RESERVE BANK OF AUSTRALIA

Metadata Management Guideline

June 2022

Version Control

Version	2
Date	16 June 2022
Document Approver	Data Governance Committee
Document Administrator	Enterprise Data Office
Document Control ID	D19/406504
Date Next Review Due	June 2023

Contents

1. Purpose

The Metadata Management Guideline supports the Bank's Data Management Policy (D19/156142). This Guideline must be applied to Critical Data Elements[1]. This Guideline outlines the specific rules, expectations and criteria that should be followed to comply with the Data Management Policy, in respect to the followings:

- Documentation of Business Metadata and
- Metadata that should be captured to help explain Data Lineage from the point of creation through to the point of consumption.

2. Guideline Objective

The objective of the Metadata Management Guideline is to support the Bank's Data Management Policy and to provide guidance for handling metadata across the data lifecycle.

3. Metadata Management

The following diagram describes where the Metadata Management guideline should be used in the data lifecycle. A description of each data lifecycle step is provided in the Glossary.

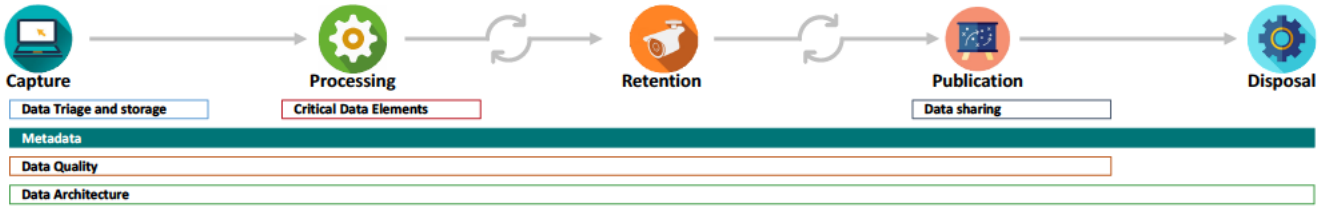


Figure 1 - Metadata management in the data lifecycle

3.1 Definition

Metadata provide basic information about data. It helps in finding and working with particular instances of data. Metadata can be documented manually or automatically by using modern data technologies.

Why is Metadata essential for Data Management?

Metadata provide information about the data; this information could be either of technical nature such as where it is stored or business-related information such as the definition of data or data quality rules. For example, in the case of "Gross Domestic Product", the Technical Metadata may contain a trace of its various inputs and the Business Metadata would define business rules or logic in plain English to derive the final "Gross Domestic Product".

Metadata provide a number of important benefits to the Bank, including:

- **Improved security and quality:** Metadata contain information about data ownership, data classification, data privacy, legal and regulatory requirements. This helps in understanding the appropriate level of security and quality controls that are required to be applied to the data.

1 Definition in Glossary

- **Improved data definitions**: Metadata contain information about data. It helps in understanding terms using definitions that are agreed Bank-wide. This facilitates communication between the Bank staff and, for example, transition during staff rotation.
- **Improved transparency**: Metadata contain information about the origins of data and/or their usage. When maintained properly, Metadata allow for increased discoverability, traceability, auditability and data sharing potential.
- **Improved efficiency**: Well documented metadata accelerate data discovery and understanding. Metadata also help in the identification of potential impacts of changes to code and/or data.

3.2 Business Metadata

Business Metadata contain information that adds meaning to data produced and consumed by business users. This type of metadata assists business users to understand data concepts and their relationships. Business Metadata should be captured for all the identified Critical Data Elements and documented in the metadata register available Bank wide[2].

