information and privacy commission
new south wales

Framework for proactive risk and intelligence-based compliance program

2018 - 2019

Contents

Framework for proactive risk and intelligence-based compliance program

In 2018 – 2019 the Information and Privacy Commission (IPC) will implement a proactive risk and intelligence-based compliance program, in accordance with its commitment to do so in the IPC Business Plan 2017 – 2019.

This framework was developed by the Legal Counsel and Regulatory Advice (LCRA) unit of the IPC in consultation with the Information Commissioner / CEO and the Privacy Commissioner. The IPC has drawn on similar programs in other jurisdictions, including the Office of the Australian Information Commissioner's (OAIC) assessment program, the Office of the Information Commissioner Queensland's audit program, as well as the performance audit program of the Audit Office of NSW. Prior to the drafting of this framework, the IPC had already piloted its self-audit tool with selected agencies and commenced three audits in the 2018 - 19 financial year, of Sydney Water, Sydney Cricket & Sports Ground Trust, and the Office of Sport. These experiences informed the development of this framework.

Under section 21 of the *Government Information (Information Commissioner) Act 2009* (the GIIC Act) the Information Commissioner may investigate and report on the exercise of any functions of one or more agencies under the *Government Information (Public Access) Act 2009* (GIPA Act), including the systems, policies and practices of the agencies. Under section 17(g) of the GIPA Act, one of the Information Commissioner's functions is to monitor, audit and report on agencies' exercise of functions under, and compliance with, the GIPA Act.

Under section 36(2) of the *Privacy and Personal Information Protection Act 1998* (the PPIP Act), the Privacy Commissioner has the following functions:

> (a) 'to promote the adoption of, and monitor compliance with, the information protection principles'
>
> (f) 'to conduct research, and collect and collate information, about any matter relating to the protection of personal information and the privacy of individuals'
>
> (j) 'to prepare and publish reports and recommendations about any matter (including developments in technology) that concerns the need for, or the desirability of, legislative, administrative or other action in the interest of the privacy of individuals',
>
> (l) 'conduct such inquiries, and make such investigations, into privacy related matters as the Privacy Commissioner thinks appropriate'.

The PPIP Act grants the Privacy Commissioner powers to compel agencies to provide information and documents in connection with these functions.

In this framework 'audit' means monitoring, assessment or other regulatory intervention. This is in line with the Commissioners' functions (noted above) and as described in their authorising legislation.

PROGRAM OBJECTIVES				
Identify risk	Treat and mitigate legal risk	Improve agency compliance	Provide sector guidance	Increase community interaction

Key Performance Indicators	
Performance indicator	**Target**
Percentage of audits informed by evidence	100% of all audits reflect a sound evidentiary basis
Guidance produced for remediation and compliance	Where issues are identified for remediation, guidance is issued to promote sector compliance
Audits result in improved agency compliance	Follow-up audits demonstrate improved compliance
Percentage of auditees responding positively to certain questions on a post-audit survey	80% of auditees respond positively to a post-audit survey regarding their experience of the audit
IPC self-assessment scores regarding utility of audit	Self-assessment scores regarding the utility of each audit average over 80% for the year
A reduction in the number of complaints received by the IPC about agency handling of information access requests	A reduction in the number of complaints in the 12 months following the timeframe for the audit recommendations compared to the 12 months prior to the audit

The objectives and key performance indicators (KPIs) of the risk and intelligence-based compliance program ('the program') are tailored towards achieving measurable impact, through:

- a focus on agency outcomes and improvement verified through follow up audits and metrics
- a focus on locating risks and issues for remediation and guidance
- continuous improvement of the program through self-assessment and agency assessment.

