted by the OAIC in conjunction with Australian Government agencies. This was the third statutory IPS review, following previous reviews in 2018 and 2012.

The IPS review highlighted a concerted effort is required by agencies to support the proactive release of information and should assist agencies to identify where improvements can be made. The review has also informed the OAIC's forward work program, which includes actively engaging with senior leaders across the Australian Public Service to secure their commitment to this important and mandated responsibility. The OAIC will also conduct a survey of agency practices and needs and use this information – along with the results of the IPS review – to inform the resources we provide and updates to the FOI Guidelines on the IPS. Our objective is to promote understanding and make compliance easy so the Australian community receives access to information as intended under the FOI Act.

The OAIC is empowered to investigate complaints into agencies' IPS and aims to increase general awareness around making a complaint about an agency's IPS.

Prior to the IPS review, the OAIC substantively revised our FOI Guidelines on the IPS. The Information Commissioner remade these guidelines in July 2023 following a public consultation process. The revised guidelines support and instruct agencies in operating their IPS and publishing information proactively. For example, a new section encourages agencies to commit to being 'open by design' and sets out what this might involve in practice.

Government-held information is a national resource that should be managed for public purposes. The timely release of government-held information, with a focus on quality decision making and proactive release of information, is consistent with the objects of the FOI Act and supports participative democracy. The OAIC continues to focus on the need for agencies to make timely decisions and encourages proactive disclosure of information to increase transparency and support an efficient FOI system.

We will do this by improving the delivery of our IC review functions, with a view to providing timely reviews and improving decision making by agencies and ministers. We will support this by:

- providing guidance as set out in review decisions and informed by the survey of FOI practitioners
- reviewing key guidelines that can facilitate a pro-disclosure approach
- ensuring agencies make sound and timely decisions, including through intervening early in reviews of deemed access refusals
- investigating complaints
- considering applications for extension of time
- making available a self-assessment tool to assist agencies to identify gaps and areas for improvement in their practices
- proactively publishing agency FOI statistics
- identifying agencies that model better practice in proactive publication
- considering issues related to the maintenance of disclosure logs and the IPS.

During 2023–24, the OAIC implemented changes to the Directions as to certain procedures to be followed in IC reviews, which came into effect on 1 July 2024. The

changes aim to promote timely and efficient resolution of IC reviews.

We engage with agencies and ministers to promote understanding of the FOI Act and ensure FOI practice is both consistent with the legislation and meets community expectations. We will develop capability by providing guidance, including new and updated resources on our website.

As a key integrity agency dedicated to managing government-held information as a national resource, the OAIC will continue our work as part of the Open Government Partnership Australia to progress the commitments in the Third National Action Plan.

Our ability to promote access to information rights is bolstered by our strong relationships with domestic and international regulators. The OAIC actively collaborates with Australian and New Zealand information access regulators through the Association of Information Access Commissioners, which promotes best practice in information access policies and laws across the 2 countries. In June 2024, the OAIC was elected as an executive member of the International Conference of Information Commissioners, which aims to improve people's right to public information and their ability to hold to account bodies that provide public functions. We also assist emerging FOI jurisdictions within the Indo-Pacific and ASEAN countries with the aim of advancing the right to access information both nationally and internationally.

## Key activity 4

### Take a contemporary, harms-based approach to regulation

The OAIC takes a contemporary, harms-based approach to promoting and upholding Australia's privacy and FOI laws. We are committed to developing a skilled, multidisciplinary workforce that is supported by the tools needed to deliver our regulatory role in a dynamic, responsive and targeted manner.

During 2023–24, a strategic review of the OAIC identified opportunities to sharpen our regulatory activities to be more harm focused and risk based. We will review our strategic and regulatory approach to achieve this objective.

As a regulator, we must discharge our functions and exercise our powers fairly, transparently and in the public interest. We use data and other evidence-based methods to assess risk, and use appropriate regulatory tools to address privacy and information access issues. We harness and consult with external experts where appropriate, including with technical experts.

The OAIC Data Strategy 2023–25 focuses on making high-quality data analyses integral to our decision making when fulfilling our functions and exercising our powers. Our strategy is aligned with the Australian Data Strategy's objective to uplift data capability across government.

Our approach to exercising our regulatory powers is articulated in our statement of regulatory approach, policies and guides.

**Statement of regulatory approach**

The OAIC's regulatory approach uses both encouragement and deterrence to promote and protect privacy and information access rights. We apply a proactive and harms-focused approach to prioritise our efforts. We take regulatory action to encourage and support compliance by regulated entities and to address high-risk matters with the greatest potential for harm.

We will be more likely to take regulatory action in response to issues:

- that create a risk of substantial harm to individuals and the community, especially to vulnerable people and groups
- that concern systemic harms or contraventions
- where our action is likely to change sectoral or market practices, or have an educative or deterrent effect
- that are subject to significant public interest or concern
- where our action will help clarify aspects of policy or law, especially newer provisions of the Acts we administer.

We take regulatory action in a consistent, transparent and proportionate manner. When deciding on which regulatory tools to use, and how to use them, we:

- identify the risks of harm we are responding to, and the likelihood and possible consequences of those risks
- respond in ways that are proportionate, consistent with the expectations of the community and the Australian Government, and manage risks to adequately protect the public
- take timely and necessary action
- seek to minimise regulatory burden and cost.

We routinely review our regulatory approach to ensure it aligns with government and community expectations.

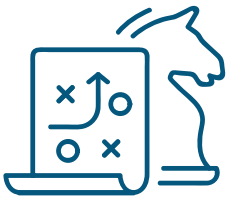
In 2024–25, the major areas of focus for the OAIC will be:

- ensuring emerging technologies, including AI, align with community expectations and regulatory requirements and targeting current and emerging harms effectively and proportionately while continuing to proactively guide compliance in a dynamic digital environment
- supporting the development of a privacy-protecting digital economy through regulating compliance and supporting entities under the NDB scheme, Digital ID system and co-regulation of the CDR
- leading the promotion of open government and cultivating the FOI capabilities of Australian Government agencies and ministers to secure timely access to and proactive release of government-held information – we will seek to make compliance easier and increase OAIC regulatory effectiveness
- strengthening and enforcing protections for personal information and contributing to privacy law reform
- building internal capability and culture to advance the OAIC's reputation as an innovative, harms-focused regulator delivering demonstrably efficient and effective regulatory action.

In discharging our regulatory functions, we adhere to the Regulator Performance (RMG-128) best practice principles.

**Regulator best practice principles**

**Continuous improvement and building trust** – We work to continuously improve our performance, capability and culture from a whole-of-system perspective to build trust and confidence in our regulatory work and our people. We are committed to continuously improving our processes, governance and capabilities, and developing our organisational values and a positive culture that supports best practice.



**Risk based and data driven** – We aim to manage risks proportionally and maintain essential safeguards while minimising regulatory burden. We leverage data, evidence-based methods and digital technology to support our activities and reduce cost and administrative burden on those we regulate.

**Collaboration and engagement** – We strive to be transparent and responsive communicators by regulating in a modern and collaborative way. We do this by providing up-to-date, clear and accessible guidance and information, being transparent in decision-making processes, and engaging and consulting genuinely with our stakeholders while remaining receptive to their feedback and diverse views.

The OAIC monitors our performance against the principles of regulatory best practice through our performance measurement framework – specifically measures 4.1, 4.2, 4.3 and 4.4.

The Attorney-General issued the OAIC with a ministerial statement of expectations in March 2023. It outlines the Australian Government's expectations of how the OAIC will achieve our objectives, carry out our functions and exercise our powers. In June 2023, the OAIC responded with a statement of intent, which outlines how the OAIC intends to meet those expectations, including how we will demonstrate progress. Both statements are available on our website.

# Part 2

## Operating context

# Our environment

A clear understanding of our operating environment is crucial to the OAIC's risk-based regulatory approach and education and enforcement-focused posture.

