

1.2 Strategic Review governance

The Strategic Review has been overseen by the OAIC Strategic Review Steering Group, which comprises senior representatives from the OAIC, the AGD and the Department of Finance. The Steering Group is responsible for:

- developing the Terms of Reference, which were endorsed jointly by the OAIC Commissioners and the Secretary of the ADG
- engaging with the reviewer (Nous) during the Review to ensure relevant matters were considered
- providing feedback to the reviewer in relation to a draft review report
- considering the Review outcomes and providing advice on potential next steps.

1.3 Strategic Review method and data sources

The Strategic Review drew on a wide range of data sources, which are summarised in Figure 7. Appendix B contains a more detailed overview of the methodology and data sources, and details of the stakeholders the Strategic Review team engaged.

Figure 7 | Overview of key data sources for the Strategic Review



2 Overview of the OAIC

This chapter provides an overview of the OAIC. It outlines relevant context, including legislative responsibilities and functions, a snapshot of recent demand and performance, and key events that have affected the OAIC's operations.

Figure 8 | Summary of context

- The OAIC's core role is as regulator of FOI and privacy. Established in 2010 under the *Australian Information Commissioner Act 2010* (AIC Act), the OAIC is an independent statutory agency within the Attorney-General's portfolio. It administers the *Privacy Act 1988* (Privacy Act) and *Freedom of Information Act 1982* (FOI Act).
- The OAIC is responsible for protecting privacy and information access rights, and managing information policy in Australia. The OAIC's purpose is to promote and uphold privacy and information access rights. Through its regulation of privacy and information, the agency supports effective government, a strong Australian economy and human rights. Australia's national interest requires that the OAIC is well placed to perform its role.
- In recent years, the agency has experienced changes to Commissioners, Senate inquiries, and legislative reform giving the OAIC additional powers and responsibilities. Its remit has expanded to cover the CDR, the Notifiable Data Breaches scheme, the Digital ID and regulation of the COVIDSafe app.
- The OAIC must balance its resources across core non-discretionary work required under its legislation and more strategic and enabling work where it has greater discretion. It must broadly perform certain functions, such as managing privacy complaints and IC reviews, in line with demand for these functions. It can undertake other discretionary functions, such as investigations and assessments, in a more targeted and strategic manner.
- The OAIC's current structure, size and resourcing reflect its legislative responsibilities. The OAIC has 193 staff working across Australia and separated into five branches that cover privacy, FOI and CDR functions. The agency is currently led by the IC and PC – a dual role performed by a single individual – and the FOIC.
- The OAIC has experienced changes to its Commissioners and was involved in Senate inquiries in 2023. The FOIC role was left vacant from 2015 to mid-2021, while the PC and IC roles have been filled by a single individual since 2015. The FOI Senate Inquiry into the operation of the Commonwealth FOI laws saw considerable focus on the processes and resourcing of the OAIC's FOI Branch.
- Agency staff direct most of their efforts towards making decisions in respect of IC reviews and FOI complaints in the OAIC's FOI jurisdiction, and privacy complaints in its privacy jurisdiction.
- This focus on making decisions in respect of IC reviews and privacy complaints has meant that increased demand for these functions has been keenly felt across the organisation.
- The OAIC has implemented a series of initiatives in response to its evolving operating environment and greater size and scope. These initiatives have been effective in responding to changing demands in an evolving external landscape.
- The OAIC met most but not all performance measures in the past financial year. Key areas where it could improve to achieve its performance measures relate to the time taken to finalise IC reviews, Commissioner-initiated investigations (CIIs) and Notifiable Data Breaches (NDBs).

- Stakeholders reflected positively on the OAIC and its approach. The OAIC received its highest score for the regulation of CDR and its lowest score for the extent to which its activities are risk-based and data-driven.

2.1 The OAIC's legislative context

The OAIC's core role is as regulator of freedom of information and privacy rights

The OAIC is Australia's national privacy and information access regulator. Established in 2010 under the AIC Act, the OAIC is an independent statutory agency within the Attorney-General's portfolio that administers the Privacy Act and FOI Act.

The AIC Act sets out a range of the OAIC's functions, including:

- FOI functions, which are about giving the Australian community access to information held by the Government in accordance with the FOI Act (and other Acts)
- privacy functions, which are mainly about protecting the privacy of individuals in accordance with the Privacy Act (and other Acts)
- IC functions, which are strategic functions concerning Australian Government information management policy and practice.

The AIC Act also provides the IC with the ability to delegate powers and functions that are conferred on the IC under provisions in other legislation.

The OAIC is empowered to perform its privacy functions under the Privacy Act. These functions include regulating the handling of personal information, investigating complaints, conducting assessments and providing advice and guidance about privacy rights and obligations. Handling of privacy complaints is the most significant privacy function exercised by the OAIC (in terms of effort), and complaints can be lodged if an applicant is concerned that their personal information has been mishandled.

Under the FOI Act, the OAIC is responsible for protecting the public's right of access to government-held information. The Act empowers the OAIC to perform a range of functions, including reviewing decisions made by agencies and ministers under the FOI Act (IC reviews), handling FOI complaints, monitoring compliance with the FOI Act, and producing guidance to support the application of that Act. Most FOI matters received by the agency are IC review applications, which can be requested if an applicant disagrees with a decision made by an agency in response to an FOI request or if the agency has not made a decision within the time the FOI Act allows.

The OAIC regulates Australian Government entities and officials (in relation to FOI and privacy) and the private sector (in relation to privacy).

It is responsible for protecting privacy and information access rights, and managing information policy

The OAIC's purpose is to promote and uphold privacy and information access rights.¹⁸ Through its regulation of privacy and information access under the Privacy Act and the FOI Act, the agency supports effective government, a strong Australian economy and human rights. Australia's national interest requires that the OAIC is well placed to perform this role. This is a challenging ask of the agency as the privacy and

¹⁸ [OAIC Annual Report 2022-23](#).

FOI landscape is constantly evolving and the OAIC must be at the forefront of the Government's response to whole-of-society future challenges.

The OAIC's roles matter to Australians and to the Government. Eighty-four per cent of Australians want more control or choice over the collection and use of their personal data.¹⁹ Over 90 per cent of Australians believe it is important that they have a right to access government information.²⁰ The Attorney-General's Statement of Expectations for the OAIC acknowledges the OAIC's 'invaluable work' as it reorients elements of its mandate.

It has a broad remit, which the Government has expanded in recent years

The OAIC has a broad range of functions under around 37 different pieces of legislation, including the *Competition and Consumer Act 2010* (in relation to CDR), the *My Health Records Act 2012* and the Privacy (Credit Reporting) Code 2014.

The OAIC's remit has expanded in recent years. Legislative change has given the OAIC additional powers and responsibilities, including new information-gathering powers in the NDB scheme; information-sharing and enforcement powers; powers and functions under the Competition and Consumer (Consumer Data Right) Rules 2020; and privacy regulation of the Digital ID and the COVIDSafe app.

It must strike a balance between performing core non-discretionary work required under legislation and its discretionary strategic and enabling work

The OAIC has some discretion about how it performs its legislated functions. It must perform certain functions, such as managing privacy complaints and IC reviews, broadly in line with demand for these functions. Other functions, including investigations and assessments, are discretionary and can be undertaken in a more targeted and strategic manner.

The OAIC has many roles for an agency of its size, reflecting the breadth of primary and subordinate legislation that fall within its remit. As a result, its priorities and resourcing allocation need to be regularly reassessed for appropriateness.

The Strategic Review team developed a framework for mapping the OAIC's statutory functions by the following three categories:

- **CRITICAL** | Mandatory functions required by legislation that are critical responsibilities for meeting privacy and FOI obligations
- **STRATEGIC** | Other activities related to privacy and FOI that the OAIC is empowered – but not mandated – to exercise by legislation
- **SUPPORTING** | All other functions that, while not directly involved in the regulatory process, are vital for the OAIC to operate.

The functions in each category across the OAIC's core regulatory remit are shown in Figure 9. Appendix C provides more detail about statutory obligations mapped to the agency's functions.

¹⁹ OAIC, Australian Community Attitudes to Privacy Survey, August 2023, p 18.

²⁰ Information and Privacy Commission and Woolcott, Cross Jurisdictional Information Access Study, June 2023, p 6.

Figure 9 | Key functions and roles

	CRITICAL	STRATEGIC	SUPPORTING
PRIVACY	<ul style="list-style-type: none"> Assess privacy complaints Administer the Notifiable Data Breaches scheme Approve code development Develop and approve legislative instruments Develop legislative instruments 	<ul style="list-style-type: none"> Initiate privacy investigations Conduct privacy assessments Produce regulatory guidance for privacy legislation Develop research and educate the public on privacy (for example, the Australian Community Attitudes to Privacy Survey) Provide advice in relation to the operation of privacy functions Conduct monitoring for privacy functions 	
FOI	<ul style="list-style-type: none"> Assess IC reviews Assess and investigate FOI complaints Assess extension of time applications Assess vexatious applicant declaration applications Administer the Information Publication Scheme (IPS) 	<ul style="list-style-type: none"> Conduct FOI investigations Conduct FOI monitoring Prepare FOI guidelines Provide advice and training on matters relevant to the operation of the FOI Act 	
CDR	<ul style="list-style-type: none"> Monitor and manage the privacy and confidentiality functions of CDR 	<ul style="list-style-type: none"> Conduct CDR assessments Develop CDR regulatory guidance CDR monitoring for small businesses and individuals Develop CDR guidelines and provide advice 	
INFORMATION		<ul style="list-style-type: none"> Engage in information management policy development Perform strategic functions relating to information management in government 	

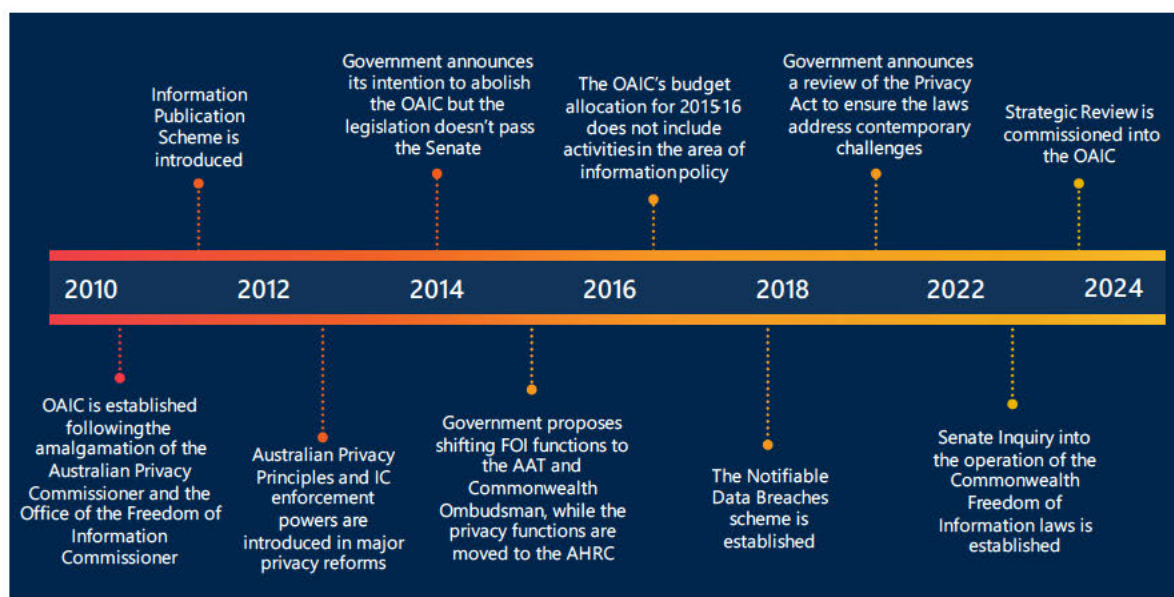
	CRITICAL	STRATEGIC	SUPPORTING
OTHER	<ul style="list-style-type: none"> Adhere to public service employment standards Ensure proper financial management and reporting Ensure workplace health and safety compliance 	<ul style="list-style-type: none"> Provide expert advice on privacy to government agencies and other entities involved in Digital ID development Provide guidance to healthcare providers on best practices for managing personal information within the My Health Record system 	<ul style="list-style-type: none"> Conduct people management and development Recruit staff and conduct onboarding Engage in data management and analytics Provide administrative and support services Conduct communication and engagement Create content and manage publication Manage technology systems Conduct procurement and resource management Abide by <i>Public Governance, Performance and Accountability Act 2013</i> (PGPA Act) requirements

2.2 The OAIC’s operating model

Since it was established in 2010, the OAIC has experienced significant changes that have required the agency to adapt and expand to respond to evolving needs and challenges in privacy protection and information management. The agency’s growing remit has required new functions, and it has had to respond to growing demand for FOI matters.