The following table lists the Business Metadata that must be captured and maintained for all Critical Data Elements according to the level of Data Governance applied:

Field Name	Description
Data Element Identifier*	A unique reference identifier for the data element. The identifier is a system generated key or a user created identifier that uniquely identifies the data element within the Metadata Registry.
Business Term Name	The business name or label assigned to the data element. The name must uniquely imply the content captured by the data element. *Example : Interest, Current Price, Fixed Capital*
Business Definition	Defines the essential meaning of the data element in a precise and unambiguous manner, without embedding definitions of other data, systems or underlying concepts. The business definition must be approved by the relevant data owner or business data steward. Usage context must be incorporated in the definition if the business term has more than one common meaning. Definition should[3]: • State what the business concept is, not only what it is not • Be stated as a descriptive sentence • Be concise, precise, unambiguous and able to stand alone • Contain only commonly understood abbreviations • Be expressed without embedding rationale, functional usage, domain information, or procedural information • Avoid circular reasoning *Example: Interest - Receivable by the owners of financial assets such as deposits, loans, and securities other than shares for putting the financial asset at the disposal of another institutional unit.*
Business Usage	Intended business purpose of the given data element. *Example: Operational reporting, Board Notes, Research and external publication, Regulatory.*

2 IBM Infosphere Information Governance Catalog (IGC) – See appendix 8.5 for screen shots
3 ISO 11179 "part 4"– international standard for representing metadata for an organization in a metadata register

Field Name	Description
Business Rule	Business Rule that defines business behaviour or constraints for the Business Definition wherever applicable. The business rule must not represent system behaviour. *Example: Household debt to GDP:* *i) Ratio should be expressed as percentage; ii) must use data with same periodicity for numerator and denominator; iii) data for shortest available period should be used; iv) values should be denominated in domestic currency*
Category	Logical grouping of related concepts or activities that have common characteristics with respect to variables, concepts and methodologies for data collection, manipulation and transformation. *Example: Banking, Account activity, Arrangement, Financial instruments…*
Permissible Values	List of permitted business values or a range of restricted values. "N/A" should be used if the data element doesn't use a list of values or a range of values. Where possible, this must be a link to a reference data value domain (code list). *Example: 3-character string to identify industry classification as per ANZSIC 2006 (Australian and New Zealand Standard Industry Classification).*
Master or Reference Data Usage	Usage categorisation to flag whether the data element is commonly used within the Bank. Each data element must have one of the following values: • **Yes:** Used cross departments • **No:** Used within a department • **Unknown:** A default value that indicates the data element has not been assessed for usage.
Data Element State	Describe how the data reached its state. Each data element must have one of the following values: • **Raw:** Most non-compounded state of data as collected from a source. *Example: unit or house number, street line 1, post-code, state, country etc.* • **Derived:** A Data Element that is derived from other data elements using a mathematical, logical, or other type of transformation such composition or aggregation. *Example: address line, post-code, state, country in composition makes up an entity address data element.*
Data Element Criticality	A mechanism to classify the data element's significance. Each data element must have one of the following values: • **Critical:** Data Elements where quality or data management practice issues would result in significant and material impacts to regulatory and audit risk, legal and compliance obligations, or make an impact to key business decision making. • **Non-critical:** Data Elements where moderate inaccuracies can be tolerated by the business. Data Elements inaccuracies at this level can generally be worked-around or remediated without material business impacts.
Data Quality Rule	Rules to monitor potential data quality problems against defined business requirements or based on issues that were identified during data profiling. *Example: A data element named 'Email ID' must contain the character '@' sign and the character must be used only once.*
Data Classification	Mirroring the Bank's Information Classification Policy (D12/89323), below are the four levels of data classification values allowed: • **General**: Data that relates to the general business of the Bank and is widely distributed. Public knowledge of its existence carries little reputational or operational risk. • **Restricted**: Data that is not widely distributed for reasons of market, commercial, political or legal sensitivity