We actively scrutinise our environment, assessing and prioritising our regulatory effort where the potential risk of harm to the community is most significant.

Our risk-based approach also means we acknowledge which environmental factors are outside our control and focus on those areas where we can make the best use of our resources and be most effective.

## OAIC operational changes

The OAIC has grown and changed significantly since it was established in 2010.

Notably, in February 2024, the office returned to having 3 commissioners: the Australian Information Commissioner (the agency head), a Privacy Commissioner and a Freedom of Information Commissioner.

A strategic review of the OAIC was conducted by the Nous Group between October 2023 and February 2024. The review identified opportunities to ensure the OAIC is best positioned to deliver our functions and respond to future challenges. The review made 9 recommendations to the OAIC, including around our regulatory posture, governance, structure, culture and values, and process change. The OAIC has accepted all recommendations directed to the agency and has begun implementing them to ensure the agency's future success.

As part of the strategic review implementation program, the OAIC has created a statement of regulatory approach (page 16) and settled 4 principles to guide our operations and support the move to a new regulatory posture (page 8). We have implemented a new governance structure, initiated a project to design the future OAIC structure in line with our enhanced regulatory posture, and started work to define new culture and leadership behaviours via a series of executive workshops. We have also identified, tested and refined process improvements across a number of our functions to support efficiency.

## Community expectations

The Australian community's expectations around privacy and access to information are changing.

Advances in technology and the increased frequency and harm of data breaches have heightened awareness and concern about privacy among the community. Our 2023 Australian Community Attitudes to Privacy Survey (ACAPS 2023) found 9 in 10 Australians have a clear understanding of why they should protect their personal information, up from 85% in 2020. While many Australians do not know exactly how they can protect their own personal information, the majority would like organisations to do more in this area. The vast majority (89%) of Australians would also like government to pass more legislation that protects their personal information.

Community expectations around accountability and transparency are also increasing. Our 2023 Australian Government Information Access Survey found 91% of Australians felt their right to access information from government sources was very or quite important, up from 84% in 2019.

The community increasingly expects organisations and agencies to be accountable for how they handle information, and they want regulators to have an enforcement focus.

## Regulatory function growth

The OAIC continues to see high and growing demand for our critical, mandatory functions, including our complaint handling and merit review of freedom of information (FOI) decisions services.

As the number of new cases has exceeded the number resolved, our case backlog (measured by the number of cases unresolved for more than 12 months) has grown. This has been most pronounced in our Information Commissioner review (IC review) function.

Applications for IC review have risen each year but 2 since the establishment of the OAIC, averaging 12% per year. In 2023–24, the OAIC received our second highest number of applications to date. Each year, we have

increased the number of cases finalised, in some years by as much as 35%. However, limited resourcing has not met the ongoing demand, and since 2018, the OAIC has carried forward cases. The cumulative impact is a significant backlog of aged cases. In 2023–24, the OAIC halted this growth trajectory for the first time in 8 years. This will increase our ability to focus on more recent IC reviews and therefore address current agency practices.

The growing focus on data protection, transparency and accountability issues has led to an increase in the complexity, scale and impact of many privacy complaints. Many privacy complaints are appropriately addressed through our early resolution and conciliation processes, or through recognised external dispute resolution schemes. However, where matters are not addressed, we investigate complaints.

There has also been an increase in representative complaints, which is a complaint made by an individual on behalf of other individuals who have similar complaints about an act or practice that may be an interference with their privacy. The Information Commissioner has accepted several representative complaints since March 2024. These include representative complaints made against Medibank Private Limited and Singtel Optus Pty Limited following major data breaches, and against the Department of Veterans' Affairs in relation to the Veterans' Medicines Advice and Therapeutic Education Services program. The Information Commissioner is also considering the validity of several other representative complaints.

We continue to implement strategies and streamline processes to deal with our workload. For example, in relation to IC reviews, we identify priority cohorts to assist us to manage the high volume of matters, achieve outcomes more quickly and reduce backlogs. We published 2 new procedural directions to direct agencies' processes towards prompt finalisation and improve their first instance decision making. We revised the FOI Guidelines to reflect case law and enhanced other guidance to ensure agencies and ministers consistently apply FOI law.

The OAIC has also established an FOI 'surge team'. The surge team comprises people from across the OAIC to provide additional capacity across a range of FOI regulatory functions. This approach has built capacity within the OAIC and provided the baseline from which we can achieve greater efficiencies and regulatory effectiveness through a whole-of-OAIC approach to resourcing.

The OAIC is also focused on enforcement, education and guidance work.

For instance, as part of our FOI functions, the OAIC provides resources, advice and training to support appropriate and timely decision making by agencies and ministers. We also monitor and engage with agencies regarding their adherence to statutory timeframes. The OAIC will be focusing on mechanisms that further enhance engagement between our agency and regulated entities to build capacity in the FOI system, including through the use of surveys and data collection.

The OAIC is investigating the personal information handling practices of entities, including Singtel Optus Pty Limited, Latitude group of companies and HWL Ebsworth Lawyers, following high-profile data breaches. We are also investigating Bunnings and Kmart, focusing on the companies' use of facial recognition technology.

Work in this space is complex and lengthy, and the volume is expected to increase as the OAIC continues to prioritise our regulatory effort based on risk of harm to the community.

## Open government and digital government

The Australian Government recently released its Third Open Government National Action Plan 2024–2025 (NAP3). NAP3 contains 8 commitments to improve public participation and engagement in government, strengthen government and corporate sector integrity, and enhance Australia's democratic processes. The commitments align with several of the 'challenge areas' identified in the Open Government Partnership 2023–2028 Strategy, which include access to information and digital governance.

OAIC executive members were involved in the co-design of NAP3, and as a key integrity agency, we are working as part of the Open Government Partnership Australia to progress the commitments. For example, Commissioner Tydd co-led the working group that developed the first commitment to create transparency in the use of automated decision making and artificial intelligence (AI).

The increase in the use of technology, such as AI and encryption, and a digital space rife with mis- and dis-information present both opportunities and challenges for government information management.

The OAIC champions best practice in government information creation, management, protection, use and access. A proactive approach to information management will play a critical role in achieving the Australian Government's Data and Digital Government Strategy.

## Legislative environment

The *Privacy Legislation Amendment (Enforcement and Other Measures) Act 2022* came into effect in December 2022. It introduced significantly increased penalties for serious and repeated privacy breaches, greater powers for the OAIC to resolve breaches, and changes to jurisdictional provisions to increase the application of Australian privacy law to overseas organisations operating within Australia.

In September 2023, the Australian Government released its response to the Attorney-General's Department's review of the *Privacy Act 1988.* Of the 116 proposals for reform, the Australian Government 'agreed' with 38, 'agreed in principle' with 68 and 'noted' 10. Notably, the agreed proposals include further strengthening the OAIC's regulatory, enforcement and investigative powers.

The OAIC has welcomed the Australian Government's response as a crucial step in ensuring Australia's privacy framework is strengthened for the future. The proposed reforms will materially change certain functions the OAIC performs and introduce new functions and powers. The proposals seek to bolster privacy protections for all Australians, adapt the legal framework to the changing technology landscape and expand the OAIC's enforcement capabilities – for example, by empowering the Information Commissioner to issue civil infringement notices for low-level administrative breaches of the Privacy Act and streamlining investigations processes. The OAIC is well prepared and committed to lending our expertise to the next phase of this much anticipated reform.

## Cyber security

The OAIC has a clear role to play in the cyber security landscape. Significant data breaches in Australia in recent years have brought a renewed focus on cyber security among government, business and individuals. They have highlighted that entities collect and hold an increasingly large quantity of personal information, which must be secured effectively. When cyber security measures fail, the risk of harm to individuals whose information is compromised can be serious.

