Australian Government
Australian Transport Safety Bureau

Records and Information Management Framework

The guide provides the framework for information and records management in the Australian Transport Safety Bureau

Version: 3.0
Issued: November 2022
Status: Final
Owner: Manager, ICT/Business Services

Version History

Version	Date of issue	Description of change	Page no.
0.1	April 2017	First release for review.	
0.2	December 2017	ATSB updates incorporated	
1.00	June 2018	Final approved version	
2.00	October 2020	ATSB organisational updates and new hyperlinks incorporated	
3.00	November 2022	Formatting, hyperlinks and ATSB updates incorporated	

CONTENTS

RECORDS AND INFORMATION MANAGEMENT FRAMEWORK

Title: Information and Records Management Framework

Effective Date: June 2018

BACKGROUND TO THE FRAMEWORK

Purpose

This Framework is a high-level statement outlining the Australian Transport Safety Bureau's (the ATSB's) vision for its information and records management.

The Framework is based on the principles and approaches recommended by the National Archives of Australia (NAA)[1] for use by Australian Government agencies.

Definitions

Accountable Authority is a term defined by the PGPA Act and means the Secretary.

BCS is the Business Classification Scheme

COO is the Chief Operating Officer

ED is the Executive Director

FOI is Freedom of Information

ICAO is the International Civil Aviation Organization

ISM is the Australian Government Information Security Manual

ISO 16175 is the *Australian Standard for Information and Documentation – Principles and functional requirements for records in electronic office environments*

NAA is the National Archives of Australia.

PGPA Act is the *Public Governance, Performance and Accountability Act 2013*

RA is the Records Authority

RCS is the Records Classification Scheme

[1] See https://www.naa.gov.au/information-management/information-governance (accessed October 2020)

Instructions

This framework must be referred to when developing business plans, policies and procedures relating to the management if information.

The Framework is the authoritative source of governing rules and principles for information and records management in the ATSB.

Framework Scope

This Framework encompasses electronic and physical records of business, in all ATSB repositories including its network drives, email systems and applications. All information created, sent and received in the course of conducting ATSB business is potentially a record.

The Framework applies to all ATSB staff, contractors and external parties working within ATSB systems.

The Framework encompasses the four major parts of the Australian government records management lifecycle (as defined by the NAA[2]):

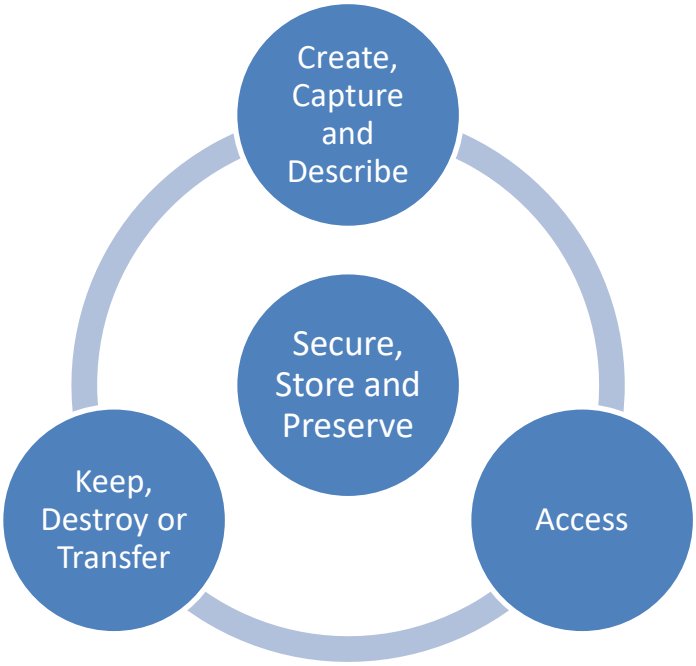

Figure 1 – Records Management Lifecycle

- **Create, Capture and Describe**: including when ATSB staff need to make a record, where to put it and how it should be described (including metadata standards).
- **Access**: ensuring ATSB records are findable and readable for as long as they are required.

[2] *Check-up Survey: a survey designed to collect data on your agency's information and records management capabilities and behaviours* https://www.naa.gov.au/information-management/check-survey (accessed November 2022)

- **Keep, Destroy or Transfer**: including how long ATSB will keep records, and how we will destroy or transfer them when they are no longer required.
- **Secure, Store and Preserve**: how the ATSB will secure, store and preserve its records, both physical and digital, throughout the entire records management lifecycle.

Framework Purpose

This Framework guides the creation, use and management of ATSB's information and records assets. The ATSB is committed to the principles set out in this document.

The Framework supports robust decision-making, risk management and compliance with external requirements. Failure to properly create, describe, capture and manage information and records exposes the organisation to increased risks. Conversely, tangible benefits flow from sound information and records management practices. The benefits include:

- avoiding the need to continually re-create corporate knowledge
- improved service delivery
- reducing staff time and effort required to locate and access relevant, complete information
- quicker and more accurate response to government demands and requests for information
- lower costs of compliance with freedom of information requests and other legal discovery
- protection of citizen rights
- mitigation of risks to our reputation that might arise from media or audit criticism of poor information and records management practices or non-compliance with legislative and regulatory obligations.