Process for identifying audit targets

The IPC will, every 6-12 months, follow a four step process for identifying audit targets (every 6-12 months)	
Step 1.	**The IPC will identify a pool of potential audit targets, predominantly with reference to key metrics collected by the Compliance Committee**
Step 2.	**The IPC will assess and compare the risks and impact associated with a selection of potential audit targets**
Step 3.	**The IPC will weigh additional factors such as recent trends and developments likely to affect the compliance or risk profile of particular agencies, and self-assessment tool responses**
Step 4.	**The IPC will exercise discretion in weighing the results of the first three steps and will prioritise audit targets for the upcoming 6-12 month cycle**
This process will take place at the same time the IPC decides which follow up audits to undertake (see below)	

This process is intended to maximise the effectiveness of the proactive compliance program in achieving its objectives, by ensuring that the selection of audit targets is rigorous, targeted, and based on risk/impact and intelligence assessments. The process uses a mix of quantitative and qualitative data metrics, risk/impact assessments, and consideration of environmental/contextual factors.

The Audit Program Determination spread sheet **[template at D18/278529/DJ]** will be used by the IPC to follow this process and determine audit targets on a periodic (6-12 monthly) basis.

The Agenda at the 6 monthly Compliance Committee meetings is to include a review of data and identification of prospective audits for the forward 6 months, based on the data.

Step 1. Identify the pool of potential audit targets

1.1 Open the Target Pool tab of the Audit Program Determination spread sheet [template at D18/278529/DJ]

1.2 Complete the following tables in the spread sheet using Compliance Committee data

Privacy: Agencies with highest proportion of complaints as a %age of applications		
#	Agency	Complaints/applications
1		
2		
3		
4		

Privacy: agencies with highest %age of internal reviews resulting in a finding of breach		
#	Agency	% reviews = breach
1		
2		
3		
4		

Information access: Agencies with highest proportion of complaints as a %age of applications		
#	Agency	Complaints/applications
1		
2		
3		
4		

Information access: agencies with highest %age of internal reviews resulting in a s 93 notice		
#	Agency	% reviews = s 93 notice
1		
2		
3		
4		

Agencies that have been the subject of particularly significant, or high numbers of, complaints		
#	Agency	Complaints
1		
2		

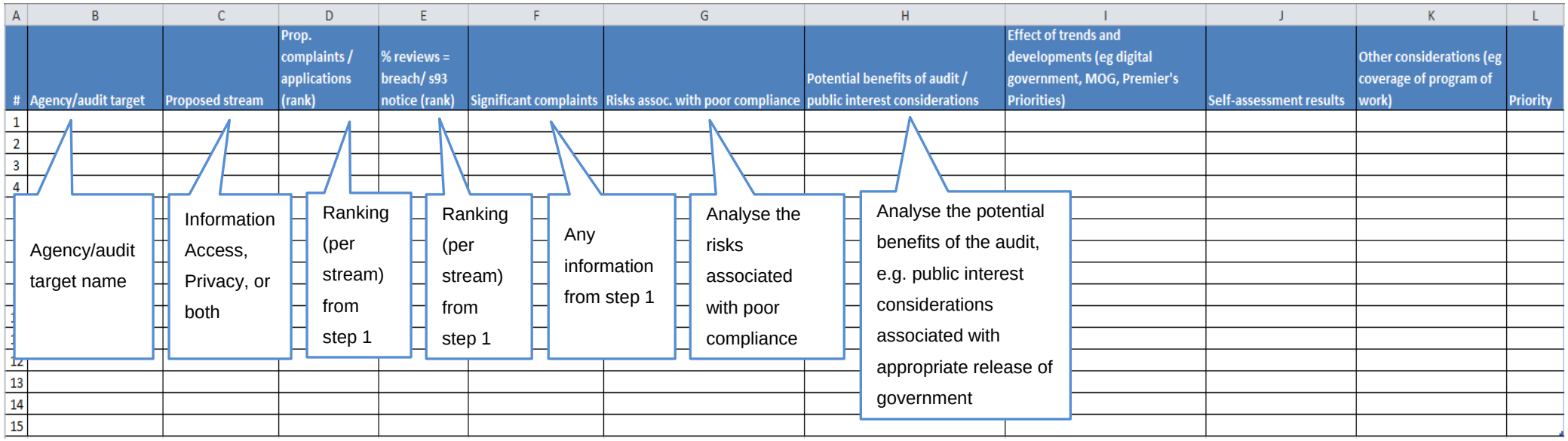
Agencies with particular privacy risks (e.g. recent data breaches) or strong public interest considerations and associated risks in relation to information access that do not appear above		
#	Agency	Risks / Public interest considerations
1		
2		
3		
4		
5		