The OAIC will continue to engage with the Australian Government on programs of work to uplift cyber security in Australia, including the proposed new cyber security legislation and changes to the *Security of Critical Infrastructure Act 2018* under the Australian Cyber Security Strategy. There is an important opportunity to achieve a consistent approach across government to reducing the risk of cyber harm, which will help to promote public trust and confidence in Australia's cyber security and privacy frameworks.

## Digital ID

The passage of Digital ID legislation in May 2024 paved the way for the system to be expanded across the economy, with the OAIC as its independent privacy regulator.

Digital ID aims to protect people's identity information by providing a way to securely verify who they are online with government services and businesses, reducing the need to share identity documents.

The OAIC will ensure there are strong privacy safeguards for people who choose to use Digital ID with an accredited provider. Digital ID will have a phased roll out of the government system to non-government participants. As the Digital ID system commences and expands, the OAIC's goal is to promote trust in Digital ID by ensuring the privacy of users is protected.

## Emerging technologies

Rapid technological innovation and the development of new data-driven products and services continue to offer significant benefits for Australians and have changed the way individuals interact, conduct business and receive services. However, they have also created new privacy risks and harms, many of which arise due to the increased amount of data and personal information collected, used and disclosed, both in Australia and globally.

The OAIC continues to focus on regulating the online environment and emerging technologies that have a large impact on privacy, including facial recognition technology and AI. We have been considering issues related to AI through our membership of the Digital Platform Regulators Forum (DP-REG) and through contributing to work across government.

The globalised digital economy can present risks, like increased cyber security threats, so a unified regulatory approach to protect Australians' data wherever it flows is essential. The OAIC cooperates and collaborates with international regulators to influence and shape the global regulatory environment and to promote higher standards of data protection around the globe.

## Consumer Data Right

The Consumer Data Right (CDR) supports innovation and economic growth by allowing consumers to ask entities in designated sectors of the economy to securely transfer their data to an accredited provider. This enables consumers to compare and access better value products and services more easily.

The CDR is currently operational in the banking and energy sectors and is expected to expand to include the non-bank lending sector. Work is also progressing to design new CDR functionality to allow consumer-directed action and payment initiation. If introduced, this would allow consumers to authorise, manage and facilitate actions like making payments, switching providers and updating their details, in the CDR.

As the CDR expands, we will ensure the data protection and privacy framework remains robust and consumers continue to be protected by effective accountability mechanisms. A strong privacy and security framework is necessary not only to protect consumers' information, but also to maintain public confidence in, and the integrity of, the CDR system.

## Digital health

ACAPS 2023 showed Australians trust health service providers and federal government agencies the most when it comes to the protection and use of their personal information. Health information is a particularly sensitive type of personal information and requires a higher level of protection.

We continue to monitor developments in digital health. There have been significant changes in government information handling practices, as well as technological advances in the digital health landscape. The OAIC acknowledges ongoing government initiatives to remove obstacles to information sharing and foster data integration for research and public policy. We seek to respond to these changes where appropriate by providing oversight and guidance to ensure each initiative has strict controls and privacy is a central consideration.

## Our capability

At the OAIC, our people are our most valuable resource, reflected in a focus on people being one of the agency's guiding principles.

We strive to preserve expertise and talent. We aim to make the best use of our resources and maximise opportunities for our people.

### Workforce capability

The OAIC has a hybrid work model, allowing us to recruit nationally to ensure we attract the right people to the right roles. As a result, we have people located in every Australian state and territory.

To ensure we continue to support our hybrid workforce, the OAIC offers an engaging virtual approach to learning and development, with a strong focus on inclusivity and accessibility, as well as training and events. We will continue to release a targeted learning and development calendar every 6 months to support and embed the OAIC's continuous learning culture.

In alignment with the Australian Public Service Commission's Highly Capable, Future-Ready: APS Learning and Development Strategy, we invest in development opportunities for our people by partnering across the Australian Public Service (APS) to access a range of relevant courses and resources.

The OAIC has recently focused on uplifting capability as we shift to a more risk-based, education and enforcement-focused posture. For example, building on recent training for our investigators, we intend to offer cyber security and AI training to our people to ensure the OAIC is at the forefront of emerging technologies and trends.

We are committed to ensuring the safety and wellbeing of our people, regardless of location. We recently updated our Workplace Health and Safety Policy to include a psychosocial hazard assessment and provided training on this topic. We will build on these foundations by running regular training and reviewing our psychosocial hazard assessment to ensure it remains fit for purpose.

The OAIC has increased opportunities for internal mobility through internally advertising expressions of interest and moving our people where they are most needed, while simultaneously offering broader role development.

We are designing a new organisational structure in response to the recommendation in the strategic review of the OAIC that we update our structure to achieve the agency's purpose and future functionality in ways that will enable us to deliver our new regulatory posture.

We will focus on developing a strategic workforce plan to identify the roles, skills and future training needed to deliver on our increasingly risk-based, enforcement- and education-focused regulatory posture and respond to future workforce needs. This will include improving our onboarding and induction processes and embedding our value proposition.

In 2024–25, the OAIC will reduce outsourcing of core work in line with the APS Strategic Commissioning Framework. Our targets for 2024–25 focus on reduced outsourcing of work across several Job Families including Administration, Legal and Parliamentary, and Portfolio Program and Project Management, with an expected reduction of $950,000 in 2024–25 in outsourcing expenditure.

## Infrastructure capability and ICT requirements

The OAIC promotes the efficient, effective and secure use of information and communications technology (ICT) tools through information sessions for our people and regular updates. Our operating systems, software applications, networking components and digital devices are regularly upgraded so they remain secure and support efficiency. Following a technology systems review in 2023–24, we will consider future system upgrades as required to ensure the OAIC's ICT capability meets our needs as a contemporary regulator.

To continue to support the learning and development of our hybrid workforce, the OAIC recently improved induction and mandatory training programs within our learning management system, Learnhub. Learnhub enables our people to undertake mandatory training, complete induction training modules and participate in courses from partnering providers. Learnhub is also providing the OAIC with a sound personal learning and development record management system.

We strive to preserve **expertise and talent**. We aim to make the **best use of our resources** and maximise opportunities for our people.

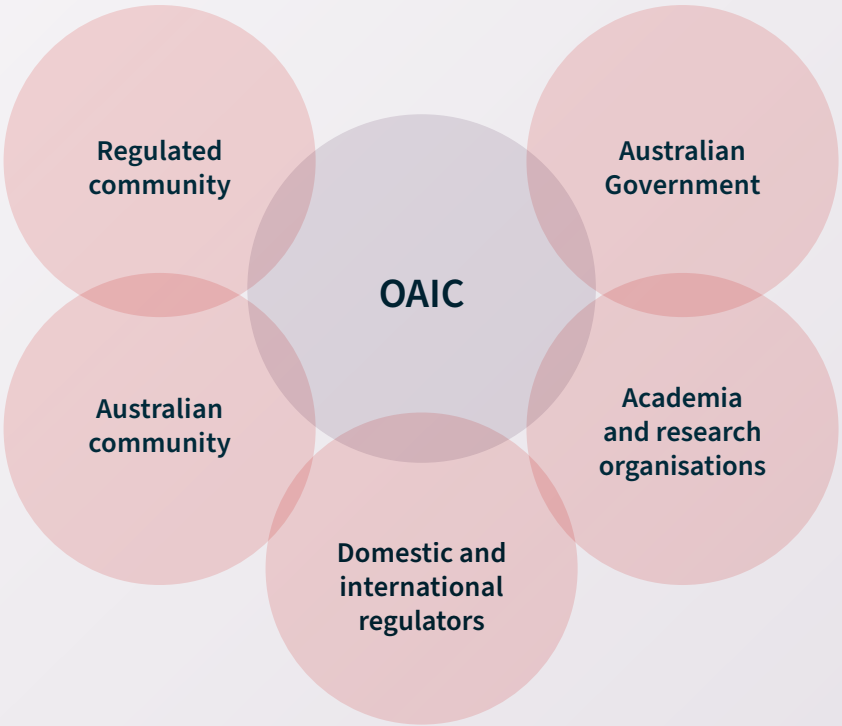
## Our cooperation and collaboration

The OAIC continues to increase our focus on regulatory cooperation by collaborating and sharing our expertise in the interests of minimising the risk of harm to the community.

