Australian Government

Australian Government Investigations Standard

October 2022

Foreword

The Australian Government Investigations Standard (AGIS) is intended to articulate Australian Government policy and is the foundational standard, framing accountability and security for entities conducting investigations relating to the government programs and legislation they administer.

The AGIS acknowledges the unique investigation environments for Australian Government entities and wholly owned Australian Government companies. Non-corporate entities will be required to comply with AGIS to the extent it articulates Australian Government policy in accordance with the *Public Governance, Performance and Accountability Act 2013.* Entities subject to the *Public Service Act 1999* are also required to comply on the basis their decisions are in accordance with Australian Government policy. This AGIS will additionally have application for non-government entities requiring investigation standards for the purpose of providing Australian Government investigation services.

This revised AGIS is principles-based supported with best practice providing an ability to measure compliance and ensure quality investigation outcomes for all entities. This is a modern approach delivering flexibility for entities to apply the AGIS relative to their own operations while also maintaining a standardised approach within investigations, particularly when working jointly.

I would like to recognise all entities for their collaboration and contribution to the process, in particular, the members of the AGIS Business Reference Group and the Criminal Justice Law Enforcement Forum.

Reece P Kershaw APM
Commissioner
Australian Federal Police

Contents

Introduction 1

AGIS Principles 1

Principle Streams 1

Application 2

AGIS review mechanism 2

1. Personnel 3

1.1 Professional role 3

1.2 Ethics and responsibility 3

1.3 Qualifications and learning 4

1.4 Competencies and mindset 5

2. Information and evidence management 7

2.1 Disclosure management 7

2.2 Information sharing 8

2.3 Investigation management system 8

3. Investigation practices 10

3.1 Risk management 10

3.2 Investigation governance 10

3.3 Investigation planning 12

3.4 Investigation activities and tools 14

4. Quality Assurance Framework 16

4.1 Quality Assurance Policy 16

4.2 Quality reviews and audits (types) 16

4.3 Scope for quality activities 17

4.4 Quality reports/outcomes 18

Appendix A: Abbreviations and Acronyms 19

Appendix B: References 20

Appendix C: Summary Table 21

Introduction

The Australian Government Investigations Standard (AGIS) establishes a standard for Australian Government entities conducting administrative, civil, or criminal (type) investigations. Where AGIS is in conflict with any applicable law, the legislative requirement will prevail. AGIS may apply in full or in part to types and stages of investigations. Entities must consider which investigations have different standards of proof, procedures and investigation requirements.

An investigation can be broadly described as an activity to collect information or evidence to a particular standard of proof related to an alleged, apparent or suspected breach. An investigation gathers information across a broad spectrum to assist entities to determine a course of action, which may also be preventative and/or disruptive action instead of prosecutorial.

The AGIS does not encompass standards for intelligence and compliance functions (including early intervention). The AGIS acknowledges the existence of these functions across the regulatory and enforcement continuum and as such, each entity should address and take the steps necessary for management of the information, conducting inquiries or assessments, and the use of specific regulatory tools in consideration of all types of investigations.

AGIS Principles

The following are principles guiding and reinforcing AGIS and apply to all types of investigations:

- **Ethics and professionalism are applied and performed to the highest order in investigations.** Ensure both decision-making procedures and process are in place and maintained including that investigation decisions are transparent and documented.
- **Investigations support the business and reputation of government.** Undertake a collaborative approach between entities and adhere to all legislative requirements to ensure appropriate use of public money, government information, and government assets.
- **A continuous cycle of review is applied to investigations.** Risk and review are managed and built into planning and process to ensure learning continues and best practice evolves.
- **Entities are responsible for investigation information management of their entity.** Provide the most secure, effective, and efficient systems to provide security and process assurance.

Principle streams

The AGIS principles are connected to **four streams** of core requirements, best practice, and guidance:

1. **Personnel**
   Each entity ensures its investigators are suitably qualified and experienced to conduct and/or supervise investigations with the highest standard of ethics and conduct.
2. **Information and Evidence Management**
   Each entity maintains appropriate information management and evidence handling protocols and uses suitable electronic systems for end-to-end investigations.
3. **Investigative Practices**
   Each entity conducts investigations in consideration of a number of risks using consistent and quality practices to meet the requirements of admissible evidence.
4. **Quality Assurance.**
   Each entity makes quality assurance a priority and introduces informal and formal processes during the lifecycle to ensure continual improvement.

The AGIS articulates what entities **should** and **must** do to achieve the Australian Government's standard.

SHOULD

An activity that is regarded as the recommended course of action or best practice. Deviation is a decision and **must** be recorded.

MUST

An activity that is required by legislation, governance, supported by case law or best practice. Deviation is a decision to be fully examined, explained, and **must** be recorded.

Both **should** and **must** are considered best practice. If a component **must** be undertaken, the activity is required by law or the severity/significance of the consequence associated with not undertaking, or as a result of judicial expectations. The risk to an entity's investigation performance is greater if this level of directive is not followed.

Application

Entities **should** have a policy regarding their investigation function. The policy **should** include:

- an outline of the entities' remit in the context of types of investigations conducted
- statements regarding the application of AGIS for particular types of investigations
- statements regarding the assignment of AGIS qualifications for investigation areas
- statements regarding the entities' responsibility to refer matters or investigations to law-enforcement entities or other relevant bodies.

AGIS review mechanism

It is important that AGIS remains consistent, relevant, and current. The Australian Government will review this AGIS formally on a five yearly basis and in the event any significant changes arise to the operating environment.

1. Personnel

1.1 Professional role

A government investigator is prescribed as a professional job role within Australian Government Frameworks[1]. Entities may also have their own prescribed professional job role equivalent to a government investigator.

Entities' recruitment documentation **should** reflect investigation roles/positions as a professional stream and consistently outline qualifications (or equivalency) competencies, skills and experience (both technical and non-technical) commensurate and required to perform types of investigations. Remuneration for investigation roles is not determined by AGIS.

Entities **must** identify and assign security clearance requirements against investigator roles/positions, proportionate with accessing classified information and to provide greater assurance in handling investigation material[2]. When assigning requirements, entities working in joint investigations **should** consider the security clearance requirements of other entity/entities.

1.2 Ethics and responsibility

1.2.1 Rule of Law

The Australian rule of law applies to everyone regardless of position or status and offers protection against the use of arbitrary power. Investigators and investigation decision makers (operational and non-operational) have a privileged position and **must** operate and conduct their duties with fairness, equality, consistency, professionalism, meet prosecutorial obligations and other regulatory duties for inquisitorial bodies. An investigator and/or investigation decision maker is accountable for actions, expected to make considered and defensible decisions and protect, to the best of their ability, vulnerable persons.

1.2.2 Conduct

Entities and investigators **must** conduct investigations in accordance with the following:

- relevant statutory entity or independent entity Values, Code of Conduct, Code of Practice and/or Code of Ethics and/or
- Australian Public Service (APS) Values, Employment Principles and Code of Conduct in accordance with Australian Government legislation[3].