Field Name	Description
	• **Highly restricted**: Data that is not widely distributed because unauthorised access could seriously damage the Bank's reputation; damage physical and financial assets; disrupt markets; endanger Bank staff; adversely affect external relationships and impede investigations. • **Extremely restricted**: Data where knowledge of its existence could threaten life directly; jeopardise national interests; damage external relationships, including with other governments. It is advised to consider data classification from a dataset perspective i.e. if a dataset can be deemed as 'Restricted' then all its member data elements should inherit the same classification. This classification must be reassessed as part of the CDE review.
Protected Information	Is this data protected information as outlined in the Bank's Policy D16/429904? (Yes/No) "Protected information" is a term defined in section 79A of the Reserve Bank Act. Detailed available under D16/429904 In general, if the information is lawfully available in the public domain from other sources (i.e. it is readily available to others either free or for a reasonable fee) then it is a "publically available" information, hence, should not be classified as "protected information".
Business Retention Requirement	The duration for which the business wishes to keep the data online in years. If unknown, specify 99.
Legal Retention Requirement	The duration for which the Bank must keep the data (or in some very rare cases, the date when the data must be deleted) in years.
Privacy Classification	Classification regarding the sensitivity status of the data element from a privacy perspective. As specified in the Bank's Privacy Guideline (D14/263782), privacy classification of a data element must have one of the following values: • **Personal:** Data about an identified individual, or an individual who is reasonably identifiable. *Example: Tax File Number, Date of Birth* • **Sensitive:** A category of personal information that covers health, disability, medical, genetic and biometric information and information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, professional or trade association or trade union, religious beliefs or affiliations, philosophical beliefs, sexual orientation or practices or criminal record. • **Not applicable** – 'N/A' While an individual data element by its own right may not be perceived as personal or sensitive, in conjunction with other data elements it may convey a personal or sensitive information and in such cases each member data elements of the composition will need to be classified as per the above.
Related Business Term	Data element having a relationship with the data element we are documenting e.g. while documenting security we can say it is a collateral, and specify "Synonym" in the next field (Relationship Type).
Relationship type	Specify the relationship between the two data elements, e.g: Synonym, Calculated from, Contains, Not Same As, See Also, Required By, Requires, Same As
Regulatory requirement	Specify which regulations (if any) apply to this data element. Example: Privacy Act
Data Owner*	Specify the individual who is accountable for the data elements within their domain and endorses data definition, data quality rules and thresholds for data elements.
Business Data Steward*	Specify the person responsible for the data governance processes within a department and performs activities such as ensuring that data elements are defined, data quality

Field Name	Description
	issues are identified, resolved and monitored, business and technical metadata are documented.
Status*	Status of Data Element – draft/in review/finalised by Data Owner.
Date*	The date when the Metadata was registered or last updated.
Changed By*	Specify the person who made the last change.
Next Review Due*	Date in which the Metadata for data element must be reviewed and updated.

* These fields will be pre-populated.

3.3 Data Lineage

Data lineage is a type of Technical Metadata. Data lineage describes the data origin, what happens to it and where it moves over time. From this lineage, one can ascertain the quality of the data based on its ancestral data and derivations. This helps in tracking back sources of errors, automatically re-enact derivations of a data element, and provide attribution of data sources.

Data Lineage is also essential to the business domain where it can be used to drill down to the source of data in a data store or data warehouse, track the creation of intellectual property, and provide an audit trail for regulatory purposes. The Data Lineage must be captured across three levels:

- **Level 1** Data Lineage must capture the flows between systems in the context of defined business processes and data Domains. Level 1 Data Lineage is meant to be descriptive and targeted to cater for a business audience.
- **Level 2** Data Lineage must capture scripts, jobs and file exchanges between systems. This includes details on technologies, script(s) or job execution details and frequencies of these runs. Level 2 Data Lineage contains a mix of descriptive and technical information and is mainly directed towards System Owners, Data Architects and Data Owners/Business Data Stewards.
- **Level 3** Data Lineage must capture all required attributes, controls, transformation rules and business logic applied in the process of transferring data between systems. Level 3 Data Lineage is ideally captured and maintained via an automated tool. The main audience of such lineage information are Database Administrators, Data Stewards, IT developers and Data Analysts.

The Level 1 and Level 2 Data Lineages should be captured at a data source level. Level 3 Data Lineage should be captured at a Data Element Level with a mapping that allows the link between a Dataset and its member Data Element(s) to be established.

The Level 1 and Level 2 data lineages are descriptive. This type of lineage can be manually documented using a common office tools e.g. Microsoft Word, Excel etc., however, the best practice is to use Business Glossary or Enterprise Cataloguing tool.

For Level 3 Data Lineage, it is recommended to automate the process of recording the metadata at physical level of data processing using one of commercial metadata management tool that have data lineage parsing capabilities.

There are two sources of metadata for automated data lineage:

- '**As built**' – meaning that metadata which is needed for the solution is already available in the database structure;
- '**As designed**' – meaning that information can be read from documentation of system design, for example, from data modelling tools.