We work closely with a range of organisations, including Australian Government agencies, domestic and international regulators, and industry, research and community organisations.

In our work resolving privacy and FOI matters and in performing our regulatory functions, the OAIC is procedurally fair, transparent and responsive in ways that are consistent with the principles of regulator best practice. Publication of OAIC priorities, guidelines and decisions provides transparency to regulated entities.

**Our cooperation and collaboration**




**Regulated community**
- Industry
- Australian Government agencies

**Australian community**
- Community groups
- Consumer advocacy organisations
- Australian Financial Complaints Authority
- External dispute resolution schemes

**Domestic and international regulators**
- State and territory regulators
- Complementary regulators
- International regulators

**Academia and research organisations**
- Universities

**Australian Government**
- Attorney-General's Department
- Australian Communications and Media Authority
- Australian Competition and Consumer Commission
- Australian Digital Health Agency
- Australian Prudential Regulation Authority
- Australian Securities and Investments Commission
- Commonwealth Ombudsman
- Department of Employment and Workplace Relations
- Department of Finance
- eSafety Commissioner
- Office of the National Data Commissioner
- Treasury

## Privacy regulation

Now in its third year of operation, DP-REG brings together the OAIC, Australian Communications and Media Authority (ACMA), Australian Competition and Consumer Commission (ACCC) and eSafety Commissioner to share information about and collaborate on cross-cutting issues and activities to address the risks and harms faced by Australians in the online environment. Members of DP-REG continue to increase collaboration and build capacity for the forum.

DP-REG regularly considers how competition, consumer protection, privacy, online safety and data issues intersect. The forum helps to support a streamlined and cohesive approach to the regulation of digital platforms as we advance online privacy protections for Australians.

The OAIC has 2 memoranda of understanding with the ACCC. The first supports the co-regulation of the CDR. The second guides and facilitates collaboration, information sharing, cooperation and mutual assistance in areas other than the CDR. We have similar memoranda of understanding with the Australian Prudential Regulation Authority (APRA) and Australian Securities and Investments Commission.

The OAIC also works closely with the ACCC in connection with Australia's expanded Digital ID system, under which both agencies have different regulatory roles.

As the work connected with the Australian Government's response to the review of the Privacy Act progresses, we will continue to bring our regulatory experience to the Attorney-General's Department to design a privacy framework that is fit for purpose in the digital age.

We engage with the Office of the National Data Commissioner on supporting the sharing and use of government-held information under the *Data Availability and Transparency Act 2022* and protecting personal information within the scheme.

As a founding member and co-chair of the Cyber Security Regulator Network (CSRN), we collaborate with APRA, ASIC, the ACMA and the ACCC to meet the challenges posed by the current environment. The CSRN works to reduce duplication or gaps in regulatory responses and improve the effectiveness and efficiency of regulatory activity.

The OAIC provides targeted, relevant and constructive advice to the Australian Government on a range of national reforms that impact privacy, including Digital ID, cyber security and online government services. Our advice focuses on ensuring reforms preserve and raise privacy standards. We also work to improve privacy protections and promote best practice with agencies such as the Australian Digital Health Agency, Services Australia, the Department of Home Affairs and the Department of Health and Aged Care.

The OAIC also cooperates with state and territory privacy regulators to share information and insights through Privacy Authorities Australia.

## Access to information

The OAIC assists Australian Government agencies and ministers to improve processes and increase knowledge and understanding of the *Freedom of Information Act 1982* (FOI Act).

The OAIC engages with FOI practitioners through regular stakeholder meetings, including commissioner-level engagement with agency heads, training sessions for members of our Information Contact Officer Network, newsletters and other direct communication. We regularly inform FOI practitioners of key decisions, investigation outcomes, our regulatory priorities and expectations, and upcoming process changes and consultations.

We also engage with the senior Commonwealth FOI leadership group, comprising Senior Executive Service (SES) Band 1 officers. A key purpose of this group is to foster greater leadership across the Australian Government around information access, with a view to improving the administration of the FOI Act and increasing the proactive disclosure of government-held information. Matters discussed at meetings include examples of best practice and innovation, and information access issues and practices across agencies.

The OAIC also actively collaborates with other information access regulators through the Association of Information Access Commissioners, which promotes best practice in information access policies and laws across Australia and New Zealand.

## International cooperation

International cooperation is essential to leverage understanding of the global privacy and information access landscape and ensure domestic frameworks are fit for purpose and aligned with best practice. The OAIC's international work complements and informs our domestic activities to advance privacy, access to information and information management.

The OAIC engages in several key international forums and networks to keep informed of challenges and opportunities in privacy and access to information. This work includes our involvement in the Global Privacy Assembly, the premier global forum for data protection and privacy authorities for more than 4 decades, and the International Conference of Information Commissioners (ICIC), a platform that connects member information commissioners responsible for the protection and promotion of access to information, to improve transparency and accountability.

The OAIC was appointed to the ICIC's 8-member Executive Committee in June 2024 for a 3-year term. Through this role, we provide international leadership to foster the protection and promotion of access to information as a fundamental pillar of social, economic and democratic governance.

The OAIC actively considers opportunities to engage in joint regulatory actions. Established memoranda of understanding with the United Kingdom's Information Commissioner's Office, Irish Data Protection Commission, Personal Data Protection Commission of Singapore and the New Zealand Office of the Privacy Commissioner are essential for identifying opportunities for regulatory and enforcement cooperation, information sharing and joint investigations.

We continue to progress our joint investigation with the New Zealand Office of the Privacy Commissioner into the privacy practices of the Latitude group of companies, commenced in May 2023.

The OAIC also actively promotes information access rights internationally, including through working with fellow agencies. We continue to collaborate to assist emerging jurisdictions to develop FOI capability and fit-for-purpose frameworks by sharing our experiences and best practice.

# Governance, risk and integrity

Appropriate governance, risk and integrity arrangements are essential to the OAIC's ability to achieve our objectives and drive improvement in a way that maintains confidence in the agency, our decisions and actions.

## Governance

The OAIC is committed to transparency, accountability and good governance.

We recently returned to an operating model with 3 commissioners. To support this model, the OAIC has implemented a new overarching governance framework that focuses on process efficiency, collaborative leadership and supporting robust and strategic decision making.

The governance arrangements facilitate informed and timely decision making and ensure the OAIC is well positioned to harness the collective expertise of the 3 commissioners, executive and our people to address opportunities and challenges of the future.

### Governance Board

Comprising the 3 commissioners, the board is responsible for ensuring good governance of the OAIC and determining the agency's strategic objectives and priorities to ensure we can achieve our purpose and regulatory functions.