1 Australian Public Service Commission, Job Family Framework, Australian Government, July 2021
2 Attorney-General's Department, Protective Security Policy Framework, Policy 9: Access to information, Australian Government, September 2020
3 Australian Public Service Commission, APS Values, Employment Principles and Code of Conduct, Australian Government, May 2021

Entities may be subject to complaints about the handling of investigations. Complaints may be via internal entity reviews, the *Public Interest Disclosure Act 2013* or through other independent government oversight authorities such as the Australian Commonwealth Ombudsman (CO), Inspector General of Intelligence and Security (IGIS) or Australian Commission for Law Enforcement Integrity (ACLEI)[4].

Entities **must** have procedures in place, relevant to legislation, which appropriately deal with complaints about the handling of investigations and cooperation with independent government oversight authorities investigating complaints made about an entity's investigation.

1.3 Qualifications and learning

1.3.1 Accredited qualifications

AGIS recognises entities will vary in the requirements for qualifications and skills to conduct types of investigations. To preserve the ongoing Australian government capability for investigations, a vocational and educational training (VET) qualification **must** be obtained, unless another qualification or internal training is determined as equivalent.

Entities **must** document the required VET accredited qualification/s (or equivalency) to conduct particular types of investigations and the timeframe in which investigators should obtain the qualification.

Entities **must** use an Australian Registered Training Organisation (RTO), or an Australian Government entity with Australian RTO status that meets the Australian VET standards to obtain or deliver investigation accredited qualifications.

The Australian nationally recognised VET accredited qualifications to conduct investigations are:

- *Certificate IV in Government Investigations* as set out in the Public Services Package (PSP) for persons/officers working in operational roles undertaking government entity investigation related functions (foundational)
- *Diploma of Government Investigations* as set out in the PSP for persons/officers engaged in the operational coordination and supervision of entity investigations in government related functions (supervisory)
- *Advanced Diploma of Government Investigations* as set out in the PSP for persons/officers working in operational coordination and supervision of multi-entity investigations in government related functions (extension supervisory).

Entities **must** ensure foundational qualifications (or equivalency) are obtained prior to supervisory qualifications.

4 Australian Government, Public Interest Disclosure Act 2013, No. 133, July 2013

1.3.2 Qualifications, training and/or experience for equivalency

Equivalency relating to a VET qualification for investigations can be:

- changes made to VET investigation qualification packages by industry Skills Service Organisations (SSO)
- other recognised or relevant qualification/s for undertaking investigations under Australian standards supported by evidence
- formal industry training that has imparted skills and knowledge which results in a demonstrated investigations competency
- informal training or experience that has imparted skills and knowledge which results in a demonstrated investigations competency.

Entities **must** determine and document qualifications, training or experience equivalent to VET accredited qualifications required for a type of investigation. In doing so, entities **should**:

- determine legal, enforcement or regulatory qualification/s as equivalency to replace VET accredited qualification/s to perform the role of an investigator or supervisor or operational decision maker
- determine formal training (type, currency) as equivalency to perform the role of an investigator or supervisor or operational decision maker
- determine informal training and/or experience (type, currency and time spent) as equivalency to perform the role of an investigator or supervisor or operational decision maker with regard to contemporary skills and changing environment
- outline additional requirements for learning and/or entity certification requirements in order to satisfy conducting a type of investigation as an investigator or supervisor or operational decision maker.

1.3.3 Qualifications risk management

Entities **must** consider the legal risk associated with investigators, supervisors or operational decision makers without an appropriate VET accredited qualification or appropriate equivalency engaged in an investigation role. Entities opting to use recognition of prior learning (RPL) in order to obtain accredited qualifications should take into consideration the currency of the prior learning and the changing investigative environment.

1.4 Competencies and mindset

1.4.1 Competencies

Competency is a measure of both proven skill and knowledge, theory, and practice. An investigator **should** have the capability to apply both a foundational and advanced set of related investigation knowledge, skills, and abilities to successfully perform critical analysis, decision-making, and investigation tasks.

Foundational competencies **should** be met and continue to be met against the following critical investigation elements:

- planning/conducting/initiating/finalising an investigation
- collecting, assessing and presenting evidence
- information management and disclosure
- formal interviewing and taking statements (person of interest and witnesses)
- search and seizure
- preparing briefs of evidence
- compile/use official notes
- applying powers.

Competencies such as data analysis, surveillance and/or detainment/arrest **should** be considered as part of an entity's broader support for learning once skills, knowledge and experience are beyond foundational, unless required sooner under an entity's legislative or functional remit.

1.4.2 Maintaining capability

The ever-growing complexities of the operating environment and ongoing demand requires investigators to constantly review and upgrade capabilities. Constant change both domestically and internationally means investigators **must** maintain a keen sense of the environment within which the investigation is being managed.

An entity **should** have clear support measures for an investigator's continued skills uplift, learning, and professional development proficiency.

An entity's investigation capability support and guidance **should** focus on:

- implementing investigation and/or crime type learning frameworks into broader entity learning strategies
- maintaining and expanding the knowledge base and competency of investigators
- supporting the individual needs of investigators with professional development and specialised learning
- providing current, contemporary, and relevant activities that augment and develop the overall investigative capability of the entity
- providing an allowance of dedicated time, where possible, for continuing professional development or formal development to safeguard the integrity of the investigation profession.

1.4.3 Mindset

The investigative mindset highlights attributes, knowledge, and cognitive skills relevant to the investigations craft. A good investigator:

- is committed, naturally inquisitive and continually engages in personal and organisational learning
- applies critical thinking and innovation in the development of investigative strategies that are adaptable in application
- is a responsible leader and an excellent communicator who always asks questions while being respectful of all
- identifies and utilises all available resources including specialist expertise
- is tenacious, collaborative, courageous and unrelenting in the search for the truth without being inflexible
- is always current with laws, governance, and investigative techniques
- is a calculated risk-taker who is accountable for their actions and whose decisions are reasonable, proportionate, and necessary[5].

5 Australian Federal Police, AFP Doctrine, March 2022

2. Information and evidence management

Information management is a critical component of investigation management and is essential in ensuring all relevant information is retained in a format which best supports investigations, auditing, and judicial proceedings.

Entities' information management policies and practices (inclusive of information sharing) **should** support all types of investigations as well as prevention, disruption, or inquiry outcomes.

An entity's investigation policies and practices **must** have regard to the legislative scheme under which information is obtained to ascertain any restrictions on the use of the information and the circumstances in which information may be disclosed.

2.1 Disclosure management

Disclosure management (duty of disclosure) varies between jurisdictions and types of investigations. Legal advice should be obtained by entities involved in gathering, obtaining, revealing and producing material in relation to disclosure during and post an investigation. An investigator's duty to disclose is ethical in nature, and is an obligation owed to the court to ensure the accused's right to a fair trial. Accused persons are entitled to know the case against them to properly defend the charges faced. Applicable local statutory obligations (state or territory) relating to disclosure also require compliance[6].