This Framework will be used to support the ATSB's *Information and Records Management Strategy*. The framework should also support achievement of a score of 4 or 5 in the following sections of Check-up Survey:

- 1.2: My agency's information governance framework is digital-ready
- 1.3 Senior management supports digital information management as a priority[3]

The Framework includes:

- Environmental context: this lists the legislation, policies and other factors which influence our information and records management planning, practices and activities
- Key directives: this lists our principles, key priorities, control systems, and the implementation approach for these directives
- Application: this shows how the Framework will be applied in the organisation.

[3] https://www.naa.gov.au/information-management/check-survey (accessed November 2022)

ENVIRONMENTAL CONTEXT FOR RECORDS AND INFORMATION MANAGEMENT

This section details the internal and external environmental factors influencing the information and records management approach in the ATSB.

Public Accountability for Information and Records

The *ATSB Corporate Plan 2022-23*[4] includes the goals, strategies and key activities the ATSB has committed to government to achieve. The following tables show the information impacts of each strategic goal.

Primary outcome – *Improved transport safety in Australia including through: independent 'no blame' investigation of transport accidents and other safety occurrences; safety data recording, analysis and research; and influencing safety action.*

Strategy	Information Impacts
Attracting, developing and retaining staff from diverse backgrounds. Delivering those investigations of accidents and safety occurrences that have the greatest potential to deliver improved transport safety outcomes, with a particular focus on the safety of the travelling public	Information and records management capabilities must be incorporated into staff training, development and performance agreements
A greater focus on how we engage with our stakeholders with enhanced use of digital mediums which we know amplifies our safety messaging. particular focus on ensuring a strong culture of reporting safety matters through transparent arrangements for the appropriate reporting, sharing and use of safety information	Personnel must be able to effectively share information with others in the organisation who have a need to know
Deliver a program of safety research and analysis that draws on the results of investigations and safety occurrence datasets	The organisation must be able to leverage its data sets to create useful information
Undertake safety communication and education with an emphasis on identified priority areas where safety risk can be reduced	Personnel must be able to effectively share information with others outside the organisation who have a need to know

[4] https://www.atsb.gov.au/sites/default/files/media/5781849/atsb-corporate-plan-2022-23.pdf (accessed November 2022)

Strategy	Information Impacts
Engage with and, as appropriate, provide support to regional and international partners, focusing on developing cooperation in our region and on ensuring that safety lessons and operational innovations are shared internationally	
Continue the transition to being the national rail safety investigator, as established through the Council of Australian Governments' Intergovernmental Agreement on Rail Safety Regulation and Investigation Reform	ATSB information and records management practices must align with the expectations of our industry and government partners to support our joint missions

ATSB Information Directives and Objectives

The ATSB compliance environment as pertains to information and records management includes the following sources of accountability:

Legislation

The ATSB complies with the following laws that relate to information and records: *Archives Act 1983, Electronic Transactions Act 1999, Evidence Act 1995, Australian Information Commissioner Act 2010, The Public Governance, Performance and Accountability Act 2013, Freedom of Information Act 1982, Privacy Act 1988, Public Service Act 1999* and the *Crimes Act 1914.*

The ATSB also has special provisions under the following Acts:

- Transport Safety Investigation Act 2003
- Air Navigation Act 1920
- Navigation Act 2012
- Civil Aviation Act 1988

The Acts are supported by the following regulations:

- Transport Safety Investigation Regulations 2003
- Civil Aviation Regulations 1988
- Transport Safety Investigation (Voluntary and Confidential Reporting Scheme) Regulation 2012

See the Appendix for the impacts of these instruments on ATSB information and records management policy and practices.

Standards and Best Practices

The ATSB will work towards compliance, as necessary, with the requirements of the *Australian Standard on Records Management (AS ISO 15489); Australian Government Recordkeeping Metadata Standard (AGRkMS); National Archives of Australia Standard for the Physical Storage of Commonwealth Records* and the *Australian Standard for Information and Documentation – Principles and functional requirements for records in electronic office environments (AS ISO 16175).*

Whole-of-government requirements

The ATSB is subject to the *Australian Government Information Security Manual (ISM)* and the *Australian Government Protective Security Policy Framework (PSPF).*

The ATSB will comply with whole-of-government policies and directives that are relevant to the management of agency information and records including, but not limited to, the *Digital Transition Policy (National Archives of Australia), Principles on open public sector information* and the *Information Publication Scheme* (Office of the Australian Information Commissioner), and other relevant and current ICT policies.

In support of the whole-of-government Web 2.0 direction, the ATSB will work towards a fully digital, accessible collaboration-focused information and records management environment.

Internal policies and procedures

The ATSB will develop information and records management practices and systems with appropriate evidential characteristics to enable us to demonstrate compliance with these legislative obligations. ATSB information and records management processes and systems will comply with the internal *Secure ICT Policy*, which is the source of authority for all ATSB information security principles, and other internal relevant policy controls.

The ATSB's *Information and Records Management Strategy* will describe our endorsed planned approach and priorities to meet information and records management requirements now and in the future, with a focus on continual improvement.

The ATSB's *Information and Records Management Policy* will provide guidance to staff on creating and managing agency information and records. It will identify responsibilities for all staff and additional responsibilities for certain staff.