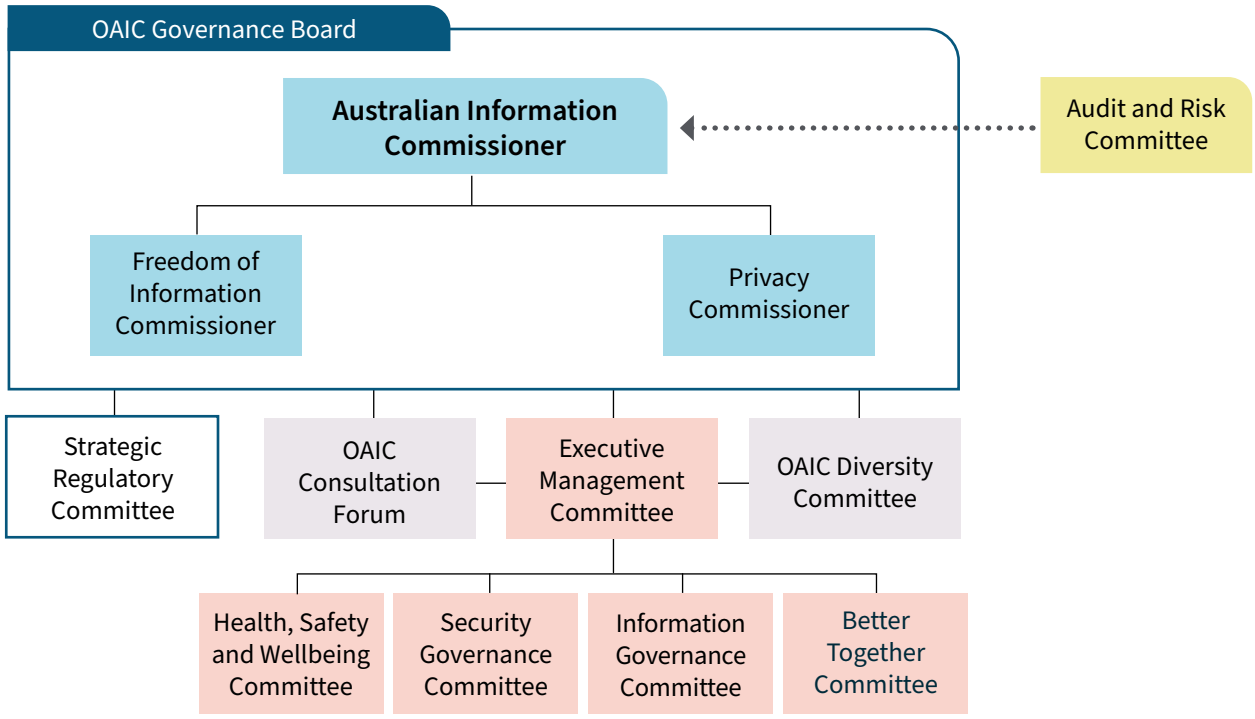
### Strategic Regulatory Committee

Comprising the 3 commissioners as independent statutory decision makers, this committee provides collective leadership and support for decision making on the OAIC's privacy and FOI regulatory approaches and information access functions.

### Executive Management Committee

Comprising all SES-level staff, this committee ensures executive oversight and engagement in the operational management of the OAIC.

**OAIC's governance structure**



### Audit and Risk Committee

This committee comprises members external to the OAIC who provide independent advice to the Information Commissioner and the Governance Board on the appropriateness of the OAIC's financial reporting, performance measures, systems of risk oversight and management, and systems of internal control.

### Function-based committees

The OAIC also has a range of internal function-based committees.

#### OAIC Consultation Forum

This forum facilitates consultation between the OAIC, our people and, where they choose, their representatives. It considers issues relating to implementing the OAIC Enterprise Agreement 2024–2027, policies and guidelines for working arrangements, and other matters affecting working arrangements.

#### OAIC Diversity Committee

This committee prepares the OAIC Workplace Diversity Strategy, implements actions under our Multicultural Access and Equity Plan, and champions diversity and multicultural activities across the agency to promote a fair, inclusive and productive workplace.

#### Better Together Committee

This committee focuses on fostering a 'OneOAIC' culture, which acknowledges all our people are an integral part of the agency and contribute to the delivery of our purpose – no matter where they are or what type of work they do.

#### Health, Safety and Wellbeing Committee

This committee facilitates cooperation between the OAIC and our people when instigating, developing and carrying out measures designed to ensure work health and safety. The committee helps ensure the OAIC complies with work health and safety legislative standards and requirements.

#### Security Governance Committee

This committee supports the chief security officer to understand the agency's security risks and determine appropriate mitigation strategies, monitor the OAIC's performance against the requirements of the Protective Security Policy Framework, and provide assurance to the Information Commissioner that the OAIC is meeting our protective security obligations.

#### Information Governance Committee

This committee ensures a consistent, systematic and OAIC-wide approach to managing information assets. It is responsible for OAIC record, information and data matters.

#### OAIC Social Committee

This committee organises social and networking opportunities for OAIC colleagues with the purpose of promoting a connected, collaborative workplace environment.

## Risk oversight and management

Our Risk Management Policy and Framework details our robust and holistic approach to risk oversight and management. It is aligned with the requirements of the *Public Governance, Performance and Accountability Act 2013* (PGPA Act) and the Commonwealth Risk Management Policy.

To implement the policy and framework and enable a consistent approach to risk management oversight, control and accountability, the OAIC has a range of tools and resources; training, monitoring and reporting activities; and escalation pathways.

The chief risk officer and director of governance and risk work collaboratively to oversee and champion risk management, risk capability and risk culture across the OAIC. The OAIC regularly reports to the Information Commissioner and executive through various governance committees, receives independent advice from the OAIC's Audit and Risk Committee, and has a robust internal audit program. This enables the OAIC to monitor and respond to current and emerging risks, threats and opportunities efficiently and effectively.

Our risk culture drives innovation and assists us in managing threats, embracing opportunities and empowering our people to make informed and risk-based decisions. The OAIC is committed to investing in the skills of our people and the continuous development of a positive risk culture in which people at every level can confidently and appropriately manage risk as part of their day-to-day work.

## Risk appetite

Our risk appetite is the amount and type of risk the OAIC is prepared to accept in pursuit of our objectives and is articulated in our risk appetite statement.

### Risk appetite statement

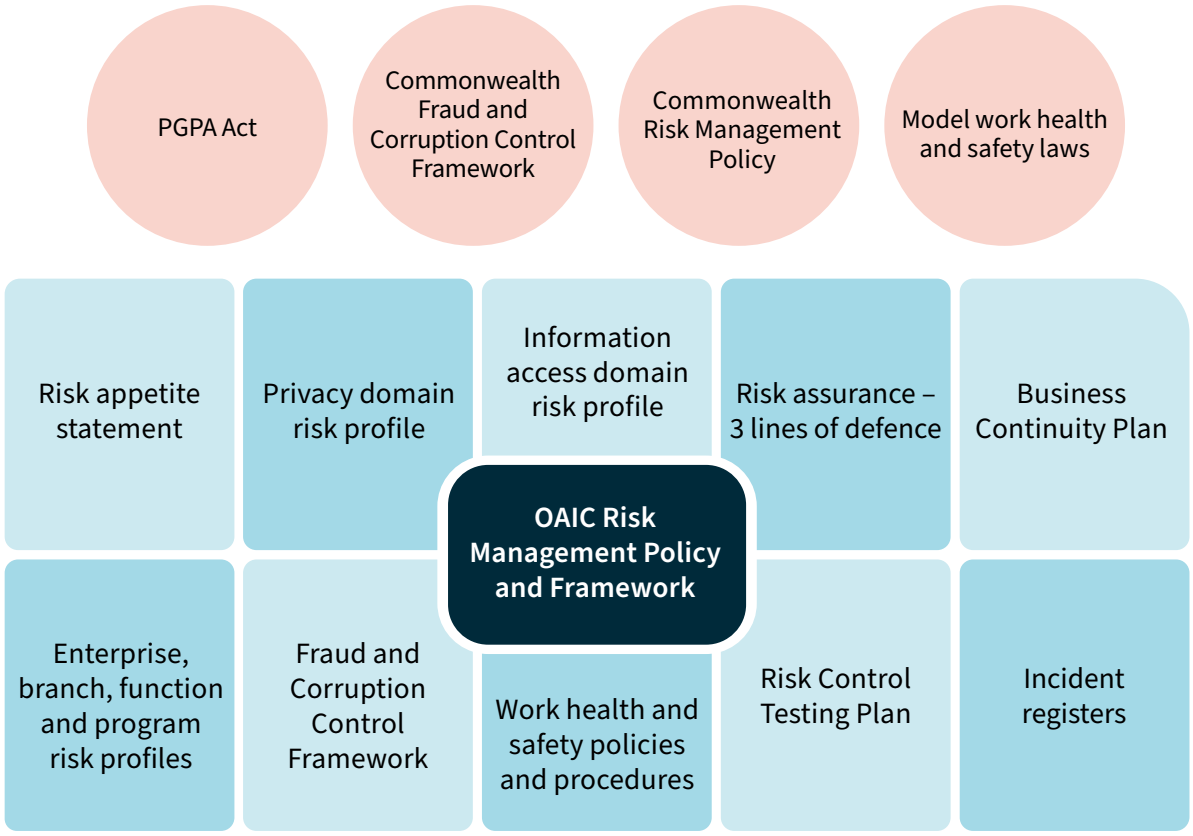
The OAIC has a crucial role to play in promoting and upholding privacy and information access rights. Australian citizens, businesses and our government have high expectations of us, and our work is subject to constant scrutiny. Effectively engaging with and managing risks is central to achieving our mission and key to meeting their expectations.