Commensurate with the type of investigation, an investigating entity's duty of disclosure **must** be considered in initial investigation planning including the implications of disclosure. Investigators **must** make available material relevant to the investigation and the activities **must** be recorded and retained to enable the investigative entity and prosecuting entity (both determined as the prosecution) to comply with the duty of disclosure. The duty of disclosure is ongoing throughout a prosecution process and continues after a trial and the conclusion of any appeals.

Entities **must** develop clear procedures and supporting tools to record, retain, register, review, reveal, and produce investigation information. An entity **must** also have clear procedures on the request, retention, and disclosure of material held with a third party (entity). Investigators or persons responsible for disclosure coordination **must** retain all records on requests or attempts to obtain material relevant to an investigation. In consideration of the scale, complexity and type of investigation, entities **should** appoint a Disclosure Coordinator to coordinate and oversee the recording, retaining, registering, reviewing, and handling of all disclosure material, and conduct the application of exceptions (with decision) to disclose, throughout the course of an investigation.

2.1.1 Disclosure in criminal proceedings

Information, material, other legal claims or other outcomes protected from disclosure **must** be in accordance with the law, policies, and entity legal direction (grounds for protection). Exceptions may be related to public interest immunity (PII), precluded by statute and/or legal professional privilege (LPP).

The milestones and timeframes for criminal proceeding disclosure **must** be in accordance with State/Territory law, practice, and court directions to produce a Brief of Evidence (BoE).

6 Office of the Director of Public Prosecutions, Statement on Disclosure, Australian Government, March 2017.

2.1.2 Disclosure in civil/administrative proceedings

A duty to disclose information can arise through a number of avenues in both the civil and/or administrative investigation context. These avenues may include but are not limited to summonses, orders of discovery issued by a court in civil proceedings, requests for information under the *Freedom of Information Act 1982* (Cth) and requests for information under s.71 of the *Safety Rehabilitation and Compensation Act 1988* (Cth).[7,8] Disclosure of information may also be required in order for an entity to fulfil an obligation to provide procedural fairness in relation to an administrative decision. Entities **should** have procedures in place to manage disclosure in the civil and or administrative context.

2.2 Information sharing

Entities **should** work collaboratively to detect and respond to alleged or suspected breaches occurring across the Australian Government and jurisdictional boundaries through sharing of information.

Sharing of information **must** be in accordance with the *Privacy Act 1988* and any secrecy provisions within legislation that may govern information sharing[9]. Entities **should** have procedures in place for receiving, responding, and requesting information from other entities.

2.3 Investigation management system

Entities **should** have an electronic investigation management system (EIMS) to record, collate and manage investigations from report of allegation/information through to a BoE or other outcome actions (disruption), and finalisation (referral, closure, or prosecution). An entity's EIMS solution **should** consider integration architecture and be interfaced or synchronised with other relevant systems to ensure integrity and continuity of information/ evidence collection. An EIMS solution **must** be supported by an internal or external sustainment and/or support arrangement.

An EIMS **must** be delivered in accordance with the Australian Government Information Security Manual, Protective Security Policy Framework (PSPF), Privacy Impact Assessments (PIA), and relevant records management legislation applicable to the Australian Government. [10,11,12]

Entities **should** obtain PROTECTED accreditation for an EIMS if viable, as best practice for security and information management[13].

7 Office of the Australian Information Commissioner, Freedom of Information Act 1982, Australian Government, Oct 2021
8 Comcare, Safety, Rehabilitation and Compensation Act 1988, Australian Government, March 2022
9 Office of the Australian Information Commissioner, The Privacy Act 1988, Australian Government, Oct 2021
10 Australian Signals Directorate, Information Security Manual, Australian Government, December 2021
11 Attorney-General's Department, Protective Security Policy Framework, Australian Government, March 2022
12 Office of the Australian Information Commissioner, Australian Government Agencies Privacy Code 2017, Australian Government, 27 October 2017
13 Attorney-General's Department, Protective Security Policy Framework, Policy 8: Sensitive and classified information, Australian Government, 18 March 2022

2.3.1 Specifications

An entity's EIMS **should** have the following high level functional requirements as standard:

- **Allegation or Intelligence Receipt** – the capture and evaluation of information to determine whether an investigation or other activity should take place in accordance with priorities and legislative requirements
- **Evaluation** – activity that collates, structures, links, and facilitates the assessment of information to determine further investigative activities to take place
- **Planning** – a guide to how an investigation should be conducted (approach) that is reviewable and able to be updated
- **Investigative activities** – planned tasks that allow the collecting and collating of information to form evidence, and production of procedural products, documents, and legal instruments.

An entity's EIMS **should** also include the following specific capabilities:

- **Investigative management** – enable coordination of planning, tasking, scheduling; manage offences and respective avenues of inquiry; manage access to an investigation and related entities and relationships
- **Planning** – support creation of diverse types of plans; ability to draft, review and approve a plan
- **Tasking** – creation of a task and assignment of resource, associating task to activity, work-flowing a task, monitoring (status) and progress report
- **Scheduling** – creation of a schedule, prioritising, sequencing, and linking based on priority and timing for tasks and activities
- **Reporting** – reporting on investigative activities and administrative activities
- **Chronology** – time (zone) ordered compilation of information events being investigated, tasks and activities, created data sets and uploads
- **Procedural documents & product generation** – legal and specialised documents specific to jurisdiction including BoE
- **Investigative activity recording** – recording of decisions, activities, conversations, correspondence, and meetings
- **Library of reference data** – crime types, offence categories, offence details, elements/proofs/defences, indictments, alerts and warnings, and relationship types
- **Property/Seizures** - recording property as evidence, property as proceeds of crime, chain of custody, disposal of seizure and exchange of property
- **Information capture and management** – merging of records, source tracking, distribution and dissemination caveats, redactions, bulk ingestion and exporting.

Specifications **should** be aligned with an entity's relevant information on security manual controls including, but not limited to, security profiles, user security profiles, data security profiles, and application security.

3. Investigation practices

3.1 Risk management

Persons, or groups of persons responsible for, and in control over an entity's operations have both the opportunity and a responsibility to instil a positive risk culture. A positive risk culture encourages entities to identify and respond to potential threats, systemic weaknesses and vulnerabilities that undermine public confidence and the integrity of the government. All levels **must** be empowered to monitor and engage with risk in a manner consistent with the objectives and risk appetite of the organisation[14,15].

Risk management is designed to coordinate activities to direct and control risk. Risk is reflective of the complexity, dimensions, and scale of an investigation and is inherently simultaneous across multiple stages: the report, receipt and acceptance, process of inquiries, a referral, rejection, termination/closure, finalisation, and review/audit of an investigation.

As part of instilling a strong risk culture, entities **should** establish an investigation's Risk Management Framework and processes with a focus on:

- developing a triaging approach (use of a categorisation and prioritisation formula or model)
- outlining key responsibilities and accountabilities (positions, committees)
- establishing a reporting regime of investigation risks (internal and external) to inform the strengthening of investigation risk controls
- embedding continual risk assessment into investigation stages and processes
- implementing processes to demonstrate appropriate investigator risk decision making
- acknowledging shared and cross jurisdictional risk as part of an investigation.