Step 2. Assess risks and impact associated with selected audit targets

2.1 Open the Audit Program Pool tab of the Audit Program Determination Excel spread sheet

2.2 Select 5-15 audit targets from Step 1, and enter them into the spread sheet, along with relevant rankings and information from Step 1 into the first five columns (B – F)

2.3 For each potential audit target, analyse the risks associated with poor compliance and the potential benefits of the audit and complete columns G and H.



Step 3. Weigh additional factors such as links to recent trends and developments, self-assessment tool responses, and any other relevant considerations

3.1 For each potential audit target, complete columns I, J and K by assessing links to recent trends and developments likely to affect the compliance or risk profile of particular agencies, self-assessment tool responses, and any other relevant considerations

A	B	C	D	E	F	G	H	I	J	K	L
#	Agency/audit target	Proposed stream	Prop. complaints / applications (rank)	% reviews = breach/ s93 notice (rank)	Significant complaints	Risks assoc. with poor compliance	Potential benefits of audit / public interest considerations	Effect of trends and developments (eg digital government, MOG, Premier's Priorities)	Self-assessment results	Other considerations (eg coverage of program of work)	Priority
1											
2											
3											
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											

Assess links with recent trends and developments likely to affect the compliance or risk profile of particular agencies, for example digital government, MOG, and Premier's priorities

Insert any relevant information from self-assessments or IPC reports

Insert any other information deemed to be relevant, including the coverage of the audit target's program of work

Step 4. Exercise discretion in weighing the results of the first three steps, and prioritise audit targets for the upcoming 6-12 month cycle

4.1 Consider the information in columns B – K and select a priority rating for each potential audit target from the drop down menu in column L.

4.2 Select the highest priority agencies/audit targets as part of the audit program for the upcoming 6-12 months.

A	B	C	D	E	F	G	H	I	J	K	L
#	Agency/audit target	Proposed stream	Prop. complaints / applications (rank)	% reviews = breach/ s93 notice (rank)	Significant complaints	Risks assoc. with poor compliance	Potential benefits of audit / public interest considerations	Effect of trends and developments (eg digital government, MOG, Premier's Priorities)	Self-assessment results	Other considerations (eg coverage of program of work)	Priority
1											Urgent
2											High
3											Medium
4											
5											
6											
7											
8											
9											
10											
11											
12											
13											
14											
15											

Select a rating from the drop down menu for each agency/audit target listed.

Audit follow-ups

The IPC will conduct follow-ups regarding audits identifying serious issues requiring remediation

The form of these follow-ups will vary, depending on the issues involved and resources available

The IPC will decide on the follow up audits it will undertake at the same time it determines its audit targets for the upcoming 6-12 months or as recommended by the Compliance Committee

Where an IPC compliance audit identifies serious issues requiring remediation, the IPC will 'follow up' with the agencies involved after a period of time to assess whether remediation has successfully been undertaken. A follow up may consist of:

- requests for information or responses to questions regarding issues raised in the original audit
- a full audit of the same or similar scope as the original audit
- a smaller targeted audit selecting a sample of the issues raised in the original audit for review
- an audit of a similar subject matter / area to that covered by the original audit, which was not within the scope of the original audit, to test whether the original audit's recommendations have been implemented fully within the agency.

The form of follow ups will vary depending on the seriousness of the issues raised in the original audit and availability of IPC resources.

Audit scoping and conduct principles

The IPC will develop its approach to audit scope definition and conduct on an iterative basis

The IPC will notify the target agency or agencies of the scope of the audit prior to commencement of the audit

For the first six months of the program, the IPC will tailor the scope of each audit to the particular audit target. At the six month mark, the IPC will consider whether it should develop and adhere to certain principles regarding the scope of the audits it is conducting.