The effective management of risk plays an important role in shaping the OAIC's strategic priorities, contributes to well-informed organisational decision making and the delivery of our purpose.

We recognise in some circumstances, it is not possible or desirable to eliminate all risk and through accepting some degree of risk, we can seize opportunities, promote efficiencies and support innovation.

The OAIC is willing to accept higher levels of risk when the opportunities outweigh the consequences and when bold action is required. We also accept the very nature of risk is that sometimes when we take risks we will fail. We are all responsible for appropriately engaging with and managing risk, and in doing so we must be able to demonstrate we have made well-informed, evidence-based decisions.

### Risk management structure



### Table 2.1: Overview of the OAIC's tolerance for specific risk categories

| Risk category | Tolerance summary | |
|---|---|---|
| | **Lower tolerance** | **Higher tolerance** |
| **Our people** | • Activities or environments that adversely impact the health, safety or wellbeing of our people and visitors<br>• Risks that jeopardise our ability to recruit and retain people and best use their skills | • Recruiting above our average staffing level to maintain our workforce capability, flexible workplace arrangement and agile deployment models for our people |
| **Good governance and infrastructure** | • Compromise of any information entrusted to us<br>• Activities that may jeopardise security protections for our people and facilities<br>• Unethical behaviours<br>• Activities not representing value for money or contrary to legal advice<br>• Non-compliance with legislation | • Developing and trialling innovative and contemporary corporate processes<br>• Challenging red tape<br>• Embracing new ways of delivering our activities<br>• Leveraging expertise and experience from other Commonwealth entities through collaboration and cooperation |
| **Focus on outcomes** | • Behaviours or actions that risk the integrity of our regulatory activities<br>• Inability to respond flexibly to the evolving needs of government and our stakeholders<br>• Perception that we may be ineffective, poorly informed or inappropriately influenced in our judgements | • Challenging legacy processes and obstacles<br>• Delivering mechanisms that are more agile and responsive<br>• Taking a leadership position and working with our partners to drive positive transformational change in relation to privacy and information access<br>• Accepting that deprioritising some work may result in criticism |
| **Be community centric and stakeholder focused** | • Behaviours that counter a collegiate and collaborative environment<br>• Risks that we will not understand the views of the community or businesses<br>• Perception that we are not properly considering our position and consulting appropriately | • Maintaining our independence, influence and decision-making quality<br>• Exploring how we can provide more robust support for our stakeholders while protecting our impartiality<br>• Trialling new products to find innovative solutions<br>• Expanding and enriching our outreach arrangements |

We seek to achieve the optimal balance between identifying and engaging with risks in the context of delivering our regulatory activities, while upholding our accountability obligations and reputation as a trusted government agency and advisor. Our risk appetite statement is one of several documents and strategies that assist us to develop a better understanding of risk. An understanding of risk enables us to embrace opportunities, deal with threats, foster innovation and build a strong risk culture across the OAIC.

During 2024–25, we will review our domain risk profiles, risk appetite statement and tolerance levels to capture the strategic focus and risk approach of the agency as we adapt to an operating model with 3 commissioners. We will use this to inform our future regulatory posture and enterprise risk management activities.

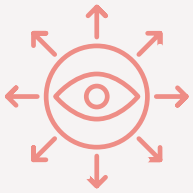
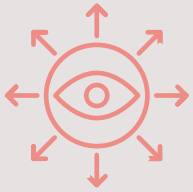
## Our enterprise risks

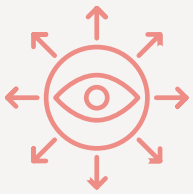
Our enterprise risk profile provides a high-level and overarching view of the risks that have the most profound impact on our ability to deliver our strategic and operational priorities. Regular review of the register and engagement with risk, control and treatment owners enables us to understand and respond in a timely manner to the current and emerging risks that may threaten – or present an opportunity for – our operations.

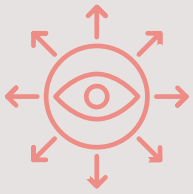
We regularly assess the broader risk landscape we operate in to manage the potential impacts it may have on our ability to deliver our regulatory objectives. These are captured in domain risk profiles and monitored and escalated through our governance processes. Project- and program-level risks are captured within subject-specific risk profiles.

Our focus in 2024–25 is to ensure transparent and consistent alignment of our agency risk appetite and tolerance levels throughout our Risk Management Policy and Framework and enterprise risk profile. We will achieve this through the design of real-time reporting and analysis and tools to support practical risk management and decision making using this information.

### Table 2.2: Enterprise risks and risk management strategies

| Risk category | Enterprise risk | Risk management strategies |
|---|---|---|
| **Our people** | The OAIC is not able to attract, grow and retain our people. | **Current:**<br>• Comprehensive and supportive welcome pack and induction program<br>• In-house recruitment and learning and development specialists<br>• Hybrid working arrangements, supported by appropriate principles and policies<br>• Learning and development program<br>• Internal and external secondment opportunities<br>• Support for professional association membership and certification for our people<br>• Staff engagement through consultation forums, meetings, surveys and exit interviews with strategies based on results from these engagements<br>**Future:**<br>• Changes to our recruitment processes, including implementation of an e-recruitment system |
|  **Focus on outcomes** | The OAIC is not able to strategically prioritise our work to deliver statutory functions. | **Current:**<br>• Strategic Regulatory Committee monitors and provides advice on the regulatory landscape<br>• Identification and publication of regulatory priorities<br>• Enhanced systems and reporting functionality<br>• Strategic and corporate planning<br>• Surge capacity to respond to changing priorities<br>**Future:**<br>• Strategies to enable agility in resource allocation<br>• Stakeholder management strategy |
|  **Focus on outcomes** | The OAIC does not contribute to increased trust and confidence in privacy and information access. | **Current:**<br>• Publication of commissioner decisions and complaints outcomes and regulatory priorities<br>• Inter-agency cooperation and coordination of activities and communication<br>• Performance measurement framework and stakeholder survey<br>• Public awareness campaigns and stakeholder communications<br>• Active engagement with domestic and international counterparts<br>• Active engagement with agency leaders on access to information matters<br>**Future:**<br>• Explore opportunities to publicly present the work of the OAIC and campaigns to highlight the importance of FOI and privacy<br>• Consider reference groups and advisory committees for engagement on key issues |