The Policy will overarch a set of

- Procedures (for activities defined by the Policy)
- Operational Guidelines (recommended practices for ensuring procedural compliance)
- Assistive Tools (forms, templates, worksheets and references for improving efficiency and consistency in records and information management activities)

ATSB Records Management Environment

The ATSB records management environment includes its business context, business processes, roles and responsibilities, information assets, key systems, organisational culture, and the expectations of its external clients and stakeholders.

Business context

The Australian Transport Safety Bureau (ATSB) is an independent Commonwealth Government statutory Agency. The ATSB is governed by a Commission and is entirely separate from transport regulators, policy makers and service providers.

The ATSB's function is to improve safety and public confidence in the aviation, marine and rail modes of transport through excellence in:

- independent investigation of transport accidents and other safety occurrences;
- safety data recording, analysis and research; and
- fostering safety awareness, knowledge and action

The ATSB is established by the *Transport Safety Investigation Act 2003* (TSI Act) and conducts its investigations in accordance with the provisions of the Act. A comprehensive regime of provisions within the *TSI Act* is in place to maintain the confidentiality of, and legal protection for, a range of sensitive safety information obtained by ATSB investigators[5].

Key business processes

There are three core functions which arise from the ATSB's functions under the Transport Safety Investigation Act 2003:

1. **Independent investigation of transport accidents and other safety occurrences**
   Independent investigations result in formal reports, records of evidence, correspondence and other supporting records.

2. **Safety data recording, analysis and research**
   Recording, analysis and research captures large amounts of data, and generates useful information based on interpretation.

3. **Fostering safety awareness, knowledge and action**
   This function results in records which are shared externally, including consultation, education, and promulgation of research and investigation findings and recommendations.

ATSB support these core business functions with a range of administrative functions, all of which result in the creation, capture and use of important business records.

Roles and responsibilities

[5] http://www.atsb.gov.au/about_atsb/overview/ (accessed October 2020)

The ATSB organisation is structured around four core streams. Accountability for information and records management governance is primarily assigned to the Strategic Capability stream – however, each of the other three streams are responsible for effectively managing the records and information the create and capture.