Lists the metadata that must be captured and maintained for the three levels are available in appendix.

4. Application per Data Governance levels[4]

Activity / Deliverable	Silver level of Data Governance	Gold level of Data Governance
Registration of dataset into Enterprise Data Inventory	Mandatory	Mandatory
Business Metadata (at business term level)	In addition to the business definition, business context, business and data quality rules, fields related to regulatory or legal requirements are mandatory: • Data Classification • RBA Act classification • Privacy classification • Legal retention requirement • Regulatory requirement Tooling: Information Governance Catalog	**Mandatory,** All fields defined in the Metadata Management guidelines (subject to a reasonable cost-benefit calculation) Tooling: Information Governance Catalog
Technical Metadata, Level 1 Data Lineage	**Mandatory,** Word/Excel/Visio – template to be defined, can be performed using a low code Data Preparation tool	**Mandatory,** Tooling: Information Governance Catalog
Technical Metadata, Level 2 Data Lineage	**Mandatory,** Word/Excel/Visio – template to be defined, can be performed using a low code Data Preparation tool	**Mandatory,** Tooling: Information Governance Catalog
Technical Metadata, Level 3 Data Lineage	**Optional,** Word/Excel/Visio – template to be defined, can be performed using a low code Data Preparation tool	**Mandatory** (subject to a reasonable cost-benefit calculation)**,** Tooling: Information Governance Catalog

5. Roles and Responsibilities

Role	Accountability/Responsibility
Enterprise Data Office – Data management and governance	Accountable for: • developing and maintaining the Metadata Management Guideline. Responsible for: • monitoring the application of the Metadata Management Guideline;

4 Application of the levels of governance per storage environment and use case are available slide 8 of D21/338285 (Process for triaging datasets to appropriate storage and governance)

Role	Accountability/Responsibility
	• facilitating training and communication of this Guideline to relevant stakeholders; and • supporting the review of the Business Metadata.
Data Owner	Accountable for the management of Critical data elements.
Business Data Steward	Act as a delegate of the Data Owner for her/his datasets. Accountable for: • locally implementing the Metadata Management Guideline; • approving the business definition of Critical Data Elements Data Elements for their domain; • approving Metadata change requests where they impact business data; and • ensuring compliance with this Guideline for their dataset(s).
Enterprise Data Office – Coordinating Data Steward	Accountable for: • maintaining business definitions of Critical Data Elements; and proposes new attribute requirements; and • the identification, definition, lineage and documentation of Critical Data Elements in accordance with the Bank's Data Management Guideline. Responsible for: • applying the Metadata Management Guideline; and • promoting the Guideline through day-to-day governance and oversight.
IT system owner	Accountable for: • the required functional and technical expertise and experience for the Metadata and contents of the Metadata for their Critical Data Elements. Responsible for: • working with Coordinating Data Steward(s) to follow the Metadata Management Guideline; and • identifying definition, lineage and documentation of Critical Data Elements in accordance with the Bank's Data Management Guideline.
Data Architect	Responsible for: • Defining the level 1 data lineage; • Ensuring that the level 3 data lineage is available in the metadata management application; and • Ensuring the presence of appropriate metadata fields (e.g. file names, system dates) within data solutions.
Data Stakeholders	**Risk Officers** are accountable for: • reviewing Metadata from a risk perspective and ensure that it is aligned to the Bank's Risk Management Framework/Policy. **Data Privacy Officers** are accountable for: • reviewing Metadata from a privacy perspective and ensure that the data elements meets privacy requirements. **Solution Architects** are accountable for: • ensuring all the scripts and codes that need analysis (across multiple domains and systems) are gathered. **Business SMEs** are responsible for: • ensuring compliance with this Guideline across various domains; and • providing support and expertise in business processes within the domain. **Technical SMEs** are responsible for: • providing inputs on the dataflow to and from their respective IT assets; • providing inputs on the data usage within their respective IT assets; • gathering technical documentations and identifying the scripts that exchange data between IT assets; and

Role	Accountability/Responsibility
	• capturing a detailed view of current controls/control gaps (relating to availability, integrity/quality and confidentiality of data) at the attribute level, if any.

