information and privacy commission
new south wales

IPC Compliance Audit Manual

Janaury 2023

Contents

Purpose

This manual was prepared by the Information and Privacy Commission, NSW (IPC) as a guide for IPC officers undertaking regulatory compliance audits. Regulatory assistance is distinguished from a compliance audit. Regulatory assistance involves a lengthier engagement with the subject agency and over a period of time. Over this period regulatory assistance guidance and education may also be provided by the IPC to the agency. However the IPC will apply the audit framework to instances of Regulatory Assistance to ensure that procedures are transparent, proportionate and fair.

A compliance audit is an assessment of a regulated agencies's activities, systems, policies and practices to assess the level of compliance with the relevant regulatory requirements.

This manual provides general procedures and protocols for conducting compliance audits. It has been prepared for the primary purpose to provide guidance to IPC officers in the Investigation and Review Team when undertaking regulatory compliance audits. The manual is intended to ensure a consistent approach to audits, helping to ensure all IPC audits are adequate, reliable and comparable.

This manual has been prepared for the purpose described and for the particular operating context for the IPC, and no responsibility is accepted for its use in any other context or for any other purpose.

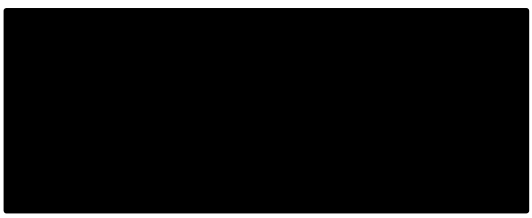
Elizabeth Tydd

Information Commissioner

NSW Open Data Advocate

CEO, Information and Privacy Commission NSW

and



Samantha Gavel

Privacy Commissioner

Information and Privacy Commission NSW

Janaury 2023

1. Introduction

1.1 What is a compliance audit?

For the purposes of this manual an audit is:

> 'a systematic, independent and documented process of obtaining objective evidence and evaluating audit evidence to determine the extent to which the audit criteria are met'.

AS/NZS ISO 19011:2018

Guidelines for auditing management systems (see References).

The specified criteria in compliance audits conducted by the Information and Privacy Commission (IPC) are generally about the legal and regulatory requirements that the IPC administers. Audits are a useful tool for monitoring and verifying the effective implementation by regulated entities of IPC legislation. At the IPC an audit may be agency specific or may be issue driven and in which case may invovle multiple agencies within a specific sector.

1.2 What is an auditee?

An auditee is an agency being audited. IPC audits agenies whose activities are regulated by legislation that the IPC administers.

1.3 IPC Legislation

The IPC administers the following legislation in NSW:

- *Government Information (Public Access) Act 2009* (GIPA Act)
- *Government Information (Information Commissioner) Act 2009 (GIIC Act)*
- *Privacy and Personal Information Protection Act 1998 (PPIP Act)*
- *Health Records and Information Privacy Act 2002 (HRIP Act)*

1.4 IPC Regulated entities

For the purposes of this manual the agencies that are subject to the legislative remit of the IPC are within the following sectors:

- State Government
- Public Universities
- Local Government
- State Owned Corporations
- Ministerial offices
- Private Health Service Providers (as defined)

1.5 Compliance audit as a regulatory tool in IPC

The IPC has responsibilities, functions and powers as prescribed by the legislation it administers.

Relevant to the IPC's compliance activity these include but are not limited under the GIPA Act [1] to:

- Assisting agencies in connection with the exercise of functions under the legislation;

[1] Section 17, GIPA Act

- Monitor, audit and report on the exercise by agencies of their functions under, and compliance with the GIPA Act;
- Make reports and provide recomendations to the Minister about proposal for legislative and administrative changes to further the object of the GIPA Act; and
- To receive and investigate complaints [2]about action or inaction under the GIPA Act.

Under the PPIP Act[3] they include to:

- Promote the adoption of, and monitoring compliance with the information protection principles;
- provide assistance to public sector agencies in adopting and complying with the informaiton protection principles and codes of practice;
- Prepare and publish reports and recommendations about any matter that concerns the need for, or the desirability of, legislative, administrative or other action in the interest of the privacy of individuals;
- Receive, investigate and conciliate complaints about privacy related matters; and
- conduct such inquiries, and make such investigations, into privacy related matters as the Privacy Commissioner thinks appropriate.

The IPC uses compliance audits as one of its regulatory tools, to assess the extent to which a regulated entity is complying with its legislative responsibilities and as an opportunity to educate and elevate compliance by regulated entities. Through improved compliance, citizens will benefit from better application of the information access and privacy legislation regimes and the objects and intent of IPC legislation will be realised.