Entities' investigation's Risk Management Framework **should** be aligned with and reflect an entity's enterprise risk framework, standards, guidance, and policies alongside that of the Australian Government. Australian Government corporate entities **should** align, and non-corporate entities **must** comply with the Commonwealth Risk Management Policy[16].

3.2 Investigation governance

3.2.1 Legislation and entity policies

Legislation, powers, and regulations in each entity may differ considerably. AGIS provides best practice noting variables may occur based on entity legislation.

In the context of federal criminal investigations, entities **must** comply with Commonwealth Director of Public Prosecutions (CDPP) guidelines or requirements in relation to engagement with the CDPP. This includes the provision of pre-brief advice and the preparation and referral of BoE's for prosecution. Where a criminal investigation is being undertaken or contemplated, evidence **must** be obtained with a view to admissibility in criminal proceedings and assessment of a BoE in accordance with the Prosecution Policy of the Commonwealth[17].

14 Department of Finance, Public Governance, Performance and Accountability Act 2013, Australian Government, February 2021
15 Department of Finance, Independent Review into the operation of the PGPA Act 2013 and Rule, Australian Government, February 2021
16 Department of Finance, Commonwealth Risk Management Policy, Australian Government, July 2014
17 Office of the Director of Public Prosecutions, Prosecution Policy of the Commonwealth, Australian Government, Canberra 2021

3.2.2 Legal adherence

Investigations **must** be conducted in a manner that is consistent with applicable laws. This is particularly relevant regarding collection, handling, and presentation of evidence and the application of powers. An investigator **must** be familiar with implications of relevant law on their ability to collect, manage and present evidence and investigate.

Investigators **should** consider the broad spectrum of legal requirements to ensure that any action taken does not jeopardise the investigation. Differing legal requirements across various jurisdictions involved **should** also be considered. Entity governance may also have implications for the conduct of investigations.

Investigators **must** be cognisant of the impact of LPP. Entities **must** have procedures and forms in place to deal with LPP during relevant types of warrants (i.e. search, monitoring) to cover:

- electronic and hard copy non-legal premises
- electronic and hard copy legal premises.

Entity LPP procedures **must** consider options for quarantining data or documents which is the subject of a LPP claim and the timeframe a LPP claimant **should** be given to advise of the option chosen.

Entities **should** have a process in place to outline who will be responsible for making entity LPP protective order applications.

3.2.3 Decision making

Decision making is a structured approach to identifying and analysing alternative approaches from which a choice can be made, and action taken to achieve an outcome. Any information available, assessment of risk and identification of options need to be provided in a decision-making process for it to be a considered decision and to apply accountability.

Entities **should** have a decision-making process in place for investigations involving options and actions that can be explained, justified, and documented. Using a decision-making process ensures decisions are effective, transparent and can sustain review and scrutiny. The individual governance of an entity **should** inform the type of decision-making process chosen for investigations, noting ethical complexities.

Decisions made during an investigation **should** be made by an appropriate person as determined by the entity. There are multiple forms in which a decision can be recorded/documented including (but not limited to) notebooks, diaries, emails, minutes, executive briefs, decision registers, and information management systems.

The recording of a decision **should** be proportionate to the seriousness and consequence of the decision. Documentation **must** include:

- the context of the decision
- the decision itself
- the reason/rationale for the decision
- person making the decision
- date of the decision
- any detail the actions associated with the implementation of the decision.

If a decision is not able to be recorded prior to action it **should** be recorded as soon as practicable after the fact.

3.2.4 Evidence and exhibit handling

Entities' evidence and exhibit handling procedures **must** comply with applicable Australian laws of evidence, relevant case law, and Australian Government directions or guidelines on search and collection/seizure. Security and continuity **must** be maintained from seizure or collection to disposal to ensure admissible evidence in judicial and administrative proceedings. Entity procedures **should** cover (but not limited to):

- preserving evidence in a timely way and handling to avoid contamination;
- engaging persons for analysis and evidence management, with appropriate training and qualifications to ensure admissibility
- using recording systems in relevant circumstances to manage risk of impropriety accusations
- employing methodology for recording evidence found in search and seizure situations
- using formal property seizure and/or receipt records
- using an exhibit register and naming convention system (or use of unique bar code) to record seizure and movements
- creation of digital evidence for preservation of perishable items
- changing of case officer (acquittal or transfer or exhibits)
- maintaining the health and safety of investigators.

Entities **should** establish evidence or exhibit rooms that align with security requirements under the PSPF and relevant Australian building standards.

3.2.5 Exhibit registry

To maintain standards of proof, investigators **should** review their case holdings (evidence) once a month in the case of high-risk exhibits (i.e. hazardous substances, weapons)[18].

An entity **must** have a documented procedure for conducting formal audits of its Exhibits Registry (commensurate with the type of investigation) to ensure:

- the accuracy of the records
- independent scrutiny of the procedures associated with possession of exhibits by an entity
- the security of the exhibits meets entity investigations policy and the PSPF
- continuity of evidence has been maintained.

The entity procedure **must** also ensure the audit regime incorporates:

- quarterly auditing of holdings (all or percentage)
- annual auditing of holdings (all or percentage)
- auditing of full holdings (timeframe).

3.3 Investigation planning

3.3.1 Function intersection

Investigations may have a relationship with an entity's compliance and/or intelligence functions.

Compliance is described as responsive regulation with variable support and enforceable sanctions. Entities may have different legislation and policies related to compliance.

18 Federal Register of Legislation, Evidence Act 1995, October 2018

Investigation planning **should** consider compliance activities and processes in respect of admissible evidence collection/use. Entities **should** obtain legal advice prior to collection and/or use of information sourced as part of a compliance activity if planning to use for another type of investigation.

An investigation can include intelligence activities and processes which may directly support the gathering of admissible evidence. Where relevant, entities **should** have a guide outlining the use of intelligence in identifying conduct which is allegedly or suspected to be a breach.

An entity **should** ensure compliance, intelligence, and fraud control functions are appropriately linked to investigations.

3.3.2 Reports, commencement to finalisation

The investigation function requires definitions, protocols, and information management processes. For the purpose of AGIS, 'report' is used and defined as a report, referral, or a notification of suspected wrongdoing or allegations in relation to breaches, noting entities' definitions and processes may differ in line with legislative requirements or investigation policies.

For reports, entities **should** have the following:

- a public facing process for the public and entities to report
- electronic systems and procedures to record the receipt of reports
- electronic systems and procedures to record the transfer of reports.

An entity's transfer of reports to law-enforcement entities **should** be informed by:

- a law-enforcement entity's authority and prioritisation model (including thresholds)
- an entity's capacity and ability to conduct the investigation
- the significance of harm to the community
- the integrity of the Australian Government
- whether the report involves *Commonwealth Electoral Act 1918* alleged breaches
- any action required in relation to proceeds of crime
- conflicts of interest and political sensitivities[19].