These key developments and reforms are outlined in Figure 10.

Figure 10 | Timeline of key events

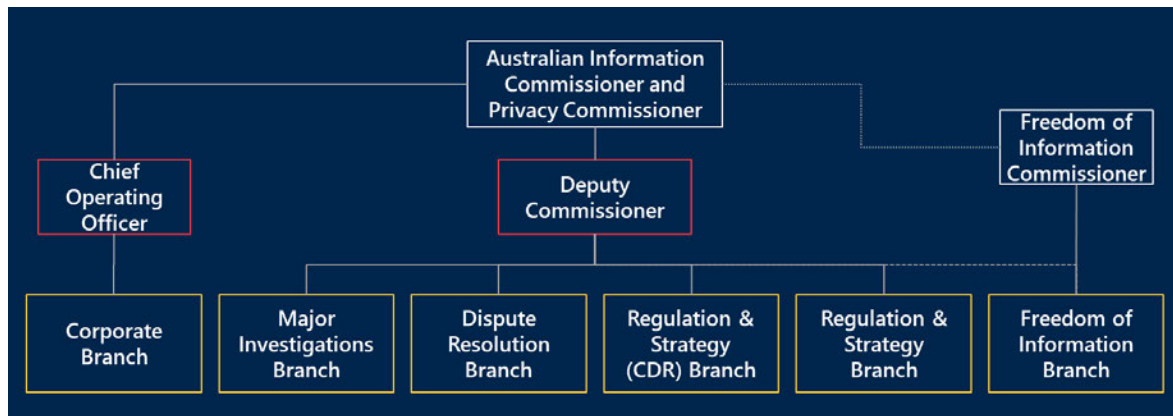


In 2014, the Government proposed abolishing the OAIC as part of its 'smaller government' agenda, with a proposal to move the OAIC's functions to other agencies. The legislation to dissolve the OAIC lapsed in the Senate at the end of 2014. **s 47C**

The current structure, size and resourcing reflect the agency's legislative responsibilities

The OAIC has 193 staff working across Australia and separated into five branches that cover privacy, FOI and CDR functions. The agency is currently led by the IC and PC – a dual role that is performed by a single individual – and the FOIC. The OAIC's structural arrangements are shown in Figure 11.

Figure 11 | OAIC structure



The agency received around \$46 million in funding in 2023-24, split evenly across ongoing and terminating funding. Over the past ten years, its total resourcing has increased significantly from an initial base of \$10 million. It has had a 117 per cent increase in ongoing funding over the decade and, since 2019, a considerable increase in funding for both ongoing base and terminating functions.

At least 37 different pieces of legislation confer functions, powers or responsibilities on the IC, or create requirements that other bodies consult with the IC on privacy matters.

An overview of the OAIC's current resourcing, staffing and structure is shown in Figure 12.

Figure 12 | Overview of resourcing, staffing and structure



The OAIC has adjusted to changes in Commissioners in recent years. The FOIC role was left vacant from 2015 to mid-2021, while the PC and IC roles have been fulfilled by a single individual since 2015. The decision to appoint three individuals to all three Commissioner roles was made in 2023 and will take effect in February 2024.

The agency has been the subject of several Senate inquiries in recent years. Most recently, the FOI Senate Inquiry focused on the processes and resourcing of the OAIC's FOI Branch, in addition to concerns raised about the agency's culture. The inquiry's recommendations are covered in more detail in chapter 3.

The OAIC has implemented reforms to its operating model in response to its changing operating environment and broader remit

The OAIC has made substantial changes across all elements of its operating model in the past few years in response to changing demands in an evolving external landscape. Key changes are shown in Figure 13.

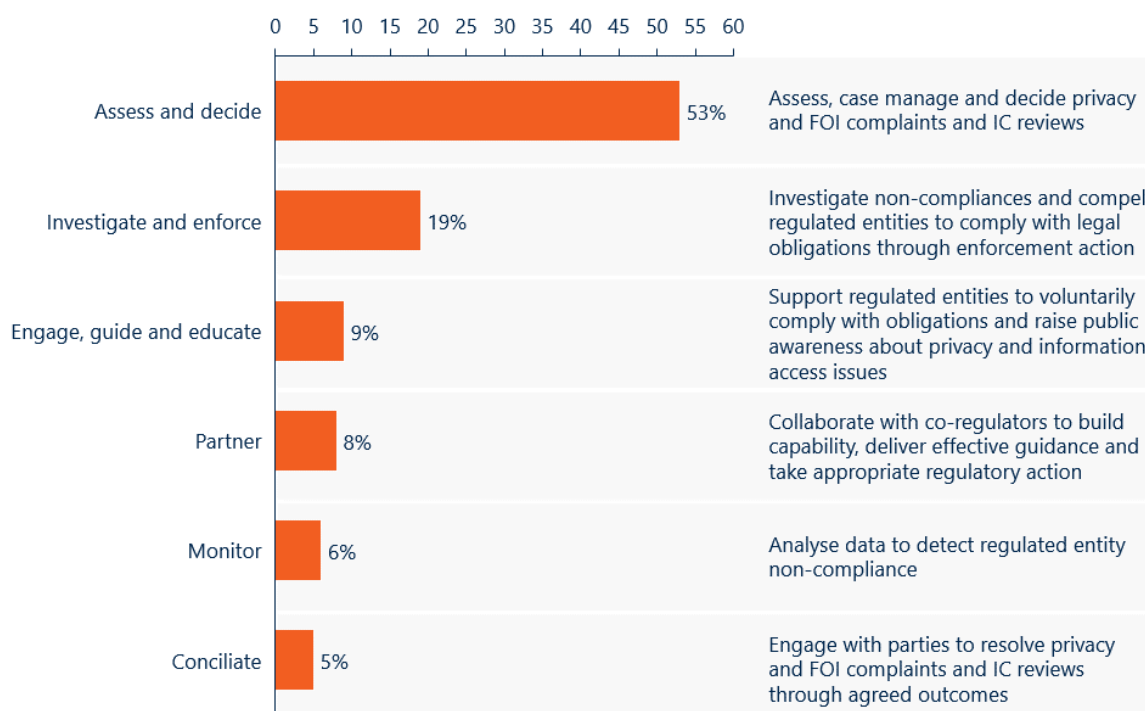
Figure 13 | Overview of recent reforms to the OAIC's operating model

<p>REGULATORY POSTURE</p> <p>Established the Major Investigations Branch in 2022-23 to carry out significant investigations – receiving dedicated funding for this work</p> <p>Issued its second civil penalty and began Federal Court proceedings against Australian Clinical Labs</p>	<p>EXTERNAL PARTNERSHIPS</p> <p>Began regulating CDR in close partnership with the ACCC</p> <p>Began collaborating with other regulators as part of the Digital Platforms Regulators Forum</p> <p>Partnered with the NZ Office of the Privacy Commissioner to investigate Latitude Financial Services</p> <p>Began participating in Global Privacy Assembly working groups and became co-chair of the Digital Citizen and Consumer Working Group</p>		
<p>GOVERNANCE</p> <p>Established the Regulatory Action Committee in 2020-21 to assess regulatory options for responding to significant and emerging privacy risks</p> <p>Delegated IC reviews to the FOI Assistant Commissioner in December 2022</p>	<p>STRUCTURE</p> <p>Changed the FOI Branch structure to address the case backlog</p> <p>Divided the Regulation and Strategy Branch into two sub-branches, with one focused on new work related to CDR</p> <p>Introduced the Corporate Branch, with a senior Assistant Commissioner position carrying out the role of the OAIC's Chief Operating Officer</p> <p>Transitioned the agency from a shared services model with the Australian Human Rights Commission to bringing financial and HR functions in-house</p> <p>Expanded the Corporate Branch to include a data and reporting team</p> <p>Introduced a Digital ID Implementation team</p>	<p>PROCESSES</p> <p>Launched new initiatives to improve the time taken to provide clearance for operational matters</p> <p>Introduced the Complaints Continuum Committee to improve oversight of privacy complaints</p>	
<p>WORKFORCE CAPABILITY</p> <p>Transitioned to a fully hybrid and remote working model and away from a Sydney-centric footprint</p> <p>Substantially increased number of staff from 127 to 183 (45%) in the year to June 2023</p>	<p>CULTURE & LEADERSHIP</p> <p>Recorded a significant increase in scores in the latest APS Census results on the back of the Census Roadmap initiatives</p>	<p>RESOURCING</p> <p>Received an increase in agency funding of approximately 53% between 2022-23 and 2023-24. However, 50% of the 2023-24 funding is terminating (short-term) funding to cover one-off initiatives</p>	<p>OTHER ENABLERS</p> <p>Initiated a Technology Systems Review to address systems limitations, focusing on the case and document management systems</p>

The majority of the OAIC's efforts are directed towards case management activities

The majority of the OAIC's staff effort is directed towards making decisions related to IC reviews and FOI complaints in the OAIC's FOI jurisdiction, and privacy complaints in the agency's privacy jurisdiction. These are broadly referred to as 'assess and decide' activities, which are outlined in Figure 14. Around 20 per cent of the OAIC's effort is directed towards investigation and enforcement activities; around 20 per cent is distributed across engage, guide and educate activities and partnering; and the remaining 10 per cent is applied to conciliation and monitoring.

Figure 14 | Allocation of regulatory effort²¹



Source: OAIC Workforce Allocation Survey

2.3 The OAIC's performance

The agency has continued to address its growing caseload while also performing its other significant functions, including monitoring, enforcement, regulatory guidance and advice.

Substantial staff effort is allocated to meeting demand for certain critical functions

The focus of OAIC staff effort on making decisions in respect of IC reviews and privacy complaints, as outlined above, has meant that increased demand for these functions has been keenly felt across the organisation.