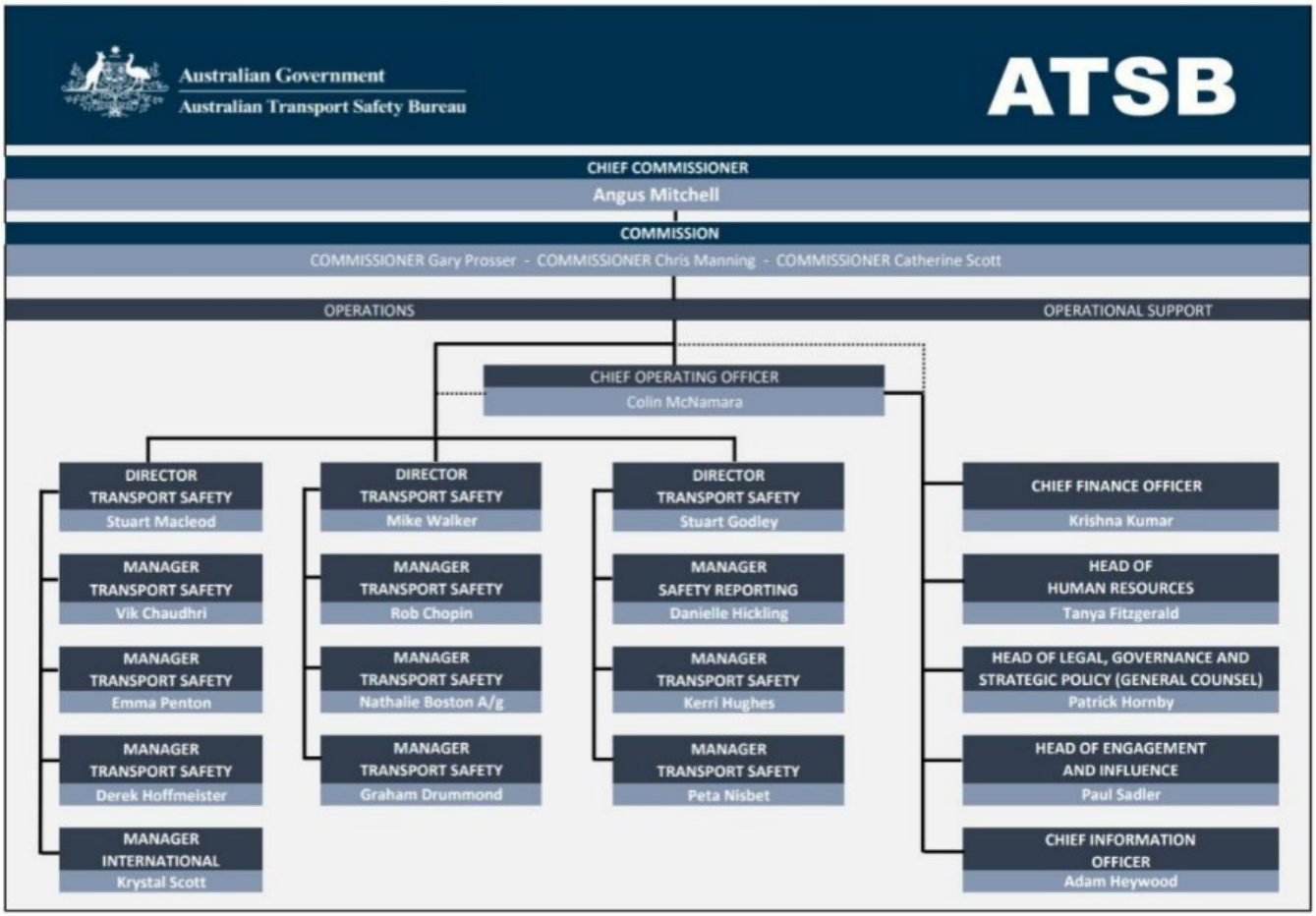

Figure 2 – ATSB Organisation Structure as at November 2022.

Information Assets

Records captured include both **unstructured** data:

- Microsoft Office documents
- PDF documents
- Emails (including attachments) to and from the @ATSB.gov.au domain
- Images, video and audio media
- Paper records (scanned and original)

And **structured** data:

- Proprietary application databases
- Proprietary content databases

The high level classification structure currently used for managing information includes repositories for both structured and unstructured data. Each function-based team in ATSB relies on different repositories to manage content produced by or for its various business activities.

Key Systems

ATSB uses several administrative and core business systems to support its functions. Some key systems include:

- Dynamics Great Plains – used for financial management
- AIMS – used for core business data
- Aurion – used for human resources management
- MS Teams /Cloud Records – used for the management of paper files
- MS Teams/Cloud Records Software – used for the management of electronic records
- Umbraco – used for web content management

HP TRIM is currently the only formal records management system in the ATSB.

Clients and stakeholders

The ATSB is a member of key safety bodies which include: the International Transportation Safety Association (ITSA); International Society of Air Safety Investigators (ISASI); Flight Safety Foundation (FSF); and the Marine Accident Investigators' International Forum (MAIIF).

Australia is a member of the Council of the International Civil Aviation Organization (ICAO), which is made up of 190 countries. The ATSB has frequently assisted with international investigations, including through the analysis of flight-recorder ('black box') data.

Australia is also a council member of the International Maritime Organization (IMO), and actively participates in its forums on accident investigations in the interests of making global improvements to shipping safety[6].

Each of these bodies rely on ATSB to make and keep accurate, useful and reliable records, and to manage those records securely, for as long as they are required. ATSB must be able to collaborate with these bodies on appropriate records.

[6] http://www.atsb.gov.au/about_atsb/overview/ (accessed October 2020)

KEY DIRECTIVES OF THE FRAMEWORK

To support the expectations of the ATSB records and information management environment, the Framework lists the following rules.

ATSB Information Principles

The following principles should be considered during the design, implementation and management of all ATSB core business process and systems. These principles will be published to staff for reference as needed in the course of conducting their work.

No.	Principle	Description
IMP1	Access to information	By default, all ATSB information is accessible by all staff. Restriction is by exception only. ATSB information is shared with our industry and government partners wherever appropriate. Additionally, some information held by the ATSB is a valuable national resource. If there is no need to restrict this information, it will be made available for public access.
IMP2	Single source of truth	Information is stored in one authoritative location, and linked to, rather than duplicated, where required. The digital version of a record is the primary one. Records in use by the business will either be 'born digital' or converted to digital format unless there is a clear need to keep them in physical formats.
IMP3	Whole of life control of information assets	Information assets are managed in accordance with their value. Information is formally managed throughout its whole lifecycle, from creation/capture to eventual disposition. Information is only disposed of in accordance with Records Authorities, through the records management team. Records are sentenced on creation wherever possible. Information assets are tracked in registers and other inventories, and all assets have a formal owner.
IMP4	Cross platform management	Information in all business systems is formally managed, either by integration with the EDRMS or within its system of record. Information is interoperable between key systems, both those within ATSB and those of its government partners. Data sets will be related, compared and integrated wherever this can provide useful analysis and information.

No.	Principle	Description
IMP5	Transparency in information governance	ATSB decision making about information creation, publication and disposition is transparent. Processes for information and records management are clearly documented, and any significant actions taken on information assets are recorded and reported. Accountability is clearly documented, and all levels of staff are aware of their responsibilities for effective information governance.
IMP6	Information security	Information assets are managed in accordance with their risk. Information with privacy, security, commercial or other restrictions is effectively protected from unauthorised access, use, loss and disclosure.

Table 1 – ATSB Information Principles

The ATSB must also abide by the whole-of-government *Digital preservation Policy.*

See the Appendix for details of other relevant whole-of-government architecture and information principles.

ATSB Key Priorities for Information and Records Management Professionals.

Our People

As part of DC2020, the National Archives introduced interim pathway targets to support information practitioner's development.

Professionalism targets under DC2020 reinforce the need for qualified and skilled information and data professionals and an accountable and business-focused information and data management environment. The NAA provides information management and data capabilities to guide employees and the government agencies through the skills and knowledge they need to manage information and data to meet business and accountability requirements.