| Risk category | Enterprise risk | Risk management strategies |
|---|---|---|
|  **Focus on outcomes** | The OAIC does not have quality regulatory processes, systems and products. | **Current:**<br>• Governance oversight over processes, systems and activities<br>• Proactive review and continuous improvement of policies, processes and systems<br>• Technical systems and secure network to support information handling and storage<br>• Ongoing capability building across the agency<br>• Implementation of a data warehouse<br>• Internal audit activities to inform any gaps and recommend improvements<br>**Future:**<br>• Review technological solutions available to business areas across the agency |
| **Be community centric and stakeholder focused** | The OAIC is not able to build and maintain strong influence and positive relationships. | **Current:**<br>• Media monitoring and response<br>• Performance measurement framework contains an evaluation of stakeholder views<br>• Participation in domestic and international forums<br>• Commitment to effective relationship management as part of our work<br>**Future:**<br>• Additional training to enhance awareness and capability in relationship management in the regulatory environment |
| **Good governance and infrastructure** | The OAIC does not have robust governance. | **Current:**<br>• Well-established governance and specialist committees<br>• Implementation of an overarching governance framework<br>• Designated Governance and Risk team<br>• Specialist boards and steering committees to inform significant projects and programs<br>• External Audit and Risk Committee and independent internal audit program<br>• Compliance reporting schedule<br>**Future:**<br>• Further enhance our people's capability through targeted learning and development opportunities<br>• Develop additional tools and resources to support governance processes, including consideration of possible technical solutions |
| **Our people** | The OAIC does not provide a safe and healthy work environment. | **Current:**<br>• SES-level work health and safety lead<br>• Work health and safety and emergency response policies and procedures, including a psychosocial hazard and risk assessment<br>• Home-based Work Policy, including security and ergonomic requirements and assessment tools<br>• Incident reporting and hazard inspection program<br>• Training and exercises for our people<br>• Employee assistance program and regular wellbeing check-ins for frontline staff<br>• Governance and oversight through committees<br>**Future:**<br>• Provide specialist training for our people, including managers, such as mental first aid and domestic violence awareness |

| Risk category | Enterprise risk | Risk management strategies |
|---|---|---|
| **Good governance and infrastructure** | The OAIC does not protect the information entrusted to us. | **Current:**<br>• Privacy management and data breach response plans and system controls<br>• Appointment of chief information officer, chief privacy officer, chief information governance officer and chief security officer<br>• Protected ICT network<br>• Mandatory annual security and privacy training for all our people<br>• Requirements and guidelines for information security during hybrid work<br>• Information security audits and process reviews<br>• Information management and security policies and procedures, aligned with government information management standards and protective security requirements<br>**Future:**<br>• Contemporary and ongoing discussions about new information handling practices resulting from changes in the regulatory environment and the way we conduct our work |
|  **Focus on outcomes** | The OAIC does not meet the expectations of contemporary regulation. | **Current:**<br>• Regulatory governance committees monitor and provide guidance and advice on current and emerging issues<br>• Proactive engagement with stakeholders and active media campaigns<br>• Collaboration and information sharing with other domestic and international regulators<br>• Proportionate regulatory action taken in line with published policies and legislative powers<br>• Performance measurement framework contains an evaluation of stakeholder views<br>**Future:**<br>• Strategies and planning to expand team capabilities and agility to enable the agency to respond efficiently and effectively to changing priorities |

## Integrity

The OAIC aims to foster a culture that embeds the highest professional standards and integrity into all aspects of our work.

We will develop a framework that brings together our existing integrity policies and procedures into a holistic and centralised structure, providing consolidated expectations and guidance for our people and stakeholders on integrity issues.

To complement this, we are developing an integrity strategy that will detail our approach to building the capability of our people and process maturity to ensure continuous development of our pro-integrity culture. Our strategy will be aligned with the Australian Government's APS Reform agenda and the principles of the Commonwealth Integrity Maturity Framework.

Our commitment and focus will include:

- ensuring and improving the accessibility and variety of reporting channels for integrity matters
- enhancing our capability to respond to integrity issues
- providing preventative and awareness education and activities
- designing practical tools and resources to support our people, especially our managers
- ensuring alignment of existing policies, procedures and systems with the requirements of the new Commonwealth Fraud and Corruption Control Framework.

# Part 3

## Performance measurement framework

Our performance measurement framework describes how we measure our progress towards achieving our mission and purpose through:

- key activities that describe our key functions and areas of work
- intended results that describe the impact, difference or results we want to achieve in relation to our key activities
- performance measures we use to evaluate our progress towards the intended results
- targets that describe the results we are aiming for in each performance measure
- methodologies and data sources that describe how our performance information is collected, analysed and reported.

To assess achievement against our key activities, we use a mix of output, effectiveness and efficiency measures:

- **Output measures** assess the quantity and quality of the goods and services produced by an activity.
- **Effectiveness measures** assess whether the activities have had the intended impact.
- **Efficiency measures** assess the cost of producing a unit of output. Measuring efficiency within the OAIC is difficult given the nature of our outputs, which are not standardised. Accordingly, we have used proxy efficiency measures based on enquiry resolution times.

This mix of measures helps us achieve an appropriate balance in our reported performance information and enables an unbiased assessment of our results at the end of the performance cycle.

Our performance management framework is reflected in our 2024–25 portfolio budget statement (PBS).

# Key activity 1

## Influence and uphold privacy and information access rights frameworks

Intended result 1.1 is the OAIC's activities support the effective regulation of the Consumer Data Right (CDR).

### Table 3.1: Intended result 1.1

| Performance measure | 2024–25 target | 2025–26 target | 2026–27 target | Methodology/ data source | Type |
|---|---|---|---|---|---|
| **1.1** Effectiveness of the OAIC's contribution to the regulation of the CDR as measured by stakeholder feedback<br>Metric: Average performance rating from stakeholders based on a composite survey-based performance index | Prior year's result exceeded | Prior year's result exceeded | Prior year's result exceeded | Annual stakeholder survey conducted by an independent professional provider | Effectiveness |

Intended result 1.2 is the OAIC's activities support the effective regulation of the Digital ID system.

### Table 3.2: Intended result 1.2

| Performance measure | 2024–25 target | 2025–26 target | 2026–27 target | Methodology/ data source | Type |
|---|---|---|---|---|---|
| **1.2** Effectiveness of the OAIC's contribution to the regulation of the Digital ID system as measured by stakeholder feedback<br>Metric: Average performance rating from stakeholders based on a composite survey-based performance index | Baseline result established | Prior year's result exceeded | Prior year's result exceeded | Annual stakeholder survey conducted by an independent professional provider | Effectiveness |

Intended result 1.3 is the OAIC's regulatory outputs are timely.

**Table 3.3: Intended result 1.3**

| Performance measure | 2024–25 target | 2025–26 target | 2026–27 target | Methodology/ data source | Type |
|---|---|---|---|---|---|
| **1.3.1** Time taken to finalise privacy complaints | 80% of privacy complaints are finalised within 12 months | 80% of privacy complaints are finalised within 12 months | 80% of privacy complaints are finalised within 12 months | OAIC information management system | Output |
| **1.3.2** Time taken to finalise privacy and freedom of information (FOI) Commissioner-initiated investigations (CIIs) | 80% of CIIs are finalised within 12 months | 80% of CIIs are finalised within 12 months | 80% of CIIs are finalised within 12 months | OAIC information management system | Output |
| **1.3.3** Time taken to finalise Notifiable Data Breaches (NDBs) | 80% of NDBs are finalised within 60 days | 80% of NDBs are finalised within 60 days | 80% of NDBs are finalised within 60 days | OAIC information management system | Output |
| **1.3.4** Time taken to finalise My Health Record notifications | 80% of My Health Record notifications are finalised within 60 days | 80% of My Health Record notifications are finalised within 60 days | 80% of My Health Record notifications are finalised within 60 days | OAIC information management system | Output |
| **1.3.5** Time taken to finalise Information Commissioner reviews (IC reviews) of FOI decisions made by agencies and ministers | 80% of IC reviews are finalised within 12 months | 80% of IC reviews are finalised within 12 months | 80% of IC reviews are finalised within 12 months | OAIC information management system | Output |
| **1.3.6** Time taken to finalise FOI complaints | 80% of FOI complaints are finalised within 12 months | 80% of FOI complaints are finalised within 12 months | 80% of FOI complaints are finalised within 12 months | OAIC information management system | Output |
| **1.3.7** Time taken to finalise written privacy and information access enquiries from the public | 90% of written enquiries are finalised within 10 working days | 90% of written enquiries are finalised within 10 working days | 90% of written enquiries are finalised within 10 working days | OAIC information management system | Output |

## Key activity 2

### Advance online privacy protections for Australians

Intended result 2 is the OAIC's activities support innovation and capacity for Australian businesses to benefit from using data, while minimising privacy risks for the community.