1.6 Objectives of the compliance audit

Compliance audits undertaken by the IPC are used to achieve the following objectives including but not limited to:

- advancing the objectives of the legislation IPC administers to promote the rights of citizens to access government information and preserve privacy rights
- improving compliance with legislative requirements
- through public audit reporting, ensuring IPC's regulatory activity is open and transparent
- educating its regulated entities about the application and operation of IPC legislation
- promoting credible and robust legislative practices
- elevating agencies' understanding and performance to achieve compliance
- addressing identified compliance vunlerabilities and/or non-compliance
- ensuring that regulation across regulated entities is proportionate to the identified risk, consistent and transparent.

[2] Sections 17 & 21 of the GIIC Act

[3] Section 36 PPIP Act

In a compliance audit the IPC will:

- **assess compliance with IPC legislation.** The IPC may assess compliance with legislation administered by IPC. This may include assessing compliance with the practical application of legislative requirements.
- **review application of systems, policies and practices implemented by the auditee**. The IPC will review the existence and quality of the systems, policies and practices adopted to enable an agency to achieve legislative compliance.
- **report findings and follow-up action**. The IPC will will report on the scope of the audit and document the assessment of compliance. A follow-up action program may be scheduled to address reccomendations materialising from a compliance audit.

Awareness of and confidence in IPC's regulatory role increases through IPC communicating and promoting audit findings. Stakeholders who are likely to have an interest include the regulated entities, citizens, ministers and parliament.

1.7 Knowledge and skills of IPC

IPC officers have the necessary knowledge and skills to apply the audit principles, procedures and techniques when undertaking compliance audits. The IPC develops its staff through internal and external training as appropriate to enable its officers to have the knowledge and ability to conduct compliance audits in accordance with this manual, relevant IPC legislation and any other internal work procedures.

At all times IPC officers conducting compliance audits will act ethically, be objective and without bias, and be versatile, open-minded and decisive. They will act to promote the ethical values as established by the *Government Sector Employment Act 2013* and the values espoused by the IPC.

1.8 Audit program

The IPC has a strong desire to engage effectively with all our external stakeholders to ensure we deliver audits that are of a high quality and lead to improved performance.

Our Annual Work Program, provides a summary of all audits to be conducted within the proposed time period and detailed information on the areas of focus. From time to time the IPC may add, remove or change the completion date of planned audits. This can be in response to changes to scope or other circumstances impacting on the work program.

Our Annual Audit Work Program is available on our website at www.ipc.nsw.gov.au.

2. IPC audit procedures

2.1 The audit process

The audit process applied by the IPC may involve a desktop audit, on-site audit or a combination of both a desktop and onsite audit. Regardless of the type of compliance audit, there are common audit components which occur and detailed further below.

The activies that are required across the compliance audit process regardless of the type of audit includes:

- Authorisation to undertake an audit
- Intelligence gathering

- Notification of compliance audit
- Collecting audit evidence through gathering information, observations and interviews, and sampling
- Evaluating audit evidence
- Compiling of audit report
- Provision of draft report to audited agency for comment
- Finalisation of draft report
- Provision of report to head of agency and/or responsible Minister if required (section 24 of GIIC Act)
- Publication of Report
- Monitoring of follow up action program.

2.2 Authorisation of a compliance audit

Any decision to undertake a compliance audit by the IPC requires the approval of the Information Commissioner or Privacy Commissioner as may be appropriate. The IPC has developed a proactive regulatory risk based approach to compliance. This approach is outlined in the IPC Framework for proactive risk and intelligence-based compliance program 2020- 2021 which recognises the role of the IPC Compliance Committee to advise on proactive compliance activies that pose the greatest risk to achieving the IPC's regulatory objectives. In addition the IPC Regulatory Framework sets out the IPC's regulatory approach to promoting compliance and protecting information access and privacy rights in NSW. Together they inform the risk based approach applied by the IPC to its compliance audit activity.

The terms of reference of the Complicane Committee provide that it has a role to:

- review intelligence and post-case analysis to advise on emerging risks that require the development of proactive compliance responses, which may include compliance audit or other activity such as regulatory assistance
- review proposals for proactive compliance activities
- advise the Commissioners on proposed proactive compliance activities.

The Compliance Committee meets on a quarterly basis or if required out of session upon request.

The decision to undertake a compliance audit by the IPC may arise through a number of channels which can include:

- referral from another regulatory entity such as ICAC, or NSW Ombudsman
- referral from the NSW Civil and Administrative Decisions Tribunal (NCAT) in accordance with section 111 of the GIPA Act
- internal IPC intelligence and assessment of reviews and complaints which may identify systemic trends or compliance issues

- a complaint, including a complaint that may be brought as a public interest disclosure to the Information Commissioner or the Privacy Commissioner[4]
- in response to a significant privacy breach such as a data breach or serious disclosure of personal/sensitive information
- any other circumstances that fall within the jurisdictional remit of the IPC and as approved by the relevant Commissioner or the IPC Compliance Committee.