Our Culture

ATSB will formalise the governance of information and records management at the executive level, by ensuring it is managed at the highest levels of the organisation will help ATSB be accountable to our clients and stakeholders, and effective in our work. Executive level engagement will provide a positive model to the wider organisation about the importance of information and records management, and will help ensure that key strategic decisions take information and recordkeeping requirements into account.

Our systems

The *Digital Transition Policy* requires ATSB to achieve the following control objective for systems:

- **Manage digital information wherever it is held**: When acquiring business systems consider how the records will be managed for as long as they are needed. Give preference to those systems that effectively support records management and comply with the international standard ISO 16175 Principles and Functional Requirements for Records in Electronic Office Environments

The *Digital Continuity 2020 Policy*, as part of its 'Governance and People' Principle 3 (Information is valued), sets specific control objectives for meeting this requirement, including:

- **31 December 2016**: Business systems procured after this date will be evaluated against the Archives' business systems assessment framework to meet functional requirements for information management.
- **31 December 2018**: [All] business systems are evaluated against the Archives' business systems assessment framework to meet functional requirements for information management; Functional requirements are implemented where required.
- **31 December 2020**: Business systems meet functional requirements for information management.

To meet these expectations, ATSB will evaluate all new and existing key business systems against the requirements of ISO 16175:3, with a view to ensuring they incorporate:

- classification and sentencing capabilities
- deletion and disposition controls
- import and export controls
- metadata controls

To support this initiative, ATSB will develop an Information Architecture, including a change control mechanism, which maps all of our key information assets and the systems that store them. System documentation controls will be updated to ensure information and records management controls are captured.

ATSB Records Management Control Systems

Successful implementation of a compliant records management environment for the ATSB will involve a combination of governance and technical controls.

The ATSB will apply three major sets of controls for managing records:

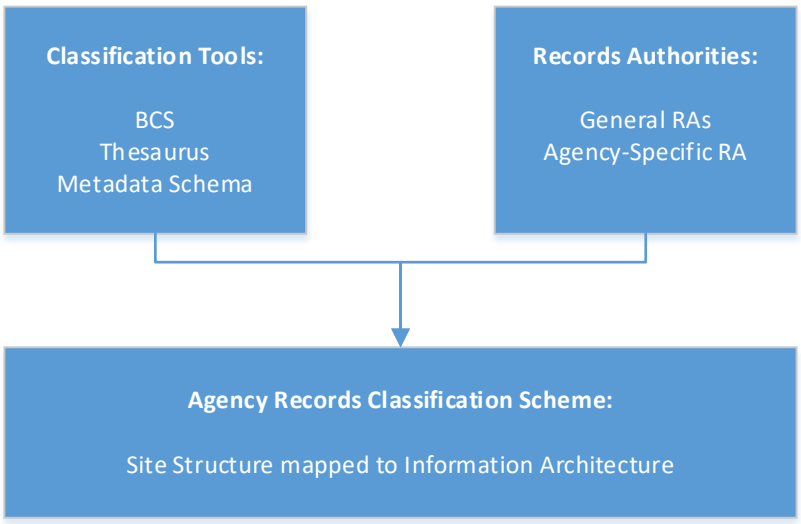

Figure 3 – Records Control Framework

Classification Tools

Classification tools identify agreed terms for describing records in a consistent and meaningful way. Records that are well described are easier to find, manage, use and understand. The classification tools used by the ATSB include a Business Classification Scheme (BCS), functions thesaurus, and set of minimum metadata to be applied to records.

Records Authorities

Records authorities enable agency records management staff to work out how long records need to be retained, and when a record will be due for destruction or transfer to the National Archives.

There are two types of records authorities applicable to ATSB. These are:

- agency-specific records authorities – covering the records created in the course of ATSB's core business, which are unique to ATSB, and provided on behalf of its clients
- general records authorities – covering administrative records common to many agencies, which are not unique to ATSB, and developed in support of its core business

The current applicable Agency-Specific Records Authorities are:

Current agency	Core business	Date issued	Authority number
Australian Transport Safety Bureau (ATSB)	International Relations; Safety Education, Communication and Awareness; Safety Investigation and Research; Safety Notification, Assessment and Recording (This Authority replaces the following classes in Records Disposal Authority 2004/00616220 issued to the Department of Transport and Regional Services in 2005: 9573-9574, 9609 and 9612. These classes have been superseded and cannot be used after the date of issue of this Authority)	17 Jun 2013	2013/00246960
Infrastructure and Regional Development, Department of	Regional services development and local government; Territory policy and development; Transport environment management; Transport infrastructure development; Transport safety; Transport services and regulations	15 Mar 2005	2004/00616220

The applicable General Records Authorities are listed on the National Archives of Australia website[7].

Note that the ATSB governing Acts and Regulations also include provisions relating to record retention and disposition.

Agency Records Classification Scheme

The Records Classification Scheme (RCS) is used to map the relationship between the classification tools, Records Authorities and the information architecture (or structure) of ATSB information systems. The RCS will be implemented as a technological control system into applications where possible. It will also be maintained as a document.