An entity **should** ensure an investigation life cycle (from commencement to finalisation) is a documented process and connected to investigation policies and risk management.

An entity **should** establish criteria for when an investigation is considered to be commenced, which may include the following circumstances:

- on direct receipt of a report
- informal assessment of a report warrants further inquiry and investigation
- intelligence activities have begun
- formal process of evaluation is conducted and completed, and acceptance of an evaluation has been conducted by decision makers.

19 Australian Electoral Commission, Commonwealth Electoral Act 1918, Australian Government, February 2022

An entity **should** establish criteria for when an investigation is considered to be finalised, which may include the following circumstances:

- an entity's treatment of the allegations has concluded (prosecution including appeal, or other)
- the allegations have been referred to another entity for further action without joint participation
- disruptive action has been effective and considered as the primary treatment
- the subject of a report is deceased.

3.3.3. Resourcing

Entities' resourcing for investigations **should** be commensurate with the type, complexity, and scale of an investigation including the breadth (or cross over) of the entity's function.

Individual investigations **should** consider assigning two investigators for each commenced investigation, supplemented by specialists as required. This best practice is related to ensuring objectivity, minimising bias and maintaining investigation integrity.

Each entity **should** conduct ongoing management and review of own investigation procedures, manuals, or instructions to ensure currency and accuracy to support capability and outcomes. The timelines for review **should** consider the changing operating environment regarding legislation, technical transformation, outcomes to investigations and risk.

3.3.4 Entity agreements

Alongside sharing of information under legislative provisions, entities **should** develop Memoranda of Understanding (MoU), Service Level Agreements (SLA) or investigation-specific Joint Agency Agreements (JAA) to assist with lawfully sharing information or conducting investigations that may cross jurisdictions or require specialist entity support.

3.3.5 Media management

Entities **should** have written procedures regarding liaison with the media and the release of media statements regarding investigations. These procedures **should** include reference to the following:

- media management strategies within investigation plans
- authority to release information to the media
- circumstances for briefing and use of media area or spokesperson
- level of release to the media
- management of multi-entity operations.

Information released to the media **should** not expose investigation sensitive methodologies, prejudice right to a fair hearing or the legal process, impinge upon the privacy or safety of others involved in the investigation, or prejudice any actions taken or future actions of the entity or other entities.

3.4 Investigation activities and tools

3.4.1 International requests

An entity investigator can seek information on an informal or formal basis from foreign authorities. Formal requests are required where information is sought when an investigation requires the exercise of a compulsory or coercive power, such as issuing of a subpoena or search warrant by foreign authorities, or where admissible evidence is required for the purpose of court proceedings.

Mutual assistance is an important part in the investigation planning process. The mutual assistance process can only be used to seek assistance to further an investigation or prosecution of a criminal matter or proceeds of crime proceedings[20]. Mutual assistance arrangements for civil or administrative investigations are governed by state or territory court rules and other relevant legislation.

The types of information and assistance sought will be dependent on the investigation. They may include travel records, taking witness statements, identification records, court documents, business and bank records, and communications service provider records.

Entities **must** use the Australian Government's mutual assistance regime request for the formal process of obtaining information for an investigation. That is unless specific entity legislation allows for requests via alternate means or advice by an administering Australian authority.

Entities **should** have written procedures for making informal requests to foreign authorities. These procedures **should** consider the use of Australian law-enforcement entities to assist.

Entities **should** additionally have written procedures for responding to both formal and informal requests from foreign authorities. If there are capital punishment (including death penalty) implications in requesting and responding to foreign requests, entities **must** consult with Australian Government administrative and/or legal entities.

Further information can be found in the *Mutual Assistance in Criminal Matters Act 1987* (Cth)[21].

3.4.2 Experts

It may be necessary to use an expert witness for the purpose of an investigation or a proceeding arising out of an investigation. The selection of an expert **should** be made following consideration of the person's professional standing, qualifications, publications, capabilities, and relevant experience. The following **should** be considered when using expert witnesses:

- ensure the expert opinion is impartial
- consideration of a non-disclosure agreement (material with security classification)
- ensure compliance with the rules of evidence
  - obtain and record relevant legal advice regarding using an expert
  - review evidence legislation, court notes or case law relating to using an expert.

3.4.3 Specialist services

Investigations may require the use of specialist services, for example surveillance (physical/digital), coercive hearing, telecommunications interception, or use of human covert sources.

Entities with powers to conduct specialist services **must** have procedures in place in accordance with legislation, the *Privacy Act 1988* and Australian Government security frameworks for handling information. Procedures **should** outline roles and responsibilities to conduct specialist services and all governance applied including the protection of sensitive methodology.

Entities **must** also have procedures in place to request specialist services from other entities with specialist services.

20 Attorney-General's Department, taking-evidence-across-international-borders, Australian Government, March 2022
21 Attorney-General's Department, international-relations/international-crime-cooperation-arrangements/mutual-assistance, Australian Government, March 2022

4. Quality assurance framework

Consistently meeting requirements, and addressing future needs and expectations, can pose challenges in dynamic and complex investigative environments. The benefits of implementing a quality assurance framework include:

- ability to consistently provide products that meet applicable legislative, statutory, and regulatory requirements
- facilitating opportunities to enhance partner entities' satisfaction
- addressing risks and opportunities associated with activities
- implement preventative controls to minimise risks
- corrective action and continual improvement process.

Quality assurance is linked to the international risk management standard (AS/NZS ISO 31000) and assurance model of 'three lines of defence'.

4.1 Quality assurance policy

Entities **must** have an investigations Quality Assurance Policy in place that includes:

- conducting quality assurance activities (type and frequency) for types of investigations; and
- linking quality assurance activities to an entity's annual enterprise risk assurance program.

Entities **should** conduct one formal external quality assurance activity every two years. Entities **should** report quality assurance decisions and activities to the relevant governing entity Committees or Executive.

A quality assurance activity for investigations **must** be done by an entity following a request by an entity's own Accountable Authority as defined under the *PGPA Act 2013* or established relevant governing entity Committee.

4.2 Quality reviews and audits (types)

Reviews and audits are both purposeful quality assessment activities of investigative performance with defined parameters to assist investigative progress, inform decision making and provide a cycle of organisational, shared, and individual learning for continual improvement. Quality reviews and audits (types) can be a continuous cycle of singular or combinations of:

- informal (self-review)– investigator/s performing investigation (first line of defence)
- informal (peer) - investigator not connected to investigation (first line of defence)
- informal (supervisory) – overseers of investigation (first line of defence)
- formal (internal audit) - own entity independent reviewers/auditors (second line of defence)
- formal (external) - other entity or external organisation reviewers/auditors (third line of defence).

4.2.1 Quality reviews

Reviews assist investigators by presenting opportunities to apply critical thinking to the progress of an investigation, confirm the direction, reflect on the outcome of an investigation, guide future activities, and integrate lessons learned.

During the planning of any investigation, informal review **should** be considered and appropriately incorporated to an investigation plan. This may include the setting of milestones or specified events which will trigger self, peer or supervisor review, or stating intervals at which reviews will be conducted during an investigation.