2.3 Intelligence gathering

The purpose of intelligence gathering in a compliance audit is to collect and gather relevant information that can be used to meet the objectives of the compliance audit. Often the intelligence gathered will be presented to the Compliance Committee and will inform the consideration of any proposed proactive regulatory activity.

Further, the collection and review of intelligence will enable familiarity with the specific statutory requirements and other regulations or guidelines that may apply to the scope of the compliance audit.

The types of relevant information that may be reviewed include:

- technical information about the processes and operations in place to give effect to the IPC's legislation
- operating manuals, plans and procedures
- systems design to preserve and promote information access and privacy
- agency policies and guidelines
- statutory and other requirements
- previous audits and compliance history
- evidence of past performance, such as reviews and complaints
- agency performance as comparable to other agencies as reported in its annual report or identified through the preparation and publication of any report by an IPC Commissioner
- agency publicly available information as provided on its website.

This information may be found by the IPC in its own files, in public reports, decisions of the NCAT, GIPA agency dashboard and agency websites. The IPC may also require specific information which requires technical expertise, in which case the IPC may refer to external specialists to seek such information to inform its understanding and intelligence gathering. A decision to seek external expertise is always approved by the relevant Commissioner.

The audit plan outlines the audit's objectives, scope and timetable, and the products that the audit will generate. See Appendix 3 for an example of an audit plan.

An audit plan should include the following key elements:

- the audit **objectives**

[4]The Privacy Commissioner is recognised under the *Public Interest Disclosure Act 2022* as an integrity agency which commences 18 months after the legislation was given assent on 13 April 2022.

- the audit **criteria** and any reference documents
- the audit **scope**
- a **quality plan** identifying reviews to be undertaken
- an **assessment of logistics and methodology**.

The purpose of the audit plan is to assist in the audit process and to provide a broad framework to support and guide IPC officers in the audit process.

2.4 Notification of compliance audit

Following a decision to authorise the conduct of an agency compliance audit, the IPC will notifiy the relevant auditee and advise of the intention to undertake a compliance audit. That notice will include:

- Sufficient explanation to describe the circusmtances which have given rise to the audit
- Any background intelligence that informed the decision
- The general scope of the audit
- The relevant contact officer for the purposes of conducting the audit
- An indicative timeframe for the audit
- Methodology of the audit – whether the audit is to be completed onsite, as a desktop or as a combination of both
- Any information that is requested to be provided
- The legislative basis which authorises the audit.

The IPC recognises that the circumstances of each audit are unique and specific to the particular auditee and variable depending on the legislative basis which underpins the compliance audit. In this regard, attached as Appendix 1 is a template notice of audit which can be modified to the particular circumstances required. The template at Appendix 1 is specific to an audit that is proposed under the GIPA Act. At the time of preparing this audit manual, the PPIP Act did not have an explicit audit provision and accordingly, no specifc template has been prepared. However, an examination is available to the Privacy Commissioner by virtue of section 36 of the PPIP Act. Appendix 2 includes a template that can be modified for such examination under the PPIP Act.

Not every audit by the IPC will require notification as outlined above. Where an audit is issue driven it may or may not necessitate the need for notification to an agency. Whether notification is required will be determined in the audit planning and scoping stage of the audit.

It is noted that the Mandatory Notifiable Data Breach Scheme (MNDB) will commence in November 2023. Under that scheme the Privacy Commissioner has particular audit functions limited to the MNDB. The requirements of this manual will guide the audits arising from the operation of the MNDB to provide consistency across the IPC.

2.5 Audit planning and preparation

For some compliance audits, an audit plan will assist the progress of the compliance audit. The audit plan outlines the audit's objectives, scope and timetable, and the products that the audit will generate. See Appendix 3 for an example of an audit plan.

An audit plan should include the following key elements:

- the audit **objectives**
- the audit **methodology**
- the audit **criteria** and any reference documents
- the audit **scope**
- an assessment of **logistics** an **audit timetable**
- **roles and responsibilities** of audit team members
- the **allocation of appropriate resources** to critical areas of the audit.

Audit objectives

The objectives of each compliance audit or audit program must be established at the outset to direct planning and establish the method for each compliance audit. The objectives define what the audit will achieve. Audit objectives can be based on various considerations such as management priorities, or statutory and regulatory requirements or identification of systemic issues.

Audit Methodology

The methodology details the manner in which the audit is to be conducted, for example an on site or insitu audit where the agency provides information in response to IPC officers questions – this is generally a more inquisitorial audit. It may also involve some degree of insitu testing, for example awareness of, or access to delegatiions or authorisations that operate to enable officers of the agency to exercise statutory functions. A desk top audit may be preferred in instances of stated non-compliance by the agency or where the risks posed by non or sub-optimal compliance is discrete. A desktop audit involves IPC officers examining publicly available information relevant to the agency and its compliance. This process is undertaken remotely. A desktop audit may also involve requests for further information or responses to questions by way of a statement. The methodology will be determined having regard to the scope of the audit and issues to be considered and may reflect a combination of manners for example on site and insitu.