[7] http://www.naa.gov.au/information-management/records-authorities/types-of-records-authorities/GRA/index.aspx (accessed April 2017)

ATSB Framework Implementation Approach

Information and records management accountability

All ATSB employees, contractors and consultants have a responsibility to properly manage the information they create, send or receive as part of their job. This information is a record and must be kept in an approved location to ensure it remains accessible and usable over time.

ATSB managers and executives have a responsibility to ensure that the handling of information by their teams is accountable and in accordance with relevant legislation as described in this Framework.

ATSB specialist records managers are responsible for disposition or destruction of information at the end of its lifespan. No deletion or other destruction of records is permitted without their approval.

Any individual, team or project making decisions about the way in which information will be created, captured, shared, stored, protected or disposed of must do so with due consideration to the Framework and the principles and policies within.

The following roles have responsibility for the management of key ATSB information assets:

Asset Type	Accountability
Transport Safety Investigation information	Director/s, Operations
Financial information	Chief Operating Officer
Human Resources and organisational information	Chief Operating Officer
ICT information	Chief Operating Officer
Legal information	Chief Operating Officer
Reporting and Research information	Chief Operating Officer
Business Services information	Chief Operating Officer
Technical Analysis information	Director/s, Operations

Strategy and planning

Information governance must be a key consideration in all strategic planning activities.

> "*Information governance is an approach to managing information assets across an entire organisation to support its business outcomes. It involves having frameworks, policies, processes, standards, roles and controls in place to meet regulatory, legal, risk and operational requirements. Information governance is an essential element of corporate governance that must be aligned with business outcomes and risks*"[8].

ATSB information governance will be aligned with other strategic governance in the following ways:

Governance Domain	Information Governance Relationship
Compliance	The ATSB must demonstrate ongoing compliance in all its activities with its governing laws, regulations and policies. Reference to this Framework as a part of all audit and assurance activities will help ensure that compliance obligations are and continue to be met.
Financial and Fraud	Effective financial control requires effective recordkeeping, as well as access to accurate, timely and complete data sets. Financial processes, policies and systems must be designed and managed in accordance with the requirements of the Information Management policy.
Quality	Successful delivery of key ATSB outcomes relies on access to trusted, comprehensive and authoritative information. Information governance will help ensure the information holdings of the ATSB can be used to support better data driven decision-making, business intelligence and evidence based reporting. Corporate business plans must refer to the Information Management framework, strategy and policy to ensure best value can be realised from ATSB records.
Risk	Control of information quality and security will help reduce enterprise risk. Corporate, team and project risk plans must refer to the Information Management Strategy for the high level information and records management risks that may affect the business.
Workforce Planning	The effectiveness and efficiency of the ATSB workforce depends on the appropriate skills, experiences and capabilities of its staff. The capability

[8] http://www.naa.gov.au/information-management/information-governance/index.aspx (accessed April 2017).

Governance Domain	Information Governance Relationship
	matrix in the Information Management Strategy should be referred to when planning staff roles, responsibilities and remuneration.
Security and Business Continuity	Information security, alongside physical and personnel security, is an increasingly important governance domain. Any existing or future information process, system or policy must be designed and implemented in accordance with the information security requirements referred to in this Framework.

Reporting and compliance

ATSB must report on its information and records management requirements in the following way:

Report	Description	Timeframe
Audits	Australian National Audit Office, International Civil Aviation Organization (ICAO) and internal Audit Committee, as well as other key bodies	As required
Check-up Digital	Report to the National Archives on the status of digital records management in the organisation	Annual
Freedom of Information	Information Publication Scheme[9] FOI log	Ongoing
Senate Order of Continuing Effect	Indexed list of all files relating to policy advice, development of legislation and other matters of public administration – tabling before parliament	6 monthly
Internal Reports	Digital Continuity Plan reviews	2017; 2018; 2019; 2020
System Certification	ATSB systems holding Unclassified: DLM or classified records must be assessed for compliance with the Information Security Manual (ISM) when they are implemented or changed	As required

[9] https://www.oaic.gov.au/about-us/access-our-information/our-information-publication-scheme/ (accessed April 2017)

Infrastructure

Key infrastructure to support information assets, and the mechanisms that must be in place for its ongoing management, includes:

Infrastructure	Control Mechanisms
Hardware	ATSB hardware is managed in a hybrid model, with some assets managed in house and some supplied by cloud services providers. Hardware must be managed to ensure availability of information in the event of a disaster.
Networks	ATSB local and hosted networks must be secured in accordance with the requirements of the ISM to protect information availability, confidentiality and integrity.
Software	Various core and administrative business software is used by the ATSB to manage information. Software must be upgraded, patched and managed in accordance with best practices to ensure ongoing availability and effective security. Systems must support the minimum requirements of ISO16175 for records management.
Storage	ATSB network and physical storage must be secure, available and controlled to ensure records integrity. Auditing, backups and access controls must be applied and monitored regularly.

APPLICATION OF THE ATSB RECORDS MANAGEMENT FRAMEWORK

To ensure the Framework is understood, applied and maintained, the following controls are in place.

Promotion of the Framework

The use of this Framework is recommended for all ATSB staff (this includes permanent, casual, part-time staff and contractors) and external personnel who create or manage ATSB business information. In particular, staff improving or introducing business processes or systems must cross reference the principles of the Framework in their design and governance documentation.