A review can take place during an investigation or post investigation.

4.2.2 Quality audits

Auditing provides quantified results in relation to a theme or topic against a set measure. An audit **must** have a set measure with which to determine compliance. Quality audits can also include performance audits (no set measure) in the absence of a standard or legislation.

An audit is performed on a collection of investigations or investigative processes rather than a single investigation, or an investigator's individual performance. An audit **should** commence with the identification of a data set relevant to a scope and objectives. A random selection is then taken to form the audit sample.

An audit **should** take place once an investigation has concluded, however, if the audit involves a theme or activity that will not jeopardise the investigation, it can be done during an investigation.

4.2.3 Conduct of quality activities

The conduct of a review or audit and any material produced during, or as a result of the review or audit, is disclosable. This **should** not restrict the conduct of activities. Material produced **should** be done with due consideration to quality, and **should** be appropriately security classified. Where necessary, material which could be subject to a claim of PII or LPP **must** be identified.

4.2.4 Integrity

A formal review or audit **must** be an independent and objective assessment of the quality of investigative practices and procedures. Unbiased review will provide integrity to the quality assurance review process. Investigators **must** only assist to provide investigation information if they are the case officer of an investigation being reviewed or audited.

4.3 Scope for quality activities

An entity's quality activity scope **should** identify performance measures such as:

- satisfaction regarding the quality of BoE submitted to the relevant prosecuting authority or external counsel
- judicial comments (both favourable and unfavourable) received about the conduct of investigations by the entity (published and unpublished)
- entity's own key performance indicators (if relevant)
- identification and reporting of risk control vulnerabilities.

Where a quality activity considers issues relevant to a prosecuting authority or external counsel, such as adequacy or satisfaction of the preparation or submission of BoE, the entity **should** consult with the prosecuting authority regarding the scope.

An entity **must** consider AGIS when considering the scope for quality assurance. Own entity investigations policy, doctrine, standards, and best practice guides **should** also be determined for reference during a quality activity.

Entities can conduct quality activities on investigation themes such as operational activity, information management, leadership, decision making, communication, and planning. Further, specified events within themes can be used such as arrest, search, bank warrant/s, person of interest interview/s, witness management, critical decision points or disruption activities. Events will be specific to each investigation and entity.

4.4 Quality reports/outcomes

For formal internal or formal external quality activities, entities **should** request opportunity to comment on the draft of a review report. The entity's comments **should** be incorporated into a final quality review report.

Finalised reports **should** be provided to the person in control of the entity, relevant governing entity Committee or delegated position.

Results of a quality activity **should** be provided by the entity (relative to information and risk management) to other relevant entities to continue to improve investigative quality across the Australian Government.

An entity can decide on the option to publish own types of quality review reports. An entity involved in a review of another entity **must** seek express authority prior to publishing a report on behalf of the owning entity, unless the entity has authority without agreement.

APPENDIX A

Abbreviations and Acronyms

ACLEI	Australian Commission for Law Enforcement Integrity
AGIS	Australian Government Investigations Standard
APS	Australian Public Service
AS/NZS ISO	Australian Standard/New Zealand Standard International Standard Organisation
BoE	Brief of Evidence
BRG	Business Reference Group
CJLEF	Criminal Justice Law Enforcement Forum
CO	Commonwealth Ombudsman
EIMS	Electronic investigation management system
IGIS	Inspector General of Intelligence and Security
ISM	Information Security Manual
JAA	Joint Agency Agreement
LPP	Legal professional privilege
MoU	Memorandum of Understanding
PIA	Privacy Impact Assessment
PII	Public interest immunity
PSPF	Protective Security Policy Framework
PSP	Public Services Package
RTO	Registered Training Organisation
SSO	Skills Service Organisation
SLA	Service Level Agreement
VET	Vocational and Educational Training

APPENDIX B

Reference Material

Australian Federal Police Doctrine

Australian Government Agencies Privacy Code 2017

Australian Government Information Security Manual

Australian Government Investigations Standards 2011

Australian Public Service Job Family Framework

Australian Public Service Values, Employment Principles and Code of Conduct

Joint Australian New Zealand International Standard (Organisation) 31000

Commonwealth Electoral Act 1918

Commonwealth Fraud Control Framework

Commonwealth Risk Management Policy

Evidence Act 1995

Freedom of Information Act 1982

Independent Review into the operation of the *PGPA Act 2013 and Rule*

Mutual Assistant in Criminal Matters Act 1987

Privacy Act 1988

Prosecution Policy of the Commonwealth

Protective Security Policy Framework

Public Governance, Performance and Accountability Act 2013

Public Interest Disclosure Act 2013

Safety, Rehabilitation and Compensation Act 1988

APPENDIX C

Summary Table

1. Personnel

PERSONNEL STREAM

TOPIC	SUMMARY/REFERENCES		PRINCIPLE
1.1 Professional role	• Entities recruitment documentation **should** reflect investigations roles as a professional stream. (Reference 1.1) • Entities **must** identify and assign security clearance requirements against investigator roles/positions proportionate with accessing classified information and handling of investigation material. (Reference 1.1)	• When assigning security clearance requirements, entities working in joint investigations **should** consider the security clearance requirements of another entity. (Reference 1.1)	Ethics & Professionalism
1.2 Ethics and responsibility	• Investigators and investigation decision makers **must** operate and conduct their duties with fairness, equality, consistency and professionalism, meet prosecutorial obligations and other regulatory duties for inquistorial bodies. (Reference 1.2.1) • Entities and investigators **must** conduct investigations in accordance with relevant legislation, regulations and/or statutory and independent codes. (Reference 1.2.2)	• Entities **must** have procedures in place, relevant to legislation, which appropriately deal with complaints about the handling of investigations. (Reference 1.2.2)	Ethics & Professionalism
1.3 Qualifications and learning	• A vocational and educational training (VET) qualification **must** be obtained in order to conduct investigations, unless another qualification or internal training is determined as equivalent. (Reference 1.3.1) (Cross reference 1.3.2) • Entities **must** document the required VET accredited qualification/s to conduct particular types of investigations and the timeframe in which investigators should obtain it/them. (Reference 1.3.1) • Entities **must** use an Australian Registered Training Organisation (RTO), or an Australian Government entity with Australian RTO status that meets the Australian VET standards to obtain or deliver investigation accredited qualifications. (Reference 1.3.1)	• Entities **must** ensure foundational qualifications (or equivalency) are obtained prior to supervisory qualifications. (Reference 1.3.1) (Cross reference 1.3.3) • Entities **must** determine and document qualifications, training or experience equivalent to VET accredited qualifications required for a type of investigation. (Reference 1.3.2) (Cross reference 1.3.1) • Entities **must** consider the legal risk associated with investigators, supervisors or operational decision makers without an appropriate VET accredited qualification or experience engaged in an investigation role. (Reference 1.3.3) (Cross reference 1.3.1)	Ethics & Professionalism
1.4 Competencies and mindset	• An investigator **should** have the capability to apply foundational and advanced set of related investigation knowledge, skills, and abilities. (Reference 1.4.1) (Cross reference 1.4.2) • Foundational competencies **should** be met and continue to be met against outlined . (Reference 1.4.1)	• Advanced competencies such as data analysis, surveillance and/or detainment/arrest **should** be considered as part of an entities' broader support for learning once skills, knowledge and experience are beyond foundational, unless required sooner under an entity's legislative or functional remit. (Reference 1.4.1) • An entity **should** have clear support measures for an investigator's continued skills uplift, learning and professional development (capability). (Reference 1.4.2) (Cross reference 1.4.1)	Ethics & Professionalism