The numbers of requests for IC reviews (see Figure 15) and privacy complaints (see Figure 16) have increased since the OAIC was established. As cases have grown faster than they have been resolved, the case backlog – as measured by the number of cases unresolved for more than 12 months – has risen. This has been most pronounced in the OAIC's IC review jurisdiction.

²¹ As assessed by the Strategic Review through a Workforce Allocation Survey that was circulated to all teams across the OAIC.

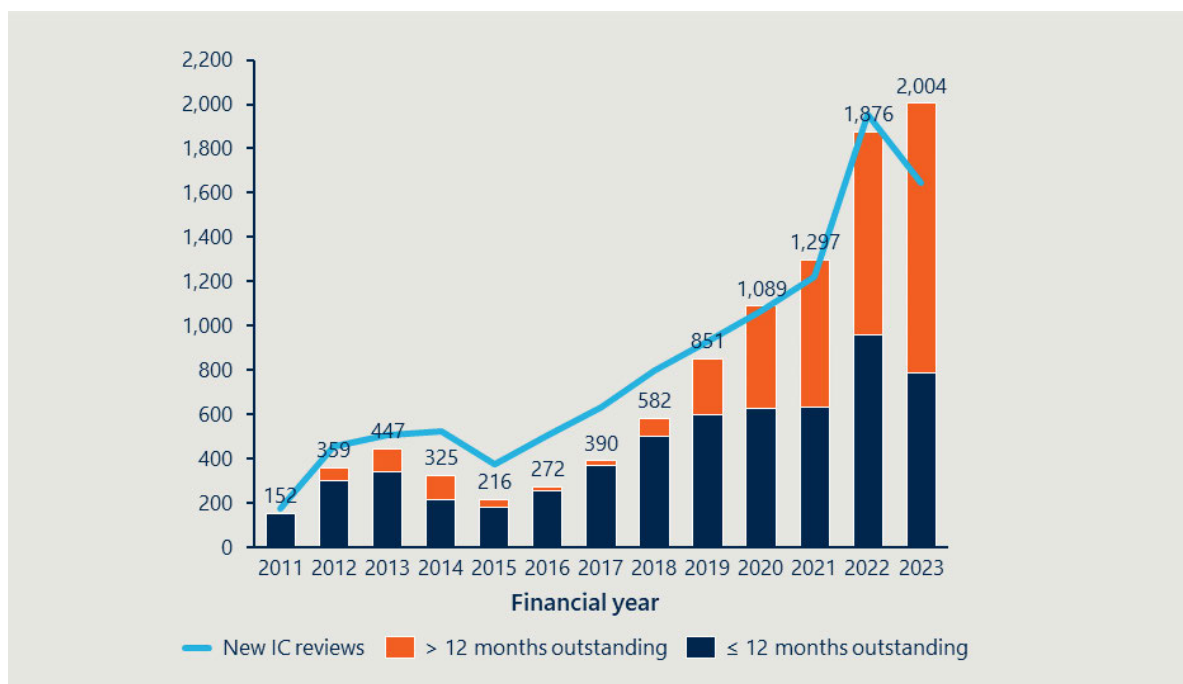
There are increasing numbers of applications for IC reviews of FOI decisions

The number of applications for IC reviews has increased steadily since 2015, with an average annual growth rate of 7 per cent over that period.

The increase in the number of IC reviews on hand is due to the backlog of IC reviews, the increasing complexity of applications seeking information relating to third-party individuals or national security matters, and an increase in the number of matters that are voluminous or raise multiple and overlapping exemption claims. Growth in the number of new IC review applications received and applications outstanding is shown in Figure 15.

As more IC review cases have been received by the OAIC than have been finalised in recent years, the number of cases over that are over 12 months old has steadily increased. There is no statutory timeframe for IC reviews but the OAIC's performance measures set a target of finalising 80 per cent of applications within 12 months. The average time taken to finalise an IC review in 2022-23 was 9.8 months.²²

Figure 15 | Number of IC reviews since 2011



Source: OAIC Annual Report 2013-14, OAIC Annual Report 2018-19, OAIC Annual Report 2022-23

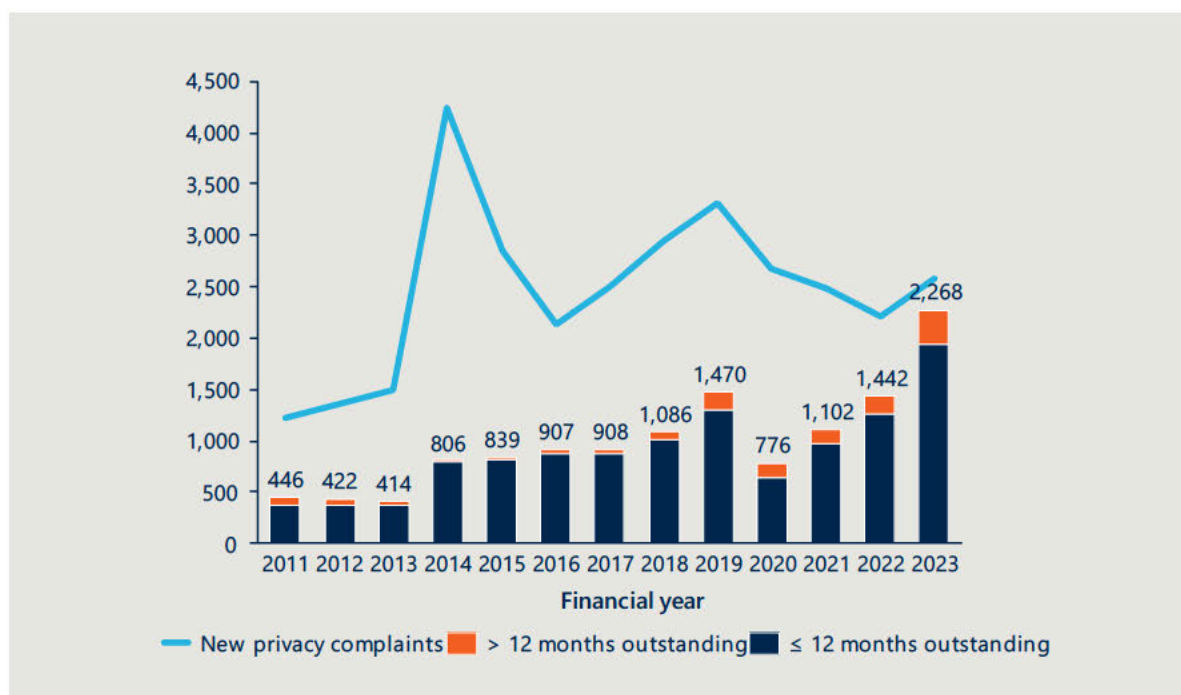
²² [OAIC Annual Report 2022-23](#).

The number of privacy complaints has fluctuated

Privacy complaints to the OAIC increased by 34 per cent in 2022-23 compared to 2021-22, but are below the 2014 peak.²³ Complaints have grown since 2011, as shown in Figure 16. As the OAIC has received more privacy complaints than it has finalised in recent years, the number of cases outstanding for more than 12 months has increased from low levels.

The increase in complaints relative to 2011 can largely be explained by a combination of increased public awareness of data privacy rights and greater use of digital services that handle personal data. A series of recent high-profile data breaches also elevated public concern about the handling of data, leading to a large uptick in privacy complaints over the past financial year.²⁴

Figure 16 | Numbers of privacy complaints since 2011



Source: OAIC Annual Report 2013-14, OAIC Annual Report 2018-19, OAIC Annual Report 2022-23

Most but not all performance measures were met in the past financial year

The OAIC Performance Measurement Framework outlines the agency's approach to evaluating its effectiveness in promoting and upholding privacy and information access rights, based on specific measures contained in its *Corporate Plan* and Portfolio Budget Statement.







Figure 17 shows how the OAIC performed last financial year against the subset of performance measures that relate to how the agency is performing its core roles. The OAIC met or was close to meeting all targets for five of the six selected performance measures. The performance measures cover a broad range of its regulatory activities, including significant functions that are unrelated to case management.²⁵

²³ The significant increase in privacy complaints in 2014-15 reflects approximately 1,000 complaints following an immigration data breach where the Department of Home Affairs published, in error, a detention report on its website that contained embedded personal information.

²⁴ The recent high-profile Optus, Medibank, Latitude Financial and Australian Clinical Labs data breaches have drawn attention to the handling of personal information.

²⁵ Overall, the OAIC achieved 69% (or 11 of 16) of its performance measures in FY23.

Figure 17 | Key Performance Outcomes 2022-23

PERFORMANCE MEASURE	TARGET	RESULT	OUTCOME
1.2.1 Time taken to finalise privacy complaints	80% of privacy complaints finalised within 12 months	84%	
1.2.2 Time taken to finalise privacy and FOI Commissioner-initiated investigations (CIIs)	80% of CIIs finalised within 8 months	68%	
1.2.3 Time taken to finalise Notifiable Data Breaches (NDBs)	80% of NDBs finalised within 60 days	77%	
1.2.4 Time taken to finalise My Health Record notifications	80% of My Health Record notifications finalised within 60 days	100%	
1.2.5 Time taken to finalise Information Commissioner (IC) reviews of FOI decisions made by agencies and Ministers	80% of IC reviews finalised within 12 months	78%	
1.2.6 Time taken to finalise FOI complaints	80% of FOI complaints finalised within 12 months	94%	

 Achieved  Not achieved

Source: OAIC Annual Report 2022-23

Stakeholders reflected positively on the OAIC and its approach

The OAIC conducted its first annual stakeholder survey in 2023 to establish a baseline for its regulatory performance.²⁶ The survey helped to assess the OAIC's performance against a number of performance measures.²⁷

Stakeholder feedback from the survey reflected a net positive view of the OAIC's collaborative efforts, giving an average score greater than 3 (where 1 = strongly disagree and 5 = strongly agree). The OAIC received its highest score for the regulation of CDR and its lowest score for the extent to which its activities are risk-based and data-driven.

Survey participants were generally satisfied with the OAIC's ability to:

- regulate and contribute to CDR (from the perspective of stakeholders involved in CDR regulation and engagement)
- raise awareness of opportunities to enhance online privacy legislation and online privacy risks
- provide guidance and advice on the operation of the IPS.

²⁶ The survey received responses from 102 stakeholders that work with the OAIC on issues relating to FOI (47), privacy (45) and CDR (10).

²⁷ These performance measures are: Effectiveness of the OAIC's contribution to the regulation of the Consumer Data Right; Effectiveness of the OAIC's contribution to the advancement of online privacy protections and policy advice; Effectiveness of the OAIC's advice and guidance on FOI obligations and the IPS in supporting government agencies to provide public access to government-held information; The extent to which the OAIC's regulatory activities demonstrate a commitment to continuous improvement and building trust; Extent to which to OAIC's regulatory activities demonstrate collaboration and engagement; and Extent to which the OAIC's regulatory activities are risk-based and data-driven.

3 Drivers of change

A range of economic, technological, social and political drivers will play key roles in shaping demand for the OAIC's work and its effectiveness as a regulator into the future. This chapter explores these drivers in detail and considers some of the likely implications for the OAIC's future regulatory strategy and elements of its operating model. It also provides important context for the findings and recommendations throughout this Strategic Review report.