For example, the IPC may want to:

- establish a rule or target regarding the number of audits separately focussed on privacy or information access, or covering both privacy and information access
- decide whether there will be a target number of 'risk based' audits versus 'compliance based' audits (the OAIC defines risk based audits as focussed on identifying privacy risks that directly relate to the entity's general compliance obligations, while compliance based audits more specifically focus on whether an entity has complied with an identified legislative obligation or explicit direction).
- standardise the scope of audits depending on whether they are focussed on privacy or information access, and/or whether they are risk based or compliance based.

Prior to the commencement of an audit, the IPC will notify the agency or agencies being audited of scope through a brief draft scoping paper or communication advising in general terms by for example, compliance with requirements for managing mandatory proactive release of information.

Audit methodologies and timeframes will also be developed iteratively, initially on a case by case basis and then potentially standardised as the IPC obtains more information and experience.

Findings and recommendations

Audited agencies will receive a draft report and will be given two weeks to provide a response for inclusion in the final report

The IPC will report on audits in accordance with its legislative obligations

Audit reports will be published on the IPC's website

The IPC will provide audited agencies with a draft report containing key findings and recommendations. Audited agencies will be:

- given 2 weeks to provide a response regarding each of the recommendations in the draft report and any perceived inaccuracies
- encouraged to commit to taking action to comply with each recommendations in their response.

The IPC will deliver final reports in accordance with its legislative obligations. Under section 21 of the *Government Information (Information Commissioner) Act 2009*, the Information Commissioner is to give an information access investigation report to the Minister responsible for any agency to which the report relates, and to the principal officer of an agency that is the subject of the report. Where the report is in response to a monitoring and auditing of systems, policies and practices under section 17(g) of the GIPA Act, it will be provided to the agency and will be published for education and compliance purposes. Under section 61C of the PPIP Act, the Privacy Commissioner may at any time make a special report on any matter relating to the Privacy Commissioner's functions to each House of Parliament and the Minister.

The IPC will publish audit reports on the IPC website, as soon as practicable after the IPC has discharged its legislative reporting obligations.

Program and project evaluation

IPC staff conducting audits will, at the conclusion of each audit, complete a survey assessing the utility of the audit

Each year, the Compliance Committee will consider the survey responses, and the performance of the program against the KPIs, and decide whether any program changes are necessary

The self-assessment survey will ask staff the following questions:

- The IPC officers were responsive and accessible during the audit process?
  (agree or disagree, scale of 1 – 5)
- The information my agency provided was considered in the audit report?
  (agree or disagree, scale of 1 – 5)
- My agency had a reasonable opportunity to comment on the draft audit report?
  (agree or disagree, scale of 1 – 5)
- The audit recommendations were implementable by my agency?
  (agree or disagree, scale of 1 – 5)
- The recommendations were helpful in assisting you/ your agency/s understanding of GIPA Act requirements?
  (agree or disagree, scale of 1 – 5)
- The recommendations were helpful in assisting my agency's compliance with GIPA Act requirements?
  (agree or disagree, scale of 1 – 5)
- How satisfied were you with the overall process including timeliness and provision of a draft report for your consideration?
  (scale of 1 – 5)
- Do you have any other feedback regarding the process for the audit of your organisation's GIPA Act compliance? In particular, if you disagreed with any of Questions 1-6 or were dissatisfied with the audit process, please explain why.

Annually, a paper will be prepared for the Compliance Committee assessing the program's performance against the KPIs. The Compliance Committee will review the paper and assess whether any changes should be made or trialled for the upcoming period.

Document information

Identifier/Title:	Framework for proactive risk and intelligence-based compliance program
Business Unit:	IPC
Author:	LCRA
Approver:	CEO/Information Commissioner
Date of Effect:	December 2018
Next Review Date:	December 2019
EDRM File Reference:	D18/278530/DJ
Key Words:	audit, compliance, proactive, risk, information access, privacy, Information Commissioner, Privacy Commissioner, IPC

Document history

Version	Date	Reason for Amendment
1.0	October 2018	Initial Draft
1.1	November 2018	Second Draft
1.2	December 2018	Third Draft
1.3	April 2019	Final