APPENDIX C

Summary Table

2. Information & Evidence Management

	TOPIC	SUMMARY/REFERENCES		PRINCIPLE
INFORMATION & EVIDENCE MANAGEMENT STREAM	2. Information & Evidence Management	• Entities information management policies and practices **should** support all types of investigations as well as prevention, disruption, or inquiry outcomes. (Reference 2.0)	• An entities investigation polices and practices **must** have regard to the legislative scheme under which information is obtained to ascertain any restrictions on the use of the information and the circumstances in which the information may be disclosed. (Reference 2.0)	Own Information Management
	2.1 Disclosure Management	• Legal advice **should** be obtained by entities involved in gathering, obtaining revealing and producing material in relation to disclosure during and post an investigation. (Reference 2.1) • An investigating entity's duty of disclosure **must** be considered in initial investigation planning including the implications of disclosure. (Reference 2.1) • Investigators **must** make available material relevant to the investigation and activities **must** be recorded and retained to enable the investigative entity and prosecuting entity (both determined as the prosecution) to comply with the duty of disclosure. (Reference 2.1) • Entities **must** develop clear procedures and supporting tools to record, retain, register, review, reveal and produce investigation information. (Reference 2.1) • An entity **must** have clear procedures on the request, retention and disclosure of material held with a third party (entity). (Reference 2.1)	• Investigators or persons responsible for disclosure coordination **must** retain all records on requests or attempts to obtain material relevant to an investigation. (Reference 2.1) • Entities **should** appoint a Disclosure Coordinator in consideration of the scale, complexity and type of investigation. (Reference 2.1) • Information, material, other legal claims or other outcomes protected from disclosure **must** be managed in accordance with the law, policies, and entity legal direction (grounds for protection). (Reference 2.1.1) • The milestones and timeframes for criminal proceeding disclosure **must** be in accordance with State/Territory law, practice, and court directions to produce a Brief of Evidence (BoE). (Reference 2.1.1) • Entities **should** have procedures in place to manage disclosure in the civil and/or administrative context (Reference 2.1.2)	Own Information Management
	2.2 Information Sharing	• Entities **should** work collaboratively to detect and respond to suspected breaches occurring across the Australian Government and jurisdictional boundaries through sharing of information. (Reference 2.2)	• Sharing of information MUST be in accordance with the Privacy Act 1988 and any secrecy provisions within legislation that may govern information sharing. (Reference 2.2) • Entities **should** have procedures in place for receiving, responding, and requesting information from other entities. (Reference 2.2)	Own Information Management
	2.3 Investigation Management System	• Entities **should** have an electronic investigation management system (EIMS) to record, collate and manage investigations. (Reference 2.3) • An entity's EIMS solution **should** consider integration architecture and be interfaced or synchronised with other relevant systems. (Reference 2.3) • An EIMS solution **must** be supported by an internal or external sustainment and/or support arrangement. (Reference 2.3) • An EIMS **must** be delivered in accordance with the Australian Government Information Security Manual (ISM), Protective Security Policy Framework (PSPF), Privacy Impact Assessments (PIA), and relevant records management legislation applicable to the Australian Government. (Reference 2.3)	• Entities **should** consider PROTECTED accreditation for an EIMS as best practice for security and information management. (Reference 2.3) • An entity's EIMS **should** have the AGIS high level functional requirements. (Reference 2.3.1) • An entity's EIMS **should** include the AGIS specific capabilities. (Reference 2.3.1) • Specifications **should** be aligned with an entity's relevant information on security manual controls, including, but not limited to security profiles, user security profiles, data security profiles and application security. (Reference 2.3.1)	Own Information Management

APPENDIX C

Summary Table

3. Investigation practices

	TOPIC	SUMMARY/REFERENCES		PRINCIPLE
INVESTIGATION PRACTICES STREAM	3.1 Risk management	• Entities **should** establish an investigations Risk Management Framework and processes. (Reference 3.1) • Entities Risk Management Framework **should** be aligned with and reflect an entity's enterprise framework, standards, guidance, and policies alongside that of the Australian Government. (Reference 3.1)	• Australian Government corporate entities **should** align, and non-corporate entities **must** comply with the Commonwealth Risk Management Policy. (Reference 3.1)	Supporting the business and reputation of Government
	3.2 Investigation governance	• Entities **must** comply with the CDPP guidelines or requirements in relation to engagement and in the context of federal criminal investigations. (Reference 3.2.1) • Evidence **must** be obtained with a view to admissibility in criminal proceedings and assessment of Brief of Evidence in accordance with the Prosecution Poliy of the Commonwealth. (Reference 3.2.1) • Investigations **must** be conducted in a manner that is consistent with applicable laws. (Reference 3.2.2) • An investigator **must** be familiar with implications of relevant law on their ability to collect, manage and present evidence and investigate. (Reference 3.2.2) • Investigators **should** consider the broad spectrum of legal aspects to ensure that any action taken does not jeopardise an investigation. (Reference 3.2.2) • Differing legal requirements across various jurisdictions **should** be considered. (Reference 3.2.2) • Investigators **must** be cognisant of the impact of Legal Professional Privilege (LPP). (Reference 3.2.2) • Entities **must** have procedures and forms in place to deal with LPP during relevant types of warrants. (Reference 3.2.2) • Entity LPP procedures **must** consider options for quarantining data or documents which is the subject of a LPP claim and the timeframe an LPP claimant **should** be given to advise of the option chosen. (Reference 3.2.2) • Entities **should** have a process in place to outline who will be responsible for making entity LPP protective order applications. (Reference 3.2.2) • Entities **should** have a decision-making process in place for investigations involving options and actions that can be explained, justified, and documented. (Reference 3.2.3)	• The individual governance of an entity **should** inform the type of decision-making process chosen for investigations, noting ethical complexities. (Reference 3.2.3) • Decisions made during an investigation **should** be made by an appropriate person as determined by the entity. (Reference 3.2.3) • The recording of a decision **should** be proportionate to the seriousness and consequence of the decision. (Reference 3.2.3) • Decision documentation **must** include, at a minimum, the decision itself including the reason for the decision, person making the decision, date of the decision, information relied on to make the decision, and any expected or potential significant impact of the decision. (Reference 3.2.3) • If a decision is not able to be recorded prior to action it **should** be recorded as soon as practicable after the fact. (Reference 3.2.3) • Entities **should** establish evidence or exhibit rooms that align with security requirements under the PSPF and relevant Australian building standards. (Reference 3.2.4) • Entities' evidence and exhibit handling procedures **must** comply with applicable Australian laws of evidence, relevant case law, and Australian Government directions or guidelines on search and collection/seizure. (Reference 3.2.4) • The security and continuity of evidence **must** be maintained from seizure or collection to disposal. (Reference 3.2.4) • To maintain standards of proof investigators **should** review their case holdings (evidence) once a month in the case of high-risk exhibits. (Reference 3.2.5) • An entity **must** have a documented procedure for conducting formal audits of its Exhibits Registry. (Reference 3.2.5) • The entity **must** ensure an audit regime follows AGIS requirements. (Reference 3.2.5)	Supporting the business and reputation of Government