Figure 18 | Relevant questions from the Terms of Reference

- How can the OAIC best respond to the likely continuing growth to the volume and complexity of its core statutory workload?
- How can the OAIC remain effective as a regulator in responding to changing technology, the growth of the digital economy and increasing cyber crime?

Figure 19 | Summary of key findings

TECHNOLOGICAL DRIVERS OF CHANGE

- Technological shifts will lead to new risks to privacy, and growing individual and community expectations that the OAIC will respond. As the digital transformation of our economy accelerates, the volume of data managed by entities regulated by the OAIC will continue to expand and the methods used to process this data will become ever more complex.
- Further developments in AI will have a profound impact on personal privacy. In response, the OAIC will need to develop regulatory guidance and enforce stricter controls on data sharing in respect of regulated entities.
- New technologies will challenge traditional frameworks for the protection of personal information. For example, biometric authentication and profiling systems continually collect vast amounts of data and are increasingly common. The OAIC's regulatory guidance will need to keep pace with these changes and provide clarity on emerging technologies and their potential impact on privacy.
- Data breaches are becoming larger in scale and more frequent amid growth in the digital economy and increasingly sophisticated cyber attacks. In response, the OAIC will need to play a role in ensuring organisations that collect personal information secure it effectively.
- Cyber crime is becoming more sophisticated and widespread, raising the risks to personal data security. The OAIC will need to contribute to government cyber security efforts and raise awareness through education initiatives.

SOCIAL DRIVERS OF CHANGE

- Changes in societal expectations are contributing to a desire for government to do more to uphold privacy and information access rights. Most Australians are now highly aware of their privacy rights due to recent large-scale data breaches, and they understand their right to access information held by public entities.
- The vast majority of Australians would like government agencies to act and do more to protect their personal information, including through legislative change. These expectations will likely lead to an increase in the OAIC's workload in relation to upholding privacy protections.

POLITICAL DRIVERS OF CHANGE

- The Government's expectations of the OAIC have evolved in response to increasing privacy harms. The OAIC is expected to take an approach that balances education of regulated entities to support voluntary compliance with enforcement to promote public confidence in the regulatory activities of the agency.
- Significant legislative and policy reforms and reviews – particularly the Privacy Act Review – will place greater demand on the OAIC. The proposed reforms from the Privacy Act Review will broaden the OAIC's enforcement powers and require updated regulatory guidance.
- The FOI Senate Inquiry's suggested reforms may require the OAIC to increase its engagement with agencies, meaning it will need to prioritise its efforts to develop guidance and build the capacity of decision-making agencies.
- In other areas of the OAIC's remit, expansions in scope and changes in legislation for CDR and Digital ID will require updated guidance.

The operating environment is changing – in particular, the rapid growth of the digital economy and advances in AI will have a profound impact on personal privacy

The privacy landscape for the OAIC over the next decade is likely to look markedly different to that of the past ten years. Advances in technology and the ongoing growth of the digital economy are expected to have a profound impact on personal privacy. Rapid growth in the sophistication and application of AI, new technologies such as biometric authentication and profiling, and the likelihood of larger and more frequent data breaches and increased cyber crime are combining to create a more complex and faster-evolving operating environment for the OAIC.

Societal expectations in relation to privacy protections are changing as technology evolves and data breaches become more frequent and more significant in their associated harms. Eighty-nine per cent of respondents to the Australian Community Attitudes to Privacy Survey 2023 would like government agencies to act and do more to protect their personal information.

Community expectations around accountability and transparency are increasing, with 91 per cent of respondents to the 2023 Australian Government Information Access Survey indicating it was important to them to have the right to access government information, up from 84 per cent in 2019.²⁸

In response to rapidly evolving technologies and societal expectations, the Government has initiated several reviews and reforms – most notably the Privacy Act Review – that will shape the OAIC's future functions and priorities.

Taken as a whole, these technological, social and political trends are expected to place increased demand on the OAIC's functions. The impact of these trends on the OAIC's functions is summarised at a macro level in Figure 20. The most significant impacts will be to the OAIC's privacy functions, as economy-wide digital transformation leads to vast amounts of data being hosted online, increasing the potential for large-scale data breaches and the need for enforcement action against regulated entities.

The remainder of this chapter explores technological, social and political trends that will shape the size and complexity of the OAIC's future statutory workload.

²⁸ [Australian Government Information Access Survey 2023](#).

s 47C

3.1 Technological drivers of change

Technological shifts will lead to new risks to privacy and a growing expectation among individuals and the community that the OAIC will respond

As the digital transformation of our economy accelerates, the volume of data managed by entities regulated by the OAIC will continue to expand and the methods used to process this data will become ever more complex.

Advances in AI and machine learning will lead to regulated entities using more sophisticated data processing techniques. This will place pressure on the OAIC to provide advice and develop guidelines on how technologies can be developed, used and stored in ways that meets privacy obligations.³⁰ Data breaches are becoming larger and more common as the amount of personal data being exchanged through digital platforms grows and rates of cyber crime increase. These breaches are linked to the regulatory context within which they occur, so the OAIC's actions and legislative reform will be important to prevent problematic data practices and behaviour by regulated entities.

Some of the most significant technological drivers of change and their likely implications for the OAIC in the coming years are summarised in Figure 21.

²⁹ Analysis assumes that the OAIC will see greater demand placed on some of its functions following the Government's decision in relation to the Privacy Act Review recommendations.

³⁰ Currently, it is unclear which regulator or regulatory scheme will address emerging issues linked to AI safety and AI ethics. In the absence of a dedicated AI regulator, the OAIC is well positioned to have a role in minimising harms from AI while maximising benefits.

Figure 21 | Technological drivers of change and the implications for the OAIC

Driver	Description	Evolving risk landscape	s47C
Growing use of AI	<ul style="list-style-type: none"> • Developments in AI will have a profound impact on personal privacy. Generative AI and large language models can collect personal data by making semi-hidden information more visible through reidentification, challenging the effectiveness of traditional privacy protections.³¹ • AI tools can combine personal information with misleading information, which will pose a new type of threat to individual privacy. • Like other participants in the economy, governments are increasingly using technology like AI to support decision-making. 	<ul style="list-style-type: none"> • Without greater regulatory guidance on the use of personal information in AI and enforcement of AI-related privacy breaches, there is potential for large-scale erosion of individual privacy. • The risk of AI tools being used to breach privacy is growing. Among Australian businesses, 68 per cent have already implemented AI technologies and a further 23 per cent are planning to implement them in the next 12 months.³² • Trust in government could be reduced without greater transparency in relation to AI-enhanced government decision-making. 	s 47C
New technologies that collect personal information	<ul style="list-style-type: none"> • New technologies will challenge traditional frameworks for the protection of personal information. Biometric authentication and profiling systems continually collect vast amounts of data. • This increases the volume of data to be protected and introduces potentially new forms of personal information that will need to be regulated. 	<ul style="list-style-type: none"> • Personal information could be hacked and misused without consequences if new technologies continue to be used to collect this information. • New technologies are collecting large volumes of personal information, with 83 per cent of Australians willing to use at least one biometric security technology in 2020.³⁴ 	s 47C

³¹ [Problematic Interactions between AI and Health Privacy](#).

³² [CSIRO Australia's AI Ecosystem Momentum Report \(Feb 2023\)](#).

³³ [Safe and responsible AI in Australia consultation: Australian Government's interim response](#).

³⁴ [Australian Institute of Criminology – Changing perceptions of biometric technologies](#), 2021.

Driver	Description	Evolving risk landscape
Larger and more frequent data breaches	<ul style="list-style-type: none"> Data breaches are becoming larger in scale and more frequent amid growth in the digital economy and increasingly sophisticated cyber attacks. Breaches are increasingly occurring in the health and financial services sectors. Increasing amounts of data are expected to be collected in these sectors, including as part of the expansion of My Health Record. 	<ul style="list-style-type: none"> If data breaches are left unchecked and not investigated thoroughly, risk of identity theft and fraud will increase and there will be a loss of public trust in digital services and institutions. The risk posed by these breaches is large and growing, with significant data breaches resulting in millions of Australians having their information stolen and leaked on the dark web in 2022.³⁵ The most recent data shows that around 70 per cent of breaches are the result of malicious or criminal attacks.³⁶
Increasing cyber crime	<ul style="list-style-type: none"> Cyber crime is becoming more sophisticated and widespread, raising the risks to personal data security. Phishing, ransomware attacks and other forms of malicious activities are aimed at illegally accessing and exploiting personal data. 	<ul style="list-style-type: none"> Without regulatory action, increasing cyber crime will lead to more significant financial and personal losses from cyber attacks. There were 94,000 cyber crime reports in 2022-23, reflecting a 23 per cent increase compared to the previous financial year.³⁷ Australians lost over \$3 billion to scams in 2022. This is an 80 per cent increase on total losses recorded the prior year.³⁸

s 47C

³⁵ [ASD Cyber Threat Report 2022-2023](#).

³⁶ [Notifiable Data Breaches Report: January to June 2023](#).

³⁷ [ASD Cyber Threat Report 2022-2023](#).

³⁸ [Targeting scams: report of the ACCC on scams activity 2022](#).

³⁹ [2023-2030 Australian Cyber Security Strategy](#).

3.2 Social drivers of change

Changes in societal expectations are contributing to a desire for government to do more to uphold privacy and information access rights

Societal expectations of individual privacy protection are changing as Australians become increasingly aware of their privacy rights and the importance of personal information security.⁴⁰ Awareness has grown following a number recent high-profile and large-scale data breaches that focused attention on online privacy and forced individuals to reflect on how their personal information is stored, managed and shared online.

The latest Australian Community Attitudes to Privacy Survey found that 62 per cent of Australians view the protection of their personal information as a major concern, but only 32 per cent feel in control of their data privacy. As a result, expectations about OAIC and broader government action are growing – 89 per cent of Australians would like government agencies to do more to protect their personal information, including through legislative change.⁴¹

Levels of public engagement on privacy issues and awareness of privacy rights are likely to increase, resulting in the OAIC needing to deal with more enquiries and complaints. When significant privacy breaches occur, expectations of government intervention are likely to increase, putting extra pressure on the OAIC's enforcement capacity.

Similarly, there is increasing public awareness of the right to access information held by public entities. Among respondents to the 2023 Australian Government Information Access Survey, 91 per cent indicated it was important to have the right to access government information, up from 84 per cent in 2019.⁴² Among respondents to the Information Access and Community Attitudes Study, 83 per cent agreed that public access to government information improves transparency and accountability.⁴³ This awareness will likely lead to more individuals exercising this right, increasing the volume of IC reviews and FOI complaints. Societal expectations reflect that the public wants more action to prevent government entities from delaying public requests for information or dealing with these requests inadequately.

⁴⁰ [Australian Community Attitudes to Privacy Survey, 2023.](#)

⁴¹ [Australian Community Attitudes to Privacy Survey, 2023.](#)

⁴² [Australian Government Information Access Survey 2023.](#)

⁴³ Office of the Victorian Information Commissioner, Cross Jurisdictional Information Access Study, May 2022.