All staff will be formally advised whenever changes are made to the Framework. The Framework will be available to all staff via corporate knowledge management systems.

Review intervals for the Framework

This Framework must be accepted and signed off by the Chief Operating Officer.

Any exceptions to this Framework must be approved by the ATSB Chief Commissioner in writing.

This Framework should be reviewed on an annual basis, or whenever major procedural changes occur.

Senior management endorsement

This Framework is issued under the authority of the Chief Commissioner and will be reviewed and amended regularly. Ownership of the Framework rests with the Chief Operating Officer who has the delegation to take a strategic role in implementing and reviewing the framework to ensure compliance with legislative requirements and Whole of Australian Government information and recordkeeping standards.

Authorisation

Reviewed by: _____ ATSB Records Manager

Authorised and approved by: _____ ATSB Senior Executive

APPENDICES

Whole of Government Information Principles

The following Digital Service Standard principles are supplied by the Digital Transformation Agency (DTA). The Standard is intended to apply to external facing client services, but its principles can be applied to the ATSB internal systems as a best-practice guideline.

ID	Principle	Rationale
1	**Understand user needs**	You need to understand the people who use your service (your users) and what they want to do (their user needs) in order to build a service that works for them.
2	**Have a multidisciplinary team**	Good government services are built quickly and iteratively, based on user needs. Your digital delivery team must be set up in the right way to do this
3	**Agile and user-centered process**	Designing services in a user-centered way means that the services you deliver will be easy to use and convenient for the people who need to use them, helping them to stay in the digital channel. Designing using agile methods allows you to be more proactive and respond easily to change, both in technology and government policy. Services should be improved frequently; they will be cheaper and more accountable to users.
4	**Understand tools and systems**	The technology you choose to build your service must help you respond quickly and regularly to the needs and expectations of users
5	**Make it secure**	If a service cannot guarantee confidentiality, integrity and availability of the system, people will not use it
6	**Consistent and responsive design**	Using responsive design, following common design patterns and style guidance for digital content, and making sure the service is accessible means it will be simpler, clearer and faster for all users

ID	Principle	Rationale
7	**Use open standards and common platforms**	Using open standards and common government platforms helps you to: • meet the needs of your users by building with proven solutions • make users' experience of government more consistent, which generates trust • save time and money by reusing things that are already available • be more efficient by sharing data appropriately • move between different technologies when you need to, avoiding vendor lock-in
8	**Make source code open**	It's important to share your source code so others with a similar need can reuse it.
9	**Make it accessible**	You need to make sure everyone who needs your service can use it. This includes people with disabilities and older people, and people who can't use, or struggle with, digital services. Your service must be accessible to users regardless of their digital confidence and access to a digital environment. This includes users in remote areas and users' different devices.
10	**Test the service**	All government services should be clear, simple and easy to use, regardless of the technology your users use, their expertise with the subject matter, or their level of digital skill. You cannot wait until the service is live to discover problems that stop people from using the service.
11	**Measure performance**	By identifying and capturing the right metrics - with the right tools - you can make sure all your decisions to improve the service are supported by data
12	**Don't forget the non-digital experience**	We need to make sure users' transitions between non-digital and digital channels, when they need to happen, are as smooth as possible

ID	Principle	Rationale
13	**Encourage everyone to use the digital service**	We still need to help users who are unable to use digital channels and provide support to those who need it. But we want to ensure digital channels are used whenever possible and to scale back, or phase out, alternative channels when we can

The following principles are part of the Digital Continuity 2020 Policy.

ID	Principle	Description
1	**Information is valued**	Information is a strategic asset that must be created, stored and managed
2	**Information is managed digitally**	By 2020 all information generated as agency business will be created and managed digitally
3	**Information is interoperable**	Interoperable information, systems and processes reduce unnecessary duplication and the impact of structural changes in government

The following Australian Government Architecture principles are supplied by the Department of Finance (ex Australian Government Information Management Office) to support the architecture and design of cross-agency services. The principles can be applied to this implementation as best-practice guideline, modified to relate to intra-agency solutions.

ID	Principle	Rationale
1	**Defined by business needs**	The business requirements define the service and the service defines any required technology support. A service will support the consumer to efficiently carry out their business, without unnecessarily and adversely affecting their business processes
2	**Trusted Service**	The consumer shall be provided with sufficient evidence to allow them to decide to trust that information provided by services is accurate and consistently reliable. The information which is provided by consumers to services will be managed such that it is safe and secure