Audit criteria

The audit criteria are defined requirements against which the audit will compare collected audit information. The criteria may include regulatory requirements, policies, processes and procedures, standards, guidelines or any other specified requirements.

Scope of the audit

The scope defines the extent and boundaries of the compliance audit activity. It identifies those aspects that will be in scope and out of scope of the audit such as the particular issue/s or timeframes that the audit may be concerned with.

Logistics of conducting the audit

Each audit must be assessed to determine whether there are any potential barriers to it being successfully carried out at the identified date. For an onsite audit, the Director, Invesigation and Reporting (DIR) should be aware of any occupational health and safety requirements for entry to the site and whether appropriate staff will be available.

Audit timetable

The audit timetable should include the date and places where on-site activities will be conducted, and the expected time and duration of the audit.

Selecting the audit team and roles of team members

The Director, Investigation and Reporting (DIR) should determine whether other personnel, other than the complaints and proactive initatives team, should be involved in the audit process. Other IPC staff may be involved in the process from the outset to help with audit planning, provide background information and, if necessary, participate in undertaking the compliance audit itself. Team members may assist with audit assessment and evaluations, prepare and draft correspondence and draft reports and provide input to the follow- up action required.

Technical experts may be called in to provide specialist knowledge. They may accompany the team on the audit inspection if required or be referred to when necessary.

The audit team, which shall generally mean the complaints and proactive initaitives team, should be fully knowledgeable of the audit scope and criteria, lead any onsite inspection, be the main point of contact between the auditee and IPC, and ensure the overall competence of the audit process.

Allocating appropriate resources

The DIR needs to ensure IPC officers required for the audit are available on the day, and ensure that sufficient resources are made available for the audit to be undertaken, including making decisions on the reprioritisation of work to enable the audits to be completed as scheduled.

2.6 Collecting background information

The purpose of collecting and reviewing background information is to assemble relevant material that can be used to meet the objectives of the compliance audit. The collection and review will enable the IPC to become familiar with the auditee's operations, the statutory requirements and other regulations or guidelines that may apply or are relevant to the particular audit.

The types of information that may be reviewed include:

- GIPA Agency Dashboard
- Agency Annual Reports
- Agency Website
- Self Assessment Checklist – if completed
- Responses to targeted audit surveys from the IPC
- technical information about the processes and operations
- policies, procedures and guidelines
- statutory and other requirements
- previous audits and compliance history
- evidence of past performance, such as reviews and complaints.

This information may be found in IPC files, reports such as the IPC reviews and complaints records, online in the GIPA Agency Dashboard, websites or annual reports.

2.7 Types of audits

In general the IPC adopts an escalation model to its compliance activity. There are three types of audit approaches that the IPC uses:

- Agency Self Assessment
- Desktop Assessment
- Onsite Audit.

Agency Self Assessment

The first step in the audit model is an agency self assessment. This involves the Agency that has been identified as subject of complaince activity being request to complete the IPC's self assessment tool for either Information Access or Privacy, as the case may be.

In this way, the Agency is asked to review their complaince and identify how the agency compares to the required compliance measure. In some instances the auditee may be compared to similar organisations' performance in specific areas. This assessment is conducted using publicly available information generally via the GIPA Dashboard, agency websites or annual reports for example.

Where the IPC requires the Agency to complete the self assessment tool, and requests that it provides a copy of the completed assessment to the IPC, the IPC will then review and assess the Agency's complaince levels.

The IPC may require the Agency to prepare and provide a remediation plan against any or all identified areas of non compliance. Such a request will be accompanied by a timeframe for implementation and a request to report back to the relevant Commissioner (section 24(3) of the GIIC Act).

Desktop Assessment

A desktop assessment will be undertaken remotely and by utilising information that is publicly available to the IPC generally by assessing the Agency's information on its website for evidence of compliance with legislative requirements. For example, this may involve an assessment of an agency's compliance with the mandatory proactive release requirements of the GIPA Act or the existence of the Agency Disclosure Log.

Onsite Assessment

The IPC will undertake on site assessments where it seeks to review and evaluate the agency's systems, policies and practices, for compliance with the IPC legislation. For example the IPC may assess how an agency receives and processes a GIPA access application, the timeframes for processing, and application of statutory requirements to determine the agency's level of compliance and whether opportunities for improvement are required or necessary.

The IPC may use a combination of the audit approaches depending on the individual circumstances of the audit. An onsite assessment is generally a more intensive audit approach and includes a review of systems, policies and practices.

Both the desktop and onsite assessment will result in an audit report being prepared by the IPC.