**Table 3.4: Intended result 2**

| Performance measure | 2024–25 target | 2025–26 target | 2026–27 target | Methodology/ data source | Type |
|---|---|---|---|---|---|
| **2.1** Effectiveness of the OAIC's contribution to the advancement of online privacy protections and policy advice as measured by stakeholder feedback<br>Metric: Average performance rating from stakeholders based on a composite survey-based performance index | Prior year's result exceeded | Prior year's result exceeded | Prior year's result exceeded | Annual stakeholder survey conducted by an independent professional provider | Effectiveness |

## Key activity 3

### Encourage and support proactive release of government information

Intended result 3 is the OAIC's activities support Australian Government agencies to provide quick access to information requested and at the lowest reasonable cost, and proactively publish information of interest to the community.

**Table 3.5: Intended result 3**

| Performance measure | 2024–25 target | 2025–26 target | 2026–27 target | Methodology/ data source | Type |
|---|---|---|---|---|---|
| **3.1** Percentage of OAIC recommendations accepted by agencies following FOI complaint investigations | 90% | 90% | 90% | OAIC information management system | Effectiveness |
| **3.2** Effectiveness of the OAIC's advice and guidance on FOI obligations and the Information Publication Scheme in supporting government agencies to provide public access to government-held information, as measured by stakeholder feedback<br>Metric: Average performance rating from stakeholders based on a composite survey-based performance index | Prior year's result exceeded | Prior year's result exceeded | Prior year's result exceeded | Annual stakeholder survey conducted by an independent professional provider | Effectiveness |

## Key activity 4

### Take a contemporary, harms-based approach to regulation

Intended result 4 is the OAIC's approach to our regulatory role is consistent with better practice principles.

**Table 3.6: Intended result 4**

| Performance measure | 2024–25 target | 2025–26 target | 2026–27 target | Methodology/ data source | Type |
|---|---|---|---|---|---|
| **4.1** Stakeholder assessment of the extent to which the OAIC's regulatory activities demonstrate a commitment to continuous improvement and building trust<br>Metric: Average performance rating from stakeholders based on a composite survey-based performance index | Prior year's result exceeded | Prior year's result exceeded | Prior year's result exceeded | Annual stakeholder survey conducted by an independent professional provider | Effectiveness |
| **4.2** Stakeholder assessment of the extent to which the OAIC's regulatory activities demonstrate collaboration and engagement with stakeholders<br>Metric: Average performance rating from stakeholders based on a composite survey-based performance index | Prior year's result exceeded | Prior year's result exceeded | Prior year's result exceeded | Annual stakeholder survey conducted by an independent professional provider | Effectiveness |
| **4.3** Stakeholder assessment of the extent to which the OAIC's regulatory activities are based on risk and data<br>Metric: Average performance rating from stakeholders based on a composite survey-based performance index | Prior year's result exceeded | Prior year's result exceeded | Prior year's result exceeded | Annual stakeholder survey conducted by an independent professional provider | Effectiveness |
| **4.4** Number of stakeholder engagement activities<br>Metric: Number of activities delivered via different engagement mechanisms | Targets not appropriate due to fluctuations in nature and complexity of policy environment in any given year | Targets not appropriate due to fluctuations in nature and complexity of policy environment in any given year | Targets not appropriate due to fluctuations in nature and complexity of policy environment in any given year | Data snapshot demonstrating key formal engagements supplemented by case studies to demonstrate breadth, variety and effectiveness of engagement activities and modes of delivery | Effectiveness |
| **4.5** Average call duration of telephone enquiries to the OAIC public enquiry line | Lower than prior year's result | Lower than prior year's result | Lower than prior year's result | OAIC information management system | Efficiency |

## Alignment with our PBS

The following table describes the alignment between our outcome and program structure described in our 2024–25 PBS and our *Corporate plan 2024–25* purposes and key activities.

**Table 3.7: Intended result 2**

| **PBS 2024–25 outcome statement** | **PBS 2024–25 program** | ***Corporate plan 2024–25* purpose** | ***Corporate plan 2024–25* key activities** |
|---|---|---|---|
| Outcome 1: Provision of public access to Commonwealth Government information, protection of individuals' personal information, and performance of Information Commissioner, freedom of information and privacy functions | Program 1.1: Complaint handling, compliance and monitoring, and education and promotion | To promote and uphold privacy and information access rights | Influence and uphold privacy and information access rights frameworks |
| | | | Advance online privacy protections for Australians |
| | | | Encourage and support proactive release of government information |
| | | | Take a contemporary, harms-based approach to regulation. |

## Performance measures and performance indicators overview

We will measure our performance in 2024–25 against our set of 17 indicators grouped by 4 key activities.

### 1 Influence and uphold privacy and information access rights frameworks

**Intended result 1.1** is the OAIC's activities support the effective regulation of the Consumer Data Right (CDR).

**1.1** Effectiveness of the OAIC's contribution to the regulation of the CDR as measured by stakeholder feedback

**Intended result 1.2** is the OAIC's activities support the effective regulation of the Digital ID system.

**1.2** Effectiveness of the OAIC's contribution to the regulation of the Digital ID system as measured by stakeholder feedback

**Intended result 1.3** is the OAIC's regulatory outputs are timely.

**1.3.1** Time taken to finalise privacy complaints

**1.3.2** Time taken to finalise privacy and freedom of information (FOI) Commissioner-initiated investigations

**1.3.3** Time taken to finalise Notifiable Data Breaches

**1.3.4** Time taken to finalise My Health Record notifications

**1.3.5** Time taken to finalise Information Commissioner reviews of FOI decisions made by agencies and ministers

**1.3.6** Time taken to finalise FOI complaints

**1.3.7** Time taken to finalise written privacy and information access enquiries from the public

### 2 Advance online privacy protections for Australians

**Intended result 2** is the OAIC's activities support innovation and capacity for Australian businesses to benefit from using data, while minimising privacy risks for the community.

**2.1** Effectiveness of the OAIC's contribution to the advancement of online privacy protections and policy advice as measured by stakeholder feedback

### 3 Encourage and support proactive release of government information

**Intended result 3** is the OAIC's activities support Australian Government agencies to provide quick access to information requested and at the lowest reasonable cost, and proactively publish information of interest to the community.

**3.1** Percentage of OAIC recommendations accepted by agencies following FOI complaint investigations

**3.2** Effectiveness of the OAIC's advice and guidance on FOI obligations and the Information Publication Scheme in supporting government agencies to provide public access to government-held information, as measured by stakeholder feedback

### 4 Take a contemporary, harms-based approach to regulation

**Intended result 4** is the OAIC's approach to our regulatory role is consistent with better practice principles.

**4.1** Stakeholder assessment of the extent to which the OAIC's regulatory activities demonstrate a commitment to continuous improvement and building trust

**4.2** Stakeholder assessment of the extent to which the OAIC's regulatory activities demonstrate collaboration and engagement with stakeholders

**4.3** Stakeholder assessment of the extent to which the OAIC's regulatory activities are based on risk and data

**4.4** Number of stakeholder engagement activities

**4.5** Average call duration of telephone enquiries to the OAIC public enquiry line

Australian Government

Office of the Australian Information Commissioner

oaic.gov.au/corporate-plans

corporate@oaic.gov.au

OAIC