ID	Principle	Rationale
3	**Present a consistent face of government**	A service will appear to the consumer with a consistent look and feel. In using a service, a consumer will not need to know by whom a service is provided. A cross-agency service will manage other services to ensure that the consumer receives a complete and consistent service
4	**Channel Independence**	All services shall be designed and built to be channel independent. In particular, citizens will be able to use their choice of available channels, depending on their preferences and circumstances
5	**Defined Availability**	The availability of a service will be clearly defined and published, recognising the increasing demand for services to be provided outside of traditional office hours, integrated into composite services and delivered through multiple channels
6	**Consistent Delivery**	A service will be designed and implemented such that it will be available to consumers for the term of the service requirement. Consumers should be largely unaware of changes to ownership of the service or underlying technology changes that can be expected to occur over the life of a service
7	**Protect the security, confidentiality and privacy of information**	A service will protect the privacy and information security of citizens, businesses and community and other organisations. Consumers can provide information to cross-agency services with the certainty that the information will be used in accordance with privacy legislation
8	**Return a Business Benefit**	A cross-agency service must be founded on a full analysis of costs and benefits, tangible and intangible, real and imputed, capital and recurrent, from a cross-agency perspective
9	**Able to adapt for change and growth**	As the priorities and requirements of the government and consumers change, services will be capable of evolving and adapting to meet changing functionality and capacity needs whilst minimising the risk and impact of change to the service
10	**Certainty of Outcome**	Consumers will be able to depend on a service to consistently deliver expected outcomes. Consumers will also receive sufficient and timely feedback from a service to understand the progress of their transactions. Failure of part or all of a service will be managed and recovered by the service, with appropriate communication to consumers to maintain user confidence and trust

ID	Principle	Rationale
11	**Manageable and Traceable**	Services must be manageable and traceable, both as a service and at the transaction level. Service Stewards will be able to monitor and manage the performance and quality of their services, end-to-end

Table 2 – AGA Principles

Relevant statements from governing Acts and Regulations

The following tables list statements from ATSB legislation that relate to information and records management.

Act	Statement summary
Transport Safety Investigation Act 2003 Section 25	**Reports** ATSB must publish reports as soon as possible after investigations are completed
Transport Safety Investigation Act 2003 Section 26	**Draft reports** ATSB may provide draft reports to anyone, but they must not copy or disclose any part of those reports without proper authorisation.
Transport Safety Investigation Act 2003 Section 45	**Retention, testing etc. of evidential material** The ATSB may take material as evidence and make copies of it, but needs to provide receipts for it. At the end of the investigation, evidence must be returned. If this is not possible, it can be destroyed.
Transport Safety Investigation Act 2003 Section 52	**ATSB may authorise persons to have access to OBR information** ATSB may authorise external persons to have access to otherwise restricted on board recording materials.
Transport Safety Investigation Act 2003 Section 53	**Copying or disclosing OBR information** It is an offence to copy or disclose on board recording information without proper authority.
Transport Safety Investigation Act 2003 Section 60	**Limitations on disclosure etc. of restricted information** It is an offence to make a record of or disclose restricted information without proper authority.

Act	Statement summary
Transport Safety Investigation Act 2003 Section 61	**Release of restricted information in the interests of transport safety** The ATSB may disclose restricted information to any person if the ATSB considers that the disclosure is necessary or desirable for the purposes of transport safety. However, the ATSB may only disclose restricted information that is, or that contains, personal information in the circumstances prescribed by the regulations.
Transport Safety Investigation Act 2003 Section 62	**ATSB may authorise persons to have access to restricted information** The ATSB may authorise a non-staff member to have access to restricted information if the ATSB considers that it is necessary or desirable to do so.
Transport Safety Investigation Regulations 2003 Regulation 5.4A	**Written reports** The following types of written reports are prescribed: (a) post; (b) facsimile; (c) email; (d) electronic lodgement using the Internet.
Navigation Act 2012 Section 281	If an inspector seizes a document, they must provide a copy of the document where allowed under the Act
Navigation Act 2012 Section 282	An inspector must provide a receipt for any seized document or item
Navigation Act 2012 Section 285	Seized items must be returned if possible. If they cannot be returned, they can be disposed of by the inspector.
Navigation Act 2012 Section 311	Logbooks must be kept for at least 5 years after being removed from a vessel.
Civil Aviation Act 1988 Section 32AP	It is an offence to copy or disclose cockpit voice recording information without proper authority
Civil Aviation Act 1988 Section 32AHM	An inspector must provide a receipt for any seized document or item

Act	Statement summary
Civil Aviation Act 1988 Section 32AHN	Seized items must be returned if possible. If they cannot be returned, they can be disposed of by the inspector under a Section 32AL.
Transport Safety Investigation (Voluntary and Confidential Reporting Scheme) Regulation 2012 Section 11	Reports not given in writing must be transcribed by the ATSB. Minimum contents are listed in the Regulation Section 12.
Transport Safety Investigation (Voluntary and Confidential Reporting Scheme) Regulation 2012 Section 14	Once the ATSB has copied report information into its database, it must return the original report to the originator, and/or destroy it. Restricted personal information cannot be added to the database unless justification exists, and if it is captured, must be removed when no longer required.
Transport Safety Investigation (Voluntary and Confidential Reporting Scheme) Regulation 2012 Section 15	If a report is suspected to contain false or misleading information, it must not be returned to the originator or destroyed for at least 2 years, or, if a prosecution is commenced until it is no longer required for that purpose.
Transport Safety Investigation (Voluntary and Confidential Reporting Scheme) Regulation 2012 Section 16	ATSB must not disclose personal information unless authorised by this part. See also Section 20.

Procedures/References

Resource Management Guide No. 418, Payment Terms for Australian Government Travel Arrangements – Card Services

For any questions about this practical guide, contact: Manager, ICT/Business Services Approved by: Chief Commissioner

Under Section 20A of the *Public Governance, Performance and Accountability Act 2013*