APPENDIX C

Summary Table

3. Investigation practices

	TOPIC	SUMMARY/REFERENCES		PRINCIPLE
INVESTIGATION PRACTICES STREAM	3.3 Investigation planning	• Investigation planning **should** consider compliance activities and processes in respect of admissible evidence collection/use. (Reference 3.3.1) • Entities **should** obtain legal advice prior to collection and/or use of information sourced as part of a compliance activity if planning to use for another type of investigation. (Reference 3.3.1) • Entities **should** have a guide outlining the use of intelligence in identifying conduct which allegedly or is suspected to be a breach. (Reference 3.3.1) • An entity **should** ensure compliance, intelligence and fraud control functions are appropriately linked to investigations. (Reference 3.3.1) • Entities **should** have reporting processes, systems and procedures in place to record the receipt of reports and transfer of reports. (Reference 3.3.2) (Cross reference IMS 2.3) • An entity **should** ensure an investigation life cycle (commencement to finanlisation) is a documented process connected to investigation policies and risk management. (Reference 3.3.2) • Entities **should** establish crtieria for when an investigation is considered to be commenced and finalised. (Reference 3.3.2)	• Entities' resourcing for investigations **should** be commensurate with the complexity and scale of an investigation and the breadth (or cross over) of the entities' function. (Reference 3.3.3) • Individual investigations **should** consider two investigators for each commenced investigation, supplemented by specialists as required. (Reference 3.3.3) • Each entity **should** conduct ongoing management and review of own investigation procedures, manuals, or instructions to ensure currency and accuracy to support capability and outcomes. (Reference 3.3.3) • The timelines for review of prodecures, manuals or instructions **should** consider the changing environment regarding legislation, technical transformation, outcomes to investigations and risk. (Reference 3.3.3) • Entities **should** develop Memoranda of Understanding (MoU), Service Level Agreements (SLA) or investigation-specific Joint Agency Agreements (JAA) to lawfully share information or conduct investigations that may cross jurisdictions or require specialist entity support. (Reference 3.3.4) • Entities **should** have written procedures regarding liaison with the media and the release of media statements regarding investigations (Reference 3.3.5)	Supporting the business and reputation of Government
	3.4 Investigation activities and tools	• Entities **must** use the Australian Government's mutual assistance regime request for the formal process of obtaining information for an investigation unless specific entity legislation allows for requests via alternate means or advice by an administering Australian authority. (Reference 3.4.1) • Entities **should** have written procedures for making informal requests to foreign authorities. Procedures **should** consider the use of Australian law-enforcement entities to assist. (Reference 3.4.1) • Entities **should** have written procedures for responding to both formal and information requests from foreign authorities. (Reference 3.4.1) • Entities **must** consult with Australian Government administrative and/or legal entities if there are capital punishment implications in requesting and responding to foreign requests. (Reference 3.4.1)	• Entities selection of an expert **should** be made following consideration of the person's standing, qualifications, publications, capabilities, and relevant experience. (Reference 3.4.2) • Entities with powers to conduct specialist services **must** have procedures in place in accordance with legislation, the Privacy Act 1988 and Australian Government security frameworks for handling information. (Reference 3.4.3) • Procedures **should** outline roles and responsibilities to conduct specialist services and all governance applied including the protection of covert methodology. (Reference 3.4.3) • Entities **must** have procedures in place to request specialist services from other entities with specialist services. (Reference 3.4.3)	Supporting the business and reputation of Government

Summary Table

4. Quality Assurance Framework

	TOPIC	SUMMARY/REFERENCES		PRINCIPLE
QUALITY ASSURANCE FRAMEWORK STREAM	**4.1** Quality assurance policy	• Entities **must** have an investigations Quality Assurance Policy in place. (Reference 4.1) • Entities **should** conduct be one formal external quality assurance activity every 2 years. (Reference 4.1)	• Entities **should** report quality assurance decisions and activities to the relevant governing entity Committees or Executive. (Reference 4.1) • A quality assurance activity for investigations **must** be done by an entity following a request by an entity's own Accountable Authority as defined under the PGPA Act 2013or established relevant governing entity Committee. (Reference 4.1)	Continuous Cylce of Review
	4.2 Quality reviews and audit	• During the planning of any investigation informal review **should** be considered and appropriately incorporated in an investigation plan. (Reference 4.2.1) • An audit **must** have a set measure with which to determine compliance. (Reference 4.2.2) • An audit **should** take place once an investigation has concluded, however, if the audit is theme or activity based that will not jeopardise the investigation it can be done during an investigation. (Reference 4.2.2) • Review material produced **should** be done with due consideration to quality, and **should** be appropriately security classified. (Reference 4.2.3)	• Where necessary, material which could be subject to a claim of PII or LPP **must** be identified. (Reference 4.2.3) • A formal review or audit **must** be an independent and objective assessment of the quality of various investigative practices and procedures. (Reference 4.2.4) • Investigators **must** only assist to provide information relevant to a formal review or audit if a case officer of the investigation being reviewed or audited. (Reference 4.2.4)	Continuous Cylce of Review
	4.3 Scope for quality activities	• Entities quality acitivity scope **should** identify performance measures as outlined in AGIS. (Reference 4.3) • An entity **should** consult with a prosecuting authority regarding the scope of a quality activity (Reference 4.3)	• An entity **must** consider AGIS when considering the scope for quality assurance. (Reference 4.3) • Own entity policy, doctrine, standards, and better practice guides **should** be evaluated and determined for use during a quality activity. (Reference 4.3)	Continuous Cylce of Review
	4.4 Quality reports and outcomes	• For formal internal or formal external quality activities, entities **should** request opportunity to comment on the draft of a review report and comments **should** be incorporated into a final quality review report. (Reference 4.4) • Finalised reports **should** be provided to the person in control of an entity, relevant governing entity Committee or delegated position. (Reference 4.4)	• Results of a quality activity **should** be provided by the entity (relative to information and risk management) to other relevant entities to continue to improve investigative quality across the Australian Government. (Reference 4.4) • An entity involved in a review of another entity **must** seek express authority prior to publishing a report on behalf of the owning entity, unless the entity has authority without agreement. (Reference 4.4)	Continuous Cylce of Review

Australian Government

Australian Government Investigations Standard

October 2022