2.8 On-site activities

Collecting audit evidence

During the on-site audit, the IPC will collect and record audit information on the audit tool.

The following tasks should be completed during the onsite audit:

- gather information—take notes, ask open questions
- complete audit assessment tool
- document any observed issues which were not anticipated during the preparation of the audit
- examine relevant documents, notices of decision, template letters, search notices
- obtain copies of any documents which may be relevant to the scope of the audit.

Sampling

Generally, the IPC will undertake a random sample of the Agency's legislative compliance in relation to the processing of access applications or privacy reviews. A random sample number is informed by the issues and the agency. In general, we aim to sample 20% of the total number of applications received by the agency for the determined assessment period. The assessment period may vary depending on the scope of the compliance audit.

In identifying the selection of sample records to be reviewed during the onsite audit, a record of the particular file reference will be made as against the assessments and observations made. This will then allow any findings to be supported and validated by the results of the onsite audit. As a matter of transparency and to ensure the integrity of the IPC's functions, the IPC will generally exclude from any audit sample any open or active reviews or complaints that are currently under consideration by the IPC with the exception of where the audit is directly responsive to the complaint.

2.9 Evaluation of audit evidence – desk top and onsite

Audit findings are generated by evaluating evidence collected before and during the onsite inspection or desktop review against the audit criteria.

The evidence collected may include observations made on-site, records and documentation on files, and documents produced by the Agency or their representative before, during or after the onsite inspection or desktop review. The evidence is generally assessed once the auditor is back in the office. IPC officers will:

1. Review information gathered to determine whether sufficient evidence has been collected to produce audit findings.
2. Identify and to the degree possible fill in any information gaps by following up with the auditee's representative.
3. Once the information gaps have been filled, evaluate the evidence against the audit criteria and compile a list of audit findings.
4. If working as an audit team, the list should be discussed among the team, and an integrated list of all auditors' findings should be compiled.

The assessments on the following page should be used to report whether each requirement has been met.

Table 1: Compliance, non-compliance, not determined and not applicable assessments

Assessment	Criteria
Compliance	There is sufficient and appropriate evidence to demonstrate the particular requirement within the scope of the audit.has been complied with.
Non-compliance	Clear evidence has been collected to demonstrate the particular requirement within the scope of the audit.has not been complied with.
Not determined	The necessary evidence has not been collected to enable an assessment of compliance to be made within the scope of the audit. There may be various reasons why the audit team could not collect the required information, including: • there was insufficient information on the file relating to the period covered by the audit to enable an assessment of compliance to be made • the wording of the criteria meant that no evidence could be gathered or it was too difficult to gather the evidence • there is no publicly available information to measure the compliance criteria in circumstances that would warrant publicly available information.
Not applicable (not activated)	There is no publicly available information to facilitate independent measurement of the compliance criteria in circumsatnces that would not warrant publicly available information.

The compliance audit officers should ensure that only the criteria are assessed, without considering what the intent is or may have been.

Once compliance with each requirement has been assessed, the auditor should document their findings in to the assessment tool.

The significance of a non-compliance can be assessed by considering factors such as:

- the level/degree of impact on or significance for citizens in being able to access their rights
- the level of alignment or otherwise with the objects of the respective legislation
- the level and extent to which the conduct does not promote openness, transparency and accountability
- the extent to which the non compliance relates to minimum mandatory requirements
- likelihood of the continued non compliance.

Appendix 4 gives an example of a risk assessment process for compliance issues that allocates a colour code to each non-compliance according to its environmental significance.

- Preparing audit conclusions.

The audit conclusion is the outcome of the audit after considering the audit objectives and all findings. The conclusion generally also summarises the extent of compliance of the auditee with the audit criteria.

2.10 Compliance audit report

The compliance audit report communicates audit findings and recommendations to the audited agency. It documents the overall assessment of compliance, and details the non- compliance identified during the audit and the follow-up actions needed to improve compliance.

The report must include details of the following:

- the audit background
- the audit scope
- the audit methodology
- identification of the auditee
- the dates and places where the audit activities were undertaken
- the audit criteria
- the audit findings
- the audit conclusions.

The report may also include:

- categorisation of the non-compliances with reference to the legislative requirements, observations made, findings made and any material relied upon to make that finding.
- recommendations for corrective or preventative action (including any projected dates for completion of the recommendation actions)
- any proposed monitoring arrangements to be applied.

The IPC applies a risk based approach to its compliance program and in this regard Appendix 4 provides a risk matrix to guide the rating and prioritisation that should be applied to recommendations made.

2.11 Draft reports and final reports

In addition to the requirement to provide procedural fairness throughout the conduct of the audit the IPC has a duty to ensure procedural fairness and natural justice in respect of the compliance audit report. Accordingly, the IPC will provide all auditees with period of not less than 2 weeks to review and provide comment on a draft compliance report unless exceptional circumstances arise. This will ensure that the requirements of section 23(2) of the GIIC Act are satisfied.