3.3 Political drivers of change

The Government's expectations of the OAIC have evolved in response to increasing privacy harms

The Government clearly articulated its priorities for the OAIC in the Attorney-General's 2023 Statement of Expectations. It expects the OAIC to promote and regulate the protection of personal information in line with the objects of the Privacy Act and access to information through the operation of the FOI Act.⁴⁴

The Government acknowledges the increasing importance of the online environment for the economy, education and social connections. It expects the OAIC to focus on regulatory activities to address privacy harms that arise from the practices of online platforms and services that impact individuals' choice and control; promote awareness of privacy risks; provide guidance on how to protect personal information online; and take an integrated approach to embedding compliance and enforcement policies, project planning and risk management activities in respect of CDR. The Government also expects the OAIC to address privacy breaches and deal with entities that are not complying with privacy obligations. It also expects the agency to promote awareness and provide guidance on privacy risks to regulated entities and individuals.⁴⁵

Significant legislative and policy reforms and reviews – particularly the Privacy Act Review – will increase demand on the OAIC

The OAIC's remit will expand if the Government implements its recent legislative and policy reforms, with the most significant being the Privacy Act Review.

Some proposals in the Privacy Act Review will materially change certain functions the OAIC performs and introduce new functions. The proposals seek to bolster privacy protections, adapt policy guidance to the changing technology landscape and expand the OAIC's enforcement capabilities – for example, by empowering the IC to issue civil infringement notices for low-level administrative breaches of the Privacy Act. The Government has agreed or agreed in principle to most of these proposals.

The expansion of CDR to more sectors of the economy will also intensify the OAIC's regulatory role, requiring further resourcing and specific CDR capabilities.

The recently completed FOI Senate Inquiry could see legislative and policy changes in relation to the IC review and complaint processes if some of the Senate committee's recommendations are accepted by Government.

s 47C

⁴⁴ Attorney-General's Statement of Expectations, p 2.

⁴⁵ Attorney-General's Statement of Expectations.

The proposed Privacy Act Review reforms will broaden the OAIC's enforcement powers and require updated regulatory guidance

The Privacy Act Review proposed reforms enhance privacy protections in a range of ways that will increase the effectiveness of the OAIC, which will have strengthened enforcement powers. Key proposals that are likely to materially increase the OAIC's responsibilities are outlined in Figure 22. Many of these proposals are expected to be implemented over the coming years.

Figure 22 | Overview of key Privacy Act proposals agreed by the Government

PROPOSAL	GOAL
Proposal 25.10 The OAIC should conduct a strategic internal organisational review with the objective of ensuring the OAIC is structured to have a greater enforcement focus.	Greater enforcement focus
Proposal 25.9 Amend the annual reporting requirements in AIC Act to increase transparency about the outcome of all complaints lodged including numbers dismissed under each ground of section 41.	Increased transparency
Proposal 28.1 Undertake further work to better facilitate the reporting processes for notifiable data breaches to assist both the OAIC and entities with multiple reporting obligations.	
Proposal 25.1 Create tiers of civil penalty provisions to allow for better targeted regulatory responses.	
Proposal 25.2 Amend section 13G of the Act to remove the word 'repeated' and clarify what a 'serious' interference with privacy may include.	Risk-based enforcement approach
Proposal 25.11 Amend subsection 41(dc) of the Act so the Information Commissioner has the discretion not to investigate complaints where a complaint has already been dealt with by an EDR scheme.	

The proposals outlined in Figure 22 are those that have been agreed by the Government. Those that have been agreed in principle and are likely to have an impact on the OAIC are provided in Figure 23. These proposals are subject to further consideration by the Government, including stakeholder consultation and impact analysis. A detailed analysis outlining the potential changes to the OAIC from the proposed reforms is contained in Appendix D.

Figure 23 | Overview of key Privacy Act proposals agreed in principle by the Government

Change	Reform proposals	s 47C	Type of work	s 47C
Enhanced enforcement powers	Proposals 25.1, 25.2, 25.4, 25.5 and 25.10: Introduction of new civil penalty provisions, public inquiry powers and structure to have a greater enforcement focus		Ongoing	

s 47C

s 47C

Change	Reform proposals	s 47C	Type of work
Data security and privacy guidance enhancement. 47	Proposals 21.3, 21.5, 28.1 and 28.4: Enhanced guidance on data security, breach responses and cross-agency cooperation in enforcement		Ongoing
Organisational and operational reforms	Proposals 25.6, 25.9 and 25.11: Greater cooperation with other bodies and introduction of new reporting requirements		Ongoing
Automated decision-making and emerging technology regulation	Proposals 13.2, 13.3, 19.1 and 19.2: Development of guidance for new technologies, privacy impact assessments, and automated decision-making processes		One-off
Increased transparency in data handling	Proposals 23.1 and 23.5: Enhanced transparency requirements for overseas data flows and entities' data handling practices		One-off
Vulnerability and consent guidance	Proposals 17.1 and 17.2: Development of guidance on handling data of vulnerable individuals and consent processes		One-off

s 47C

s 47C

The key recommendations made by the FOI Senate Inquiry are listed in Figure 24, along with an assessment of their expected impact on the OAIC if they are accepted by the Government.

Figure 24 | Overview of potential reforms from the FOI Senate Inquiry

Area	Suggested reforms	s 47C	s 47C	s 47C
Education, monitoring and guidance	The OAIC prioritises efforts to develop guidance and strengthen pathways for people accessing personal information outside FOI	s 47C		
The OAIC's functions	Move IC review functions and the FOIC to the Commonwealth Ombudsman's Office or remove IC reviews and allow applicants to appeal directly to the Administrative Appeals Tribunal (AAT)			
Culture	An independent external review should be conducted into the OAIC's culture			

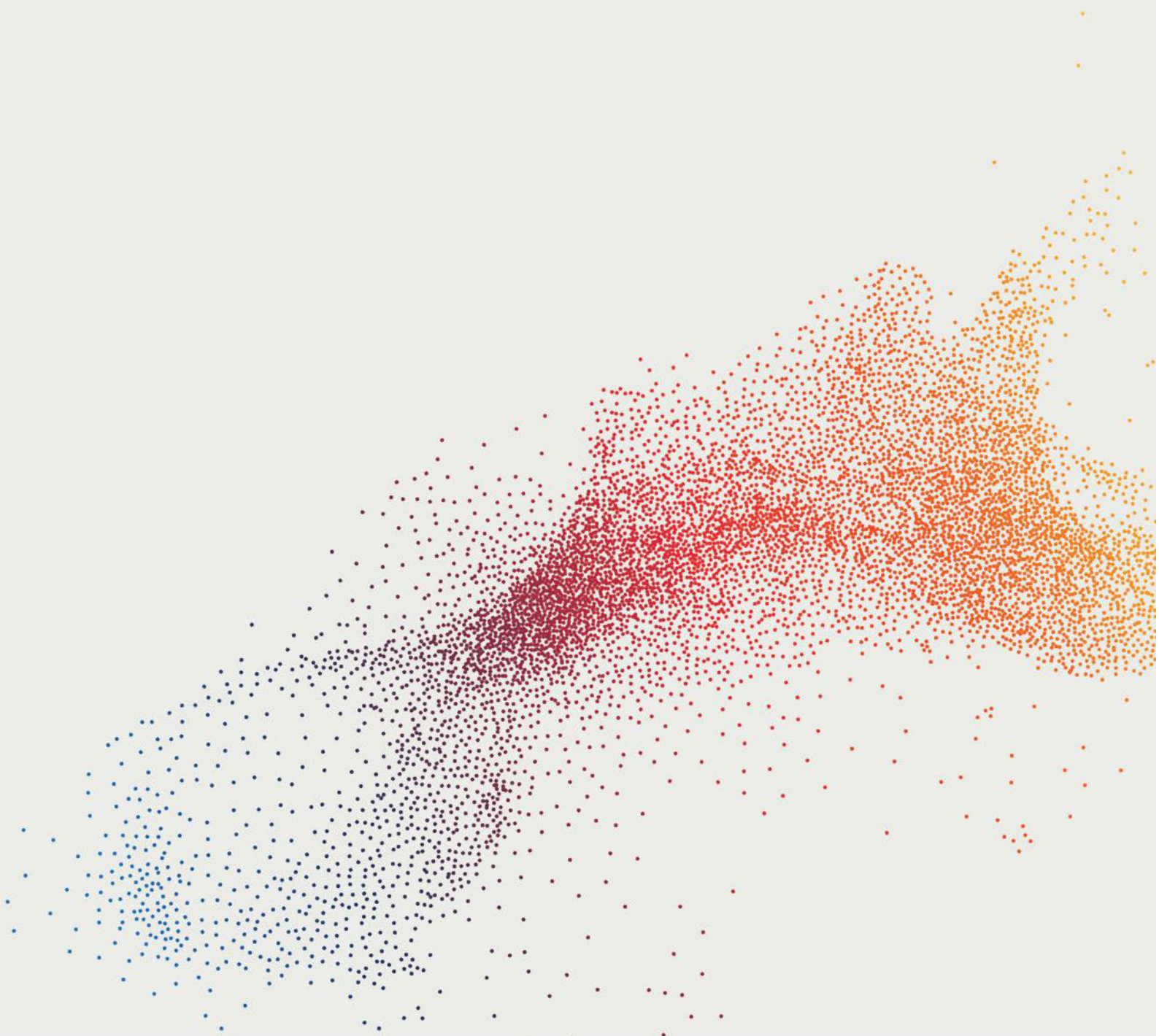
s 47C

Expansions in scope and changes in legislation for CDR and Digital ID will require updated guidance

The OAIC will be impacted by the expected expansions in the scope of CDR and Digital ID. The expected impacts of these future changes on the OAIC are outlined in Figure 25 and Figure 26.

s 47C

Part 2: The OAIIC's operating model



4 Strategy, regulatory posture and approach

Having a clear, modern and risk-based strategy, regulatory approach and posture will be critical to the OAIC's ability to respond to a growing workload and be an effective regulator of information. This chapter outlines the current state and recommendations for improvements that will enable the agency to achieve its purpose, improve its future functionality and best respond to changing demand on its workload as a result of the growing digital economy and increasing cyber crime.

Figure 27 | Relevant questions from the Terms of Reference

- How can the OAIC best respond to the likely continuing growth to the volume and complexity of its core statutory workload?
- How can the OAIC remain effective as a regulator in responding to changing technology, the growth of the digital economy and increasing cyber crime?
- What is the role of the OAIC in providing advice and reports to Government about privacy, information access and information management?

Figure 28 | Summary of key findings

STRATEGIC PLAN

- The OAIC's current strategic plan outlines its purpose and strategy. Parts of the strategic plan reflect an enforcement posture and risk-based approach, but some aspects detract from its clarity and ambition.
- Having a more active and outcomes-focused strategic plan would help to align strategic ambition with increasing government and community expectations and set the foundation for meeting these expectations.

REGULATORY POSTURE

- The OAIC's posture tends to be more reactive than proactive. This has largely been due to the significant volume of matters it is legislatively required to address (for example, IC reviews and FOI complaints) and challenges in changing embedded practices and ways of working. Until recently, the OAIC did not make heavy use of its tools and powers to change regulated entity conduct. It has increased its enforcement activities in recent years but is not perceived as a strong enforcement regulator.
- The agency's current regulatory posture does not set it up to meet the magnified and changing risk of harm to the community. These risks require the OAIC to adopt a greater enforcement and education-focused posture.
- Shifting its regulatory posture to focus more on enforcement and education will set the OAIC up to meet key challenges and ongoing change. By taking a more proactive posture, the OAIC can influence the behaviour of regulated entities before it results in a complaint and deter non-compliance through strong enforcement. This will involve a different emphasis than that for privacy and FOI matters.