All comments will be taken into account in the finalisation of the draft report.

2.12 Adverse Comments

It should be noted that in some cases of significant non compliance or poor compliance posture, this may result in adverse comments being made in respect of the Agency. In such cases, officers must be aware of the particular requirements of the GIIC Act which provide certain steps that must be followed when a compliance report involves adverse comments. IPC Officers are to consult the Director, and Commissioner about the particular requirements of the GIIC Act and build into the audit timeframe sufficient time to enable the IPC to satisfy the requirements of sections 23(3) and (4) of the GIIC Act. The PPIP Act does not contain these provisions. However, in cases where there may be the potential for adverse commentary in relation to a privacy audit, IPC Officers will ensure fairness to the auditee by providing information about any proposed adverse comments in advance of finalising the report and providing sufficient time for the auditee to consider and provide any feedback on the adverse comments to the IPC.

2.13 Publication of reports

All compliance reports prepared by the IPC are prepared with the intention of publishing those reports to the IPC website. At the conclusion of the compliance audit, and after the final report has been prepared and issued, the report should be provided to the IPC Communications and Corporate Affairs Team for the purposes of publication to the website.

When providing the final report to the Agency, the finalisation letter should include reference to an indicative date that the report will be published by the IPC on its website. All finalisation letters should provide for a minimum of 3 days between the finalisation letter being issued and the date that the compliance report will be published to the website.

2.14 Follow-up action program

The purpose of the follow-up action program is to monitor the implementation of any proposed recommendations by the audited agency, and if required or requested to provide assistance and general guidance to the agency in achieving compliance with the recommendations. It also provides a mechanism to ensure that the Agency has taken postive action to remedy the particular issues identified within the audit by the IPC. Not every audit will necessitate monitoring of follow up action, each audit is considered on its circumstances and whether follow-up monitoring will be required will be informed by factors including but not limited to:

- The auditee's compliance history and posture
- Extent of and nature of the recommendations
- Previous evidence of non compliance or implementation of recommendations.

Monitoring the follow-up action program involves the following steps:

1. Establishing the follow up recommendations case type in Resolve
2. Listing all recommendations made in the audit report as individual recomendations and capturing a description of the recommendation, the date of recommendation, and date of implementation
3. Closely monitor the progress in implementing the follow-up actions and update and recognise satisfication of implementation of each recommendation
4. Once all recommendations have been implemented in full, close the follow up recommendation case type.

3. Quality assurance and record keeping

The value, rigour and credibility of a compliance audit depends on its proper management. All IPC compliance audits must be undertaken in accordance with the quality procedures detailed below.

The purpose of quality assurance procedures is to ensure that all audit tasks are carried out consistently. All compliance reports will be internally quality assured with peer review as set out below:

Table 2: Quality Assurance approach

Author	First Review
Regulatory Officer	Senior Regulatory Review Officer
Senior Regulatory Review Officer	Director, Investigation and Reporting
Director, Investigation and Reporting	Commissioner

All draft reports will be reviewed by the Director, Investigation and Reporting and the respective Commissioner before the report is issued to the Agency.

The purpose of record keeping is to ensure the proper and systematic recording of information and observations collected during a compliance audit. Good record keeping and filing procedures will ensure that all supporting documentation and observations are kept for future reference. This requirement also ensure that the IPC satisfies its requirements for record keeping under the *State Records Act.*

Every compliance audit is to be created in Resolve with all audit information stored in the file. A new file is created for each compliance audit. Each file should be retained electronically and the IPC adopted approach to the naming of documents convention is to be applied.

The table below gives an example of what sort of information should be kept in each file.

Table 3: Records to be kept for filing

File contents	Details
Audit correspondence	Store all correspondence relevant to the audit
Contact details	Include the name of any nominated contact person for the audited agency in conjunction with the details of the IPC officers who conducted the audit and dates of audit
Policy documents/guidelines	Include all policy documents and guidelines used to assess compliance.
Audit reference material and observations	Include all documents generated during the audit and preliminary tasks (ie, checklists, policies, observation notes). Include all other information sourced for the purposes of the audit and a copy of the assessment tool used.
Assessment of compliance	Include a copy of the compliance audit report including any detailed assessments undertaken.

File contents	Details
Audit notes	Include any file notes or records of observations, telephone discussions taken that have informed the compliance assessment
Compliance reports	All copies of the compliance reports including drafts are to be retained.
Other	Any other documents, not specifically referred to above that are relevant to the decision making process for the compliance audit.

4. Conclusion

This internal audit manual has been prepared to assist and guide the work of the IPC in its proactive compliance audit activity. It should be read in conjunction with the IPC's legislation at all times. In this respect it is not a comprehensive stand alone manual.