REGULATORY APPROACH

- The OAIC published its regulatory priorities for 2023-24, providing guidance on where it will direct resources. It has also provided some clarification on its regulatory priorities and how its approach will work in practice. But the priorities are not sufficiently focused or integrated into

its approach to regulatory action, making it difficult for staff to apply them in their day-to-day work.

- The OAIC’s development of policies for regulatory action demonstrates deep thinking about its areas of expertise and a desire to consider risk when selecting an action.
- Its approach to regulatory action is not sufficiently integrated or linked to its regulatory priorities, strategic plan or regulatory posture. By splitting its regulatory approach into different components, it has missed an opportunity to take an agency-wide, strategic approach.
- The OAIC is moving towards a more risk-based approach in some areas. But to continue its journey to becoming a modern risk-based regulator, it needs an overarching approach that uses the full spectrum of regulatory tools. The effort that is required for different areas of the framework of regulatory powers and tools will reflect the recommended changes to its regulatory posture. The OAIC should increase its use of certain elements of its regulatory approach and be more efficient in its use of others.
 - **It should significantly** increase its engagement with community and industry, to build relationships, gain insights into levels of compliance among regulated entities and understand emerging risks. It should also increase its guidance and education to address non-compliances before they cause harm and encourage a more pro-disclosure FOI culture. Finally, it should significantly increase its use of enforcement to deter non-compliance and address and reduce significant harms.
 - **It should increase** partnership with co-regulators, to build capability, deliver more effective guidance and education, and take joined-up regulatory action. It should also increase monitoring to capture emerging risks and identify non-compliances at an earlier stage to reduce risk of potential harm. Finally, it should increase investigation to identify non-compliance early and remedy this through appropriate regulatory action.
 - **It should be more efficient and discerning** when providing advice and reports to the Government; conciliating low-risk complaints; and assessing and making decisions about routine, low-risk complaints and IC reviews.
- The above means it will be likely to more frequently exercise its discretion not to investigate privacy complaints or undertake IC reviews, and will decide cases quickly if they are not a valid complaint or another body is better placed to respond.

s 47C

Figure 29 | Strategic Review recommendations

1. The OAIC shift its regulatory posture to be more risk-based, with a greater focus on enforcement and education activities, to ensure its effectiveness as a regulator in response to its changing operating environment.
2. The OAIC further consider its role in providing advice to the Government on whole-of-government reforms so that advice and submissions are more consistently informed by the agency’s updated posture and regulatory priorities. This will likely result in the OAIC developing fewer and more targeted submissions to reforms and inquiries.

4.1 Introduction to effective regulatory strategy

The OAIC needs a clear regulatory strategy to be best positioned to respond to changes in technology and demand, and to maximise the potential impact of its regulatory action. Effective regulation is supported by a clear regulatory strategy. A regulatory strategy typically comprises a strategic plan, regulatory posture and approach. Each of these elements is explored in Figure 30.

Figure 30 | Overview of elements of regulatory strategy

ELEMENT	OVERVIEW
Strategic plan	<p>A strategic plan sets out the overarching purpose and vision, and what the regulator seeks to achieve, including:</p> <ul style="list-style-type: none"> regulatory purpose, articulating what it is, what it does and for whom. This should be derived from its legislative mandate and organisational context regulatory vision, identifying its desired future strategic objectives, identifying specific, longer-term goals it seeks to achieve.
Regulatory posture	<p>Regulatory posture describes where it will focus its effort. The regulator needs to decide what proportion of its activities will be about reacting to instances of non-compliance and what proportion will be proactive attempts to promote compliance. Some decisions around where to place regulatory emphasis are enshrined in the legislation administered by the regulator, but many involve considering the external operating environment and organisational priorities.</p>
Regulatory approach	<p>Regulatory approach is how the regulator uses its regulatory tools and powers to achieve its strategic plan and posture. It comprises:</p> <ul style="list-style-type: none"> how the regulator prioritises matters how the regulator exercises its regulatory functions in respect of the matters it prioritises. <p>A risk-based approach focuses resources and effort on the risks associated with non-compliance with rules, rather than the rules themselves. It is based on the notion that it is impossible to avoid all risks and that regulatory tools and powers should be used to effectively manage risks. One of the Regulator Performance Guide principles for best practice regulator performance is being 'risk-based and data-driven'.</p>

The analytical framework for the Strategic Review articulates the criteria we have used to:

- assess the effectiveness and appropriateness of the OAIC's current regulatory strategy
- identify changes that will enable the OAIC to respond to the likely continuing increases in the volume and complexity of its regulatory environment, and play an appropriate role in providing advice and reports to the Government.

These criteria and the associated tests are outlined in detail in Figure 31.

Figure 31 | Tests of effective regulatory strategy

CRITERIA	TEST
STRATEGIC PLAN	
Is clear and concise	Can the community, staff and regulated entities easily understand what the OAIC is seeking to achieve?
Is focused	Does the strategic plan set the OAIC's focus and direction and how it uses its regulatory powers and tools?

CRITERIA	TEST
REGULATORY POSTURE	
Articulates emphasis of effort	Does the regulatory posture describe where effort is focused and where the OAIC sits on the regulatory spectrum?
Reflects demand	Does the regulatory posture reflect current and future demand and expectations of the OAIC?
Aligns with strategic plan	Are regulatory tools and powers being used consistently to further the objectives in the strategic plan?
REGULATORY APPROACH	
Reflects risk of harm	Does the regulatory approach identify the greatest risks the OAIC is seeking to address?
Enables prioritisation	Does the regulatory approach prioritise high-risk matters with the greatest potential for harm?
Focuses powers and tools	Does the regulatory approach outline which powers and tools to apply to address that risk?

4.2 The strategic plan

The strategic plan outlines the agency's purpose and strategy for upholding information rights

The current strategic plan includes the elements expected of a regulator with the OAIC's remit. A high-level snapshot of the plan is shown in Figure 32. The OAIC's purpose, vision and key activities and/or strategic priorities have not changed since 2019.

Figure 32 | Summary overview of the current strategic plan

PURPOSE	Promote and uphold privacy and information access rights.			
VISION	To increase public trust and confidence in the protection of personal information and access to government-held information.			
STRATEGY	Prevent privacy harm and uphold the community's access to information rights in the areas of greatest impact and concern.			
KEY ACTIVITIES	Influence and uphold privacy and information access rights frameworks.	Advance online privacy protection for Australians.	Encourage and support proactive release of government information.	Take a contemporary approach to regulation.
SUCCESS MEASURES	The OAIC's regulatory outputs are timely.	The OAIC's activities support innovation and capacity for Australian businesses to benefit from using data, while minimising privacy risks for the community.	The OAIC's activities support government agencies to provide quick access to information requested and at the lowest reasonable cost, and proactively publish information of interest to the community.	The OAIC's approach to its regulatory role is consistent with better practice principles.
ENABLERS	Continuous improvement and building trust.	Adopting a risk-based and data-driven approach.	Collaboration and engagement.	

Source: OAIC's Corporate Plan 2023-24

Aspects of the plan already reflect an enforcement posture and risk-based approach. The strategy to 'prevent privacy harm and uphold the community's access to information rights in the areas of greatest impact and concern' is strong and reflects an intention to take a risk-based approach. This is bolstered by the OAIC's commitment to adopt a risk-based and data-driven approach to its activities in its key activity of 'taking a contemporary approach to regulation'.

Aspects of the strategic plan detract from its clarity and ambition

The OAIC is regulating in an environment of increased risk that has prompted new and different expectations from the Government and the community, as discussed in chapter 3. These expectations call for an ambitious strategic plan that clearly articulates the OAIC's commitment to protecting the community from harm, and how the agency will deliver on that commitment.

Its vision relates to the public's trust and confidence in the OAIC's core remit of protecting personal information and access to government-held information. Compared to the OAIC's strategy and purpose, which are active and refer to the protection of rights and prevention of harm, the vision is passive and relates to a consequence of effective regulation (public trust and confidence) rather than a more direct measure of effective regulation (actual protection of rights).

One aspect of a typical strategic plan that the OAIC does not clearly articulate is the outcomes or objectives it is seeking to achieve. Regulatory outcomes are important to understand the regulator's intent by identifying outcomes it should seek to achieve. While certain outcomes are referred to in the OAIC's key activities and success measures, they are not standalone, clear or focused. Having specific and clear outcomes would help to focus the agency's activities on addressing the biggest harms.

The strategic plan should be adjusted to be more active and outcomes-focused

Having a more ambitious vision and adding objectives would enhance the strategic plan. This would lay the foundation for the agency to respond to the Government's expectations, external trends and demand. Figure 33 provides examples of updates the OAIC could make to its existing strategic plan. The proposed changes make its vision more active and ambitious, and introduce the strategic outcomes it is seeking to achieve. Changes should be refined and finalised by the new Commissioners. It will be important to generate staff buy-in for the strategic plan to enable them to apply it to their everyday work.

Figure 33 | Indicative updates to the strategic plan



4.3 The OAIC's regulatory posture

The OAIC focuses its efforts on responding to individual cases

The OAIC generally focuses on complaints and individual matters, reacting to matters received. It allocates around 60 per cent of its regulatory effort to responding to individual complaints and IC reviews.⁴⁹ These are critical functions that are legislatively mandated (as described in chapter 2), and by their nature are generally reactive.

The OAIC has discretion over how it exercises its critical functions and how it balances its effort across critical, strategic and supporting functions. As discussed in chapter 2, it has a broad remit that includes critical and strategic functions such as investigations, education and engagement. The agency must respond to complaints but has discretion over how to respond and what proportion of its overall effort it should invest in responding to complaints over other functions.

Despite increased enforcement activity the OAIC is not yet perceived as a strong enforcement regulator

Until recently, the OAIC did not place a strong emphasis on using its tools and powers to deter non-compliance among regulated entities. In recent years, it has been moving towards a more enforcement-focused posture. Key changes include the following:

- A Major Investigations Branch was established in 2022-23. The OAIC has three open investigations – against Optus, Medlab and Medibank – in relation to significant data breaches. It launched its first civil proceedings in 2020 against Facebook and issued further proceedings against Australian Clinical Labs in 2023. Both proceedings are on foot in the Federal Court.
- The OAIC's Regulatory Action Committee (RAC) provides a forum for considering matters for enforcement. In recent years, matters identified through privacy assessment have been referred to the RAC and resulted in CILs.
- The OAIC conducts assessments to monitor regulated entities' compliance with privacy obligations. These assessments enable identification of non-compliances and inform enforcement action.
- The OAIC conducted a CII and follow-up into the Department of Home Affairs' compliance with FOI processing timeframes in 2020. This investigation found shortfalls and made recommendations that have been implemented, significantly improving the department's FOI policy, procedures and outcomes for applicants.

Despite its increased enforcement efforts, the Strategic Review heard from a range of staff and stakeholders that the OAIC is not perceived as a strong enforcement regulator. A staff member who engages with regulated entities expressed the view that the agency needs to “restore confidence that it is a trusted regulator” and that it has “a timid regulatory posture, meaning the community is not getting the protections/rights it expects. Regulated entities are not worried about us.”

Respondents to the OAIC's first stakeholder survey identified that it could improve its use of the full range of its regulatory tools and powers to pursue privacy breaches in the digital environment. One stakeholder engaged for the Strategic Review reported that there is “no sense of fear

“Rather than such significant resourcing spent on one individual complaint, can we put our resources into activities that can assist more people in the community?”

OAIC staff member

⁴⁹ The percentage of FTE involved in regulatory activities was obtained from a staff workshare survey submitted to the Strategic Review team in December 2023.

among regulated entities” that action will be taken following non-compliance.

These perceptions support the need for the OAIC to take, and to be seen to take, stronger regulatory action.

Difficulties changing embedded practices and ways of working, high workloads and the reactive nature of some of the agency’s functions have contributed to the challenges in shifting to a stronger, proactive regulatory posture. One OAIC staff member noted staff “struggle to find time to modernise due to constantly high workloads”. Another said they would like to see the agency develop an “ability to say no to things, not always agreeing that we will get something done and considering workload based on priorities”. The OAIC’s reactive posture is partly due to the inherently reactive nature of certain of its critical functions – particularly privacy complaints and IC reviews.

The current regulatory posture does not set up the agency to meet the magnified and changing risk of harm to the community

The OAIC’s predominantly reactive nature and focus on individual matters is not appropriate for responding to increasing potential harms. If it continues working in this way, it will not shift regulated entity behaviour far enough towards greater compliance, even as it receives ever-increasing and complex individual matters that reflect the greater external risks.

As detailed in chapter 3, the entities the OAIC regulates pose increasing risks to the information rights of individuals and the community. This requires the OAIC to adopt a more enforcement and education-focused posture to effectively respond to and deter non-compliance and shift regulated entity behaviour through education.

Government, stakeholders and the community expect the OAIC to respond to changing risks and demand by focusing on enforcement and education activities

Expectations of the OAIC are expanding in line with changing and increasing risks in its operating environment. The Government and the community expect the agency to be more interventionist and to conduct more education and enforcement activities in the areas of privacy and FOI.

The Government has provided strategic direction on the agency’s changed regulatory posture in the Attorney-General’s Statement of Expectations. It expects the OAIC to focus on addressing privacy harms, promote awareness of privacy risks and provide guidance to regulated entities and individuals.

In addition, the community and stakeholders expect more government intervention for both privacy and FOI (see section 3.2):

- The community would like government agencies to act and do more to protect their personal information (89 per cent of respondents to the Australian Community Attitudes to Privacy Survey 2023).
- Witnesses to the FOI Senate Inquiry called for a more responsive FOI culture, a proactive disclosure culture and stronger pathways for accessing personal information outside the FOI regime.
- Stakeholders who responded to the OAIC’s first stakeholder survey would like to see more timely guidance and advice on the operation of the FOI Act.

Shifting the regulatory posture towards enforcement and education activities will help the agency to meet key challenges in the face of ongoing change

A more proactive posture focused on influencing the behaviour of regulated entities will support the OAIC to effectively respond to increased demand and risk in relation to more sophisticated external threats. It will be better able to influence regulated the behaviour of regulated entities before it results in a complaint (such as by guiding an entity to improve practices following a privacy assessment). The agency can also deter non-compliance through strong enforcement, sending a message to other regulated entities that action will be taken if they do not comply. Education and enforcement are aimed at changing the behaviour of regulated entities and could shift compliance on a larger scale compared to addressing individual matters.

Undertaking more enforcement and education activities will look different for FOI and privacy matters:

- Increasing enforcement of privacy breaches will act as a deterrent and improve compliance. Privacy risks are increasing and strong enforcement will allow the agency to address the most significant harms affecting the community. In turn, this should reduce the number of individual complaints as regulated entity behaviour shifts, although this is not the focus of the regulatory action.
- To complement strong enforcement action against regulated entities for privacy breaches, the OAIC should address community concerns and use education and awareness-raising campaigns to improve understanding of how to protect personal information.
- Many witnesses to the recent FOI Senate Inquiry called for a more responsive FOI culture among agencies and increased OAIC guidance. Supporting compliance and improving practices among regulated entities through education will increase proactive disclosure and improve FOI culture. In time, this should reduce the individual IC reviews received by the OAIC.

RECOMMENDATION 1

1

The OAIC shift its regulatory posture to be more risk-based, with a greater focus on enforcement and education activities, to ensure its effectiveness as a regulator in response to its changing operating environment.

4.4 The OAIC's regulatory approach

Regulatory approach puts regulatory posture into practice, by detailing how a regulator will use its tools and powers to deliver on the activities it decides to focus on under its regulatory posture. The OAIC's current regulatory approach has two key elements – its regulatory priorities and its regulatory action policies. Each element is discussed in this chapter, which also outlines the Strategic Review's recommended future regulatory approach for the agency.

4.4.1 Updating regulatory priorities will enable the OAIC to identify the highest risk matters for regulatory action

The OAIC has released its regulatory priorities

The OAIC published its regulatory priorities in 2023-24 to guide where it would direct resources. These priorities are set out in Figure 34. It uses these regulatory priorities to ensure that the OAIC's resources are focused on the prevention of privacy harm and upholding the community's access to information rights in the areas of greatest impact and concern.

Figure 34 | The OAIC's regulatory priorities

REGULATORY PRIORITIES	
1. Online platforms, social media and high privacy impact technologies	Harms which impact on individuals' choice and control, through opaque information practices or terms and conditions of service. Technologies and business practices that record, monitor, track and enable surveillance, and the use of algorithms to profile individuals in ways they may not understand or expect, with adverse consequences.
2. Security of personal information	Serious failures to take reasonable steps to protect information or report. Risks and mitigations have previously been publicised by the OAIC. Finance and health sectors.
3. Consumer Data Right	Coordinated compliance and enforcement activities by the OAIC and the ACCC. Ensuring that the fundamental privacy safeguards provided by the system are upheld by participants to protect consumers' information.
4. Proactive disclosure of government-held information	The need for agencies to make timely decisions and proactively disclose information to support an efficient access to information regime.

Source: [OAIC's Regulatory Priorities](#)

The OAIC's regulatory priorities are not sufficiently focused or integrated into its approach to regulatory action

The OAIC's existing regulatory priorities are not sufficiently targeted or specific to enable prioritisation between matters in the OAIC's regulated areas. This makes it difficult for staff to practically apply them to their day-to-day work. In particular, priorities 3 (CDR) and 4 (proactive disclosure of government-held information) do not meaningfully narrow down the agency's remit in respect of these regulated areas. One staff member reported that "objectives in corporate documents are so broad that they do not provide a focus" and it was "unclear how these areas should be prioritised in practice".

There is a disconnect between the OAIC's regulatory priorities and its regulatory action documents. The regulatory priorities are set out separately to the regulatory action documents, making it difficult to

understand how they are meant to work together. In particular, it is not clear how the regulatory priorities feed into prioritising matters in each regulated area.

The OAIC has made some progress on clarifying how the regulatory priorities and approach work in practice. The Regulation and Strategy Branch's draft prioritisation framework sets out prioritisation principles to guide decision-making on where the branch should direct its effort, including impact on the community, strategic significance, risk of action or inaction, and resourcing implications. Practical guidance in the draft framework is in line with the modern risk-based approach discussed in section 4.4.

Refining, regular reviewing and implementing regulatory priorities will help to focus efforts where they can have the greatest impact

If the OAIC consistently identifies the highest risk matters, with significant potential for harm, across its whole remit, it will be able to refine its regulatory priorities to make them more targeted and sufficiently clear to identify and address risks through regulatory action.

The highest risks it will need to address are likely to change from year to year. In its decision-making on prioritising its activities to address risks, it will need to consider increased demand for action and the changing expectations of government and the community. There is value in the OAIC reviewing its regulatory priorities on a more regular basis to ensure it focuses on areas where it can have the greatest impact.

It will be important to embed regulatory priorities in day-to-day operations by:

- providing communications from senior leaders and Commissioners around the harms that the regulatory priorities address so that staff understand why certain matters are prioritised
- achieving buy-in from staff so that they consider regulatory priorities as part of regulatory decision-making and deliver work in line with the priorities
- using the regulatory priorities to inform strategic decision-making by the Commissioners.

4.4.2 The current approach to regulatory action is not sufficiently risk-based

The agency has articulated its approach to regulatory action across its remit, and some aspects are risk-based

The agency has released detailed information about its approach to using its regulatory powers. It has published regulatory action policies for privacy, FOI, CDR, digital health and international work, as well as a guide to privacy regulatory action. These policies demonstrate deep thinking about its areas of expertise.

Aspects of the current approach to regulatory action are risk-based. The RAC considers significant privacy regulatory risks and what actions to take in response. It takes a risk-based approach to decision-making by prioritising significant privacy risks, in line with its regulatory priorities. The Regulation and Strategy draft prioritisation framework identifies 'impact upon the community' as a prioritisation principle that should prompt consideration of relevant harms and their impact when making decisions about the branch's work.

The approach to regulatory action is not sufficiently integrated or linked to the OAIC’s strategic plan or regulatory posture

Splitting the OAIC’s regulatory approach into different components is a missed opportunity to articulate an agency-wide, strategic approach to regulation. The breadth of its regulatory functions means that stakeholders and staff do not have a clear sense of its overall approach to regulation. One Executive-level staff member noted that “every branch has a focus, we need an agency focus now”.

The current regulatory approach is largely focused on the process for exercising individual powers. The FOI and privacy documents refer only to regulatory powers rather than the agency’s full range of regulatory tools. The joint Australian Competition and Consumer Commission (ACCC) and OAIC Compliance and Enforcement Policy for CDR goes beyond setting out powers and processes, stating priority conduct for enforcement action. This policy approach could be translated to the FOI and privacy documents.

The regulatory approach documents are not clearly linked to the agency’s strategy or posture, hindering the OAIC from integrating its approach with its strategic outcomes and focus. Its regulatory action policies do not refer to the regulatory priorities or key activities. They do not outline when the agency will take certain actions over others (for example, which matters are appropriate for education versus enforcement).

The culture of technical excellence hinders a risk-based approach

The OAIC’s culture of technical excellence and detail orientation (see section 7.3) limits its ability to be risk-based. The Strategic Review team observed that the agency appears to place a premium on delivery, being technically expert, getting the details right and managing risk to the agency. This means it makes decisions that can withstand external scrutiny but result in less constructive outcomes, where effort invested is disproportionate to the risk, or the focus is on risk to the agency instead of risk of harm to the community.

Changes to the OAIC’s culture will be required to support it to embed a risk-based approach. OAIC staff need support to consistently focus on harm to the community by regulated entities, permission to step up from the detail where appropriate, and an ability to take risks, which is inherent in litigation and required for an enforcement posture.

The Government and stakeholders expect a more risk-based approach

The Government expects the OAIC to prioritise its regulatory functions and take a contemporary and proportionate approach to regulation. The Regulator Performance Guide lists ‘risk-based and data-driven’ as one of three principles of regulator best practice. The Government expects the agency to use resources strategically to provide the greatest benefit for the community and to prioritise regulatory activities in accordance with these principles.