As the IPC continues to evolve its proactive compliance activity, the IPC will continue to review and build upon this manual.

Through the application of this manual to the IPC's proactive compliance activity will enable the IPC and staff to achieve three important objectives to :

- Encourage compliance
- Monitor compliance
- Respond to noncompliance.

5. Glossary

Audit element. A component of the activity/process/discharge that is being assessed for compliance with a regulatory instrument.

Auditee. An agency within the IPC's legislative remit being audited. The IPC audits agency's whose activities are regulated by legislation the IPC has a duty to uphold.

Case management system. Is the electronic systems used by the IPC to record and manage its regulatory acitivites and is known as Resolve.

Checklists. Lists of all the activities, processes and discharges to be addressed during the audit including a list of elements to be audited and the type of observations to be made to assess compliance.

Compliance Committee. Is an internal committee established within the IPC to lead, monitor and inform the IPC's regulatory activities.

Compliance audit. An assessment of an auditee's activities to determine whether the audit criteria are being met.

Commissioner. At the IPC shall mean either the Information Commissioner or the Privacy Commissioner.

IPC legislation. Legislation administered by IPC which includes:

- *Government Information (Public Access) Act 2009* (GIPA Act)

- *Government Information (Information Commissioner) Act 2009 (GIIC Act)*
- *Privacy and Personal Information Protection Act 1998 (PPIP Act)*
- *Health Records and Information Privacy Act 2002 (HRIP Act)*

Monitor. To systematically and repeatedly to track changes or establish the baseline or current conditions.

Quality assurance. A system of procedures to ensure that all audits are carried out correctly.

Appendix 1. Notice of audit

Enquiries: [insert contact officer]

Telephone: 1800 472 679

Our reference: [file reference]

Insert Agency Head

Insert Address

Dear [agency head]

Notice of Audit under the *Government Information (Public Access) Act 2009* (GIPA Act)

I refer to your correspondence of [insert date] to you concerning compliance by [insert agency] (the Agency) with the requirements of the *Government Information (Public Access) Act 2009* (GIPA Act) for [insert description of the audit issues].

The purpose of this correspondence is to provide you notice of my decision to undertake an investigation and to provide you with further information.

Section 21 of the *Government Information (Information Commissioner) Act 2009* (GIIC Act) provides that the Information Commissioner may investigate and report on the exercise of any function by an agency under an Information Act, including the systems, policies and practices of agencies. The reporting requirements in relation to an investigation under section 21 are set out in accordance with section 21(2) of the GIIC Act. Section 24 of the GIIC Act is also relevant to my reporting function.

This investigation will commence with an audit pursuant to section 17(g) of the GIPA Act. The audit aims to identify whether the [delete as appropriate : practices together with the systems, policies and culture] within the Agency promote compliance with the GIPA Act.

At this time the parameters of this audit will be limited to the specific [insert the a brief description of the scope of the audit] The audit will be conducted as a [insert whether the audit will be by way of desktop audit or on site audit] and will have regard to the information provided by the Agency along with its self-assessment results.

Additionally, I request copies of any [insert any information that you would to be provided to be used in the audit].

I anticipate that the audit, which will be point in time, will take place during [insert expected timing of the audit]. You may wish to nominate a contact officer, for the purposes of facilitating any engagement with the IPC that may be necessary during the audit.
Your co-operation in this audit will assist to ensure that the Agency's compliance is consistent with the requirements of the GIPA Act. Your response by way of:

- provision of copies of [insert description of information]
- and

- a nominated contact officer for the Council

should be provided by [insert due date for provision of the requested information]. It would be appreciated if in your return correspondence you confirm that you have provided all available complaints/enquiries and responses to those complaints/enquiries.

Please do not hesitate to contact me either on my direct number XXXX or by email on elizabeth.tydd@ipc.nsw.gov.au. Alternatively, your officers may also contact Ms Sonia Minutillo, Director, Investigation and Reporting on XXXX, or by email, sonia.minutillo@ipc.nsw.gov.au, if you have any questions.

Yours sincerely

Elizabeth Tydd

CEO, Information and Privacy Commission NSW

Information Commissioner

NSW Open Data Advocate

Appendix 2. Privacy Notice of Audit

Enquiries: [insert contact officer]

Telephone: 1800 472 679

Our reference: [file reference]

Insert Agency Head

Insert Address

Dear [agency head]

Notice of Audit under the *Privacy and Personal Information Protection Act 1998* (PPIP Act)

I refer to correspondence of [insert date] in which I wrote to you [insert background ie a notification of a data breach] by [insert agency] (the Agency) relating to the application of the information protection principles under the PPIP Act.

In that correspondence I requested your advice as to the [insert what we asked for]. On [insert date the Agency provided a response which included [insert summary of the response]

Having had the opportunity to consider the information provided by the Agency and the issues raised by the [insert as appropriate] I have determined that it appropriate to make further inquiries in relation to the matter.