Stakeholders also expect the OAIC to take a more risk-based approach. Stakeholders who responded to the OAIC’s first stakeholder survey gave it the lowest score for the extent to which its activities are risk-based and data-driven. They also identified that the OAIC could improve how it prioritises resources, to focus more on the areas of highest risk or harm.⁵⁰

4.4.3 The future integrated regulatory approach

To continue its journey to becoming a modern risk-based regulator, the OAIC needs an overarching statement of its risk-based approach

Effective, modern regulators prioritise activities in areas they consider high-risk, and other areas of identified strategic importance. A risk-based approach acknowledges the limited resources at a regulator’s

⁵⁰ OAIC stakeholder survey, 2023.

disposal. The advice on best practice, risk-based regulation in this section is based on the Regulator Performance Guide.⁵¹ and Nous' extensive experience working with regulators and designing their regulatory strategies. It is consistent with the best practice criteria for regulatory strategy outlined in section 4.1.

The OAIC can improve how it prioritises matters and uses its regulatory tools and powers across the agency so that it takes a best practice risk-based, harm-focused approach to regulation. It can do this by:

- articulating, in an overarching statement, how it will consistently direct regulatory tools and powers to address the risks to the community and individuals that it is trying to manage
- implementing a framework for making decisions about how and when to apply regulatory tools and powers to address risks of harm.

This section describes what this best practice approach to regulation could look like. It includes the following elements.

Table 3 | Elements of a best practice approach

ELEMENT	REFERENCE
An indicative overarching statement of the OAIC's regulatory approach that sets out example principles by which the agency can direct regulatory tools and powers to address high-risk matters	Figure 35
An indicative integrated, whole-of-agency framework that outlines the regulatory tools and powers available to the OAIC and how it should use them to achieve its updated regulatory posture, as described in section 4.3	Figure 36
Concise statements of how the emphasis in the regulatory approaches to privacy and FOI might vary from the whole-of-agency framework. These statements are intended to support the application of the whole-of-agency framework	Figure 37

The indicative statement and framework are intended to be published, once refined and agreed by the OAIC, to enable transparency and accountability of the use of its regulatory powers expected by Government.⁵²

⁵¹ [Regulator Performance Resource Management Guide](#).

⁵² Attorney-General's Statement of Expectations, p 5.

An overarching statement of a risk-based regulatory approach will support a focus on high-risk matters

It is important that the agency has an overarching statement of its regulatory approach to support its shift to an enforcement- and education-focused regulatory posture. An indicative overarching approach is set out in Figure 35.

This approach will:

- enable greater integration of regulatory action across the OAIC because staff will use the same principles to identify high-risk matters
- support the OAIC to put its updated regulatory priorities into practice and assist in reviewing these priorities annually by consistently identifying the highest-risk matters
- operationalise the changed regulatory posture by identifying how it will consistently direct regulatory tools and powers to address the risks to the community and individuals that it is trying to manage.

Figure 35 | Indicative overarching regulatory approach statement

Our regulatory approach uses both encouragement and deterrence to promote and protect privacy and information access rights. We apply a risk-based approach to prioritise our effort so that we can make the biggest difference.

We direct regulatory tools to address high-risk matters with the greatest potential for harm.

The OAIC will give particular consideration to those matters that also have the following priority factors:

- conduct that is of significant public interest or concern
- conduct that results in substantial harm to individuals and the community
- where our action is likely to have an educative or deterrent effect
- where our action will help to clarify aspects of policy or law, especially newer provisions of the Acts we administer.

We apply our regulatory tools in a consistent, transparent and proportionate manner.

When deciding on which tools to use, and when using them, we:

- identify the risks we need to respond to
- assess the likelihood and possible consequences of the risks
- respond in ways that are proportionate, consistent with the expectations of the community and the Government, and manage risks to adequately protect the public
- take timely and necessary action.

An integrated, whole-of-agency framework articulates how the OAIC will use its tools and powers to take a more risk-based approach, in line with the overarching statement

The OAIC can use a number of tools and powers to achieve its new regulatory approach. These tools range from those that:

- support regulated entities to comply (partner, engage, guide, monitor)
- respond to regulated entity behaviour (assess, decide, conciliate; for example, in relation to privacy complaints and IC reviews)
- change regulated entity behaviour through direction and discipline (enforce, engage, educate).

An indicative framework staff can use to guide their choice of regulatory tools and powers is shown in Figure 36. This framework is intended to guide the application of the OAIC's powers and tools relative to its current use of them and relative to other powers and tools.

Implementing a new regulatory approach will change demand and the mix of regulatory tools and powers. For example, more education should improve compliance, resulting in less conciliation and assessment of complaints. The OAIC's framework will need to be dynamic and informed by monitoring emerging risks, which will feed into changes to the regulatory approach. The emphasis on different regulatory functions will change and should be reviewed annually, together with the regulatory priorities.

Figure 36 | Indicative framework of regulatory powers and tools



Orange = significantly increased use of tool | Yellow = increased use of tool | Blue = more efficient use of tool

The OAIC should do more with some tools and powers, and use others more efficiently

In selecting which regulatory power or tool to use in which circumstance, staff should note:

- The framework in Figure 36 intentionally moves clockwise, starting with softer powers and tools to support regulated entities to comply, through to harder enforcement powers. This does not mean all actions will be required or that actions must be taken in the clockwise order.
- Many matters will require several tools or powers; for example, the OAIC may engage with a non-compliant business and allow time for it to improve its practices. It may then monitor the business for compliance and if there is continued non-compliance, the agency may move to enforcement through harder measures such as applying to the court for a civil penalty order.
- The tool used will depend on the circumstances. For some regulated entities, the OAIC may proceed directly to enforcement following non-compliance where previous education and/or guidance efforts have been unsuccessful or where there has been serious harm. For others, such as a new online platform or a first and minor non-compliance by a regulated entity resulting in little or no harm, education or guidance would be the more effective and appropriate tool from a resourcing and behaviour change perspective.
- The framework indicates which tools and powers the OAIC should use more of and which it should use less of to achieve the updated posture and align with the strategic plan. Which tools and powers are used more or less in practice will depend on where the greatest risks lie and which will be most effective in addressing that risk.

- Not all matters require regulatory action. Under the new regulatory approach, the OAIC will be likely to more frequently exercise its discretion not to investigate privacy complaints or undertake IC reviews and will move to decide cases quickly where they are without merit, are not a valid complaint, or where another body is better placed to respond. In these circumstances, the agency can acknowledge receiving the complaint and provide guidance on how the complainant can protect themselves in future. For IC reviews, the OAIC can advise the applicant that the IC is not undertaking the review or it will be considered by the Tribunal.

Partner | Increase

The OAIC should increase partnership with co-regulators

By partnering more with co-regulators, the OAIC can become more efficient by building its capability, delivering more effective guidance and education, and taking appropriate regulatory action. Best practice regulation involves focusing on the matters a regulator is best placed to address within the broader regulatory environment, and building effective relationships with other regulators in that environment. The Regulator Performance Resource Management Guide recommends that regulators consider opportunities to collaborate with other regulators and across government entities, using existing data and digital solutions to minimise regulator burden and cost.

Regulatory complexity and convergence have prompted greater regulatory cooperation, both domestically and internationally. The OAIC is a member of the Cyber Security Regulators Network and Digital Platform Regulators Network, where regulators collaborate, coordinate and share ideas. The agency is also connected to overseas regulators to exchange best practice and conduct joint investigations (for example, a joint investigation with the New Zealand Office of the Privacy Commissioner into Latitude's personal information handling).

The OAIC's co-regulators want to collaborate more and build stronger relationships. Co-regulator stakeholders interviewed as part of the Strategic Review expressed satisfaction with their engagements with the agency and see benefits in developing deeper connections, particularly in relation to technological developments such as AI.

The agency operates in a crowded regulatory space and can become more efficient by coordinating with other regulators to avoid overlapping action, and partnering with co-regulators where appropriate. Several larger, more established regulators, such as the ACCC and the Australian Communications and Media Authority, are also regulating in the privacy space. While other regulators may not look at relevant misconduct through a privacy lens, they take action in relation to the misconduct; for example, consumer issues that might give rise to a privacy breach. The OAIC could increase its collaboration with these regulators to understand where it should leave relevant matters to be addressed by other regulators, enabling it to focus its effort where it can have the greatest impact. Where feasible and appropriate, the agency should share information during investigations and conduct joint investigations. Joint investigations are resource intensive due to the need to coordinate activities and legal issues that arise. These actions should be reserved for significant issues where it is important to increase the profile of regulatory action or apply the force of multiple regulators.

Increasing the OAIC's focus on partnering with co-regulators will build its capability. As discussed in chapter 3, new technologies pose increasing privacy risks. Building effective partnerships with other regulators with expertise in emerging technologies and cyber security will leverage expertise and better position the agency to understand and anticipate emerging trends and risks. This could include hosting shared education forums and secondments by OAIC staff.

The agency will be able to deliver more effective education and guidance to individuals and regulated entities through greater collaboration with co-regulators. Partnering with co-regulators will ensure it has a broader impact and is providing consistent and comprehensive joined guidance to regulated entities.

The OAIC should further consider its role in providing advice and reports to the Government

The OAIC has legislative advice functions and the Government expects it to provide advice on significant privacy and FOI issues. The IC has monitoring and guidance functions under the Privacy Act, including to advise the Government on the operation of the Privacy Act (s28B) and the impacts of proposed legislation or government programs on the privacy of individuals (s28). The Government expects the agency to work collaboratively with the AGD to provide accurate and timely advice on significant issues relating to strengthening privacy and FOI matters.⁵³ The AGD takes into account the agency's knowledge and expertise when considering changes to policy and legislation in its remit.⁵⁴

The agency expends around 6 per cent of its regulatory effort on advising the Government and comments widely on legislative changes. In 2022-23, the OAIC made 16 submissions to the Government and provided 75 bill scrutiny comments across privacy law and FOI, giving significant consideration to a small number of those comments.

As part of its review of regulatory posture, the agency should further consider the best way to achieve its policy mission. This is a matter for the new Commissioners to consider, and should include where the agency is equipped to provide input to the Government on policy gaps, where legislative change is needed and where it can achieve the most influence.

The OAIC's legislation monitoring and advice functions should be considered alongside its other regulatory tools. The monitoring and advice functions are important and can have broad impact by changing laws and guiding how agencies interpret the Privacy Act. However, as with all OAIC tools, effort should be placed where it can have the greatest impact and functions should be exercised in a coordinated, focused way.

By targeting engagement and advice to matters that directly relate to its regulatory posture and priorities, its advice will have more force and influence on the Government. This would mean declining to comment on legislation that does not relate to its regulatory priorities.

RECOMMENDATION 2

The OAIC further consider its role in providing advice to the Government on whole-of-government reforms so that advice and submissions provided are more consistently informed by the agency's updated posture and regulatory priorities. This will likely result in the OAIC developing fewer and more targeted submissions to reforms and inquiries.

2

⁵³ Attorney-General's Statement of Expectations, pp 5-6.

⁵⁴ Attorney-General's Statement of Expectations, p 6.