Section 36()(l) of the PPIP Act provides that the Privacy Commissiner can conduct such inquiries, and make such investigations, into privacy related matters as the Privacy Commisisoner thinks appropriate.

Furter section 36(2)(a) of the PPIP Act provides that the Privacy Commisisoner has the function to promote the adoption of, and monitor compliance with, the information protection principles. Accordingly, I have decided of my own iniative that it is appropriate for me to review, inquire and masu such investigations into the processes, practices and governance in place for management of and compliance with the information protection principles relevant to this [insert description].

The aim of this is to identify practices within the Agency together with risks and provide regulartory assistance to promote compliance with the information protection principles consistent with my general functions under section 36 of the PPIP Act, but in particular in accordance with section 36(2)(a) of the PPIP Act.

I would anticpate that Officers of the IPC would attend the Agency in the week of [insert date] for this purpose.

It would assist in the progess of the inquiries if the Agency could provide the below information by [insert date due]

- insert description of information eg Privacy Management Plan

I look forward to you co-operation in ensuring that the privacy rights of citizens are upheld.

If you have any questions about this letter, please do not hesitate to contact me at samantha.gavel@ipc.nsw.gov.au. Alternatively, your officers may also contact Sonia Minutillo, Director Investigation and Reporting by email at sonia.minutillo@ipc.nsw.gov.au to confirm arrangements for IPC to attend the offices of the Agency.

Yours sincerely

Samantha Gavel

Privacy Commissioner

Appendix 3. Audit plan

Date:……

Name of Agency: ……..

Address: ……

……..

Date of (proposed) audit inspection or desktop review: ……..

File no: ……..

IPC Officers leading the audit: ……

……..

- Audit objectives:

……

……

……

……..

- Audit criteria:

……..

……..

……..

……..

……..

- Audit scope:

……..

……..

……..

……..

……..

……..

……..

Audit logistics: (desk top, onsite, combined)

……..

……..

……..

- Audit timetable: (key dates)

……..

……..

……..

……..

……..

……..

……..

- Roles and responsibilities of audit team members:

……

……

……

……

……

……

……

- Resource allocation (ie, budget, personnel):

……

……

……

Appendix 4. Example of a risk assessment process

This appendix describes an example of a risk assessment process for the compliance audit proces. Each non-compliance is assessed to determine the significance of its actual or potential impact/harm on the citizen rights. The significance can be assessed by determining the following two criteria for each non-compliance, using detailed guidance material:

- the level of impact caused by the non-compliance
- the likelihood of harm occurring as a result of the non-compliance.

After these assessments are made, the information is transferred into the risk analysis matrix below, so a colour code can be allocated.

		Likelihood of harm occurring		
		Certain	**Likely**	**Less likely**
Level of impact	**High**	Code Red	Code Red	Code Orange
	Moderate	Code Red	Code Orange	Code Yellow
	Low	Code Orange	Code Yellow	Code Yellow

A **red** colour code denotes that the non-compliance is of considerable significance and needs to be dealt with as a matter of priority. Recommendations made against a code red should require immediate rectification action with a due date of no more than 3 months. An **orange** colour code suggests that the non-compliance could receive a lower priority but must still be addressed. Recommendations against an orange code should require medium terms rectification with a due date of between 3- 6 months. All red and orange code recommendations require report monitoring by the IPC until satisfactory evidence of remediation is received.

A **Yellow** code recommendations may be implemented over a period of 6- 12 months and do not require monitoring by the IPC where they form the only reccomendations made.

The colour code is used as the basis for deciding the priority of remedial action required by and the timeframe within which the non-compliance must be addressed. While the risk assessment of non-compliances is used to prioritise actions to be taken, IPC considers all non-compliances to be important, and auditees must ensure that all are identified issues are resolved as soon as possible.

The number of red and orange code recommendations will inform an assessment of whether a follow up audit is required 12 months post the initial audit.

Document information

Identifier/Title:	IPC Compliance Audit Manual
Business Unit:	Director, Investigation and Reporting
Author:	Information/Privacy Commissioner
Approver:	Information/Privacy Commissioner
Date of Effect:	November 2020 Janaury 2023 (update)
Next Review Date:	January 2024
EDRMS File Reference:	D23/000694/DJ
Key Words:	Audit, compliance, auditee, audited, desktop audit, onsite audit

Document history

Version	Date	Reason for Amendment
1.0	October 2020	Initial Draft
1.1	November 2020	Second Draft – Information Commissioner Feedback
1.2	November 2020	Third Draft – Privacy Commissioner Feedback
1.3	November 2020	Approved
1.4	December 2021	Annual review, minor revisions
1.5	January 2023	Annual review, minor revisions and updates
1.6	January 2023	Approved