6. Guideline Management

6.1 Administration

This Guideline are administered by Enterprise Data Office.

6.2 Implementation

The EDO is responsible for the implementation of this Guideline.

6.3 Monitoring and Review

The EDO should review this Guideline periodically as and when appropriate.

6.4 Communication

This Guideline is published on the Bank's intranet.

7. Resources

7.1 Related internal documents

- Data Management Framework
- Data Management Policy
- CDE Identification Guideline
- Data Quality Guideline
- Data Architecture Guideline
- Privacy Guidelines
- Information Classification Policy
- BI Platform Metadata Management Guideline (D16/243300)
- GERTRUDE Metadata Guide (D14/53659)

7.2 Related external documents

- Classification of Statistical Subject-Matter Domains
- Prudential Practice Guide CPG235
- Basel Committee on Banking Supervision's standard number 239
- General Data Protection Regulation
- Privacy Act 1988

7.3 Enquiries

Assistance for those applying the Data Governance Guideline:

Enterprise Data Office

8. Appendix

8.1 Glossary

Term	Definition
Business Glossary	A collection of business terms and definitions that have been approved by the stakeholders and are maintained and governed.
Metadata	Data about data - a collection of information describing various facets of a data asset, improving its usability through its life cycle. It provides understanding that unlocks the value of data.
Business Metadata	Business Metadata contain information that adds meaning to data consumed and/or produced by business users.
Metadata Registry	A metadata registry is a central location in an organization where metadata definitions are stored and maintained in a controlled method.
Capture	Data capture is the point of origination of data into the Bank systems. Data capture covers the following: • manual entry of data by a user via user interfaces; • manual and automated data feeds; and • data from internal as well as external sources.
Processing	Data Processing is the application of business rules to data, including regulatory and legal requirements. Data Processing covers the following: • movement and integration of data; • transformation of data; and • updates to data.
Retention	Data retention is the process of storing and managing data for a continuous period for regulatory, legal compliance or to meet business requirements. Data retention covers both data archival and data retrieval. It also includes hosted data (outsourced or retained offshore).
Publication	Data publication is the production of data for internal and external stakeholders, such as the public, or regulatory stakeholders. Data Sharing and Data Publication are the two methods of distributing data.
Disposal	Data Disposal is the process of either erasing or overwriting data for the purpose of regulatory and legal compliance or to meet business requirements.
Control Points	The audit related or preventative measures that are put in place on a data flow to manage and govern data. Some example of data controls are – data load assurance, data quality checks, audit logging, segregation of duties, data reconciliation etc.
Critical Data Element	Critical Data Elements are data elements deemed critical to the successful operations of the business and that need to be managed as a valuable asset i.e. all data elements where quality issues would result in high or very high impacts to senior management decisions, regulatory obligations, business functions or reputation.

Term	Definition
Data Aggregation	The process in which one or many groups of data elements, datasets are gathered, consolidated and expressed in a summary form, for purposes such as statistical analysis.
Data Element	An atomic unit of data that has precise meaning or precise semantics
Data Lineage	Data lineage includes the data origin, what happens to it and where it moves over time. Data lineage gives visibility while greatly simplifying the ability to trace errors back to the root cause in a data analytics process.
Data Quality Assurance	The process of data profiling to discover inconsistencies and other anomalies in the data, as well as performing data cleansing activities (e.g. removing outliers, missing data interpolation) to improve the data quality.
Data Replication	Copying of data from a data source to a target system so as to ensure consistency between redundant resources, to improve reliability, fault-tolerance, or accessibility
Data Transformation	The process of converting data from one format to another, usually from the format of a data source into the required format of a destination system or as required by the data consumer.
Surrogate key	It is a unique key whose only significance is to act as the primary identifier of an object or entity and is not derived from any other data in the dataset. The usual surrogate key used is a unique sequential number and is system generated.
Technical Metadata	Technical metadata describes properties of data that usually inform other computerized processes, such as whether the data is a string or an integer.

8.2 Level 1 Data Lineage

The following table lists the metadata that must be captured and maintained for the Level 1 Data Lineage:

Field Name	Description
Dataset Identifier	A unique reference identifier for the dataset. The identifier could be a system generated key or a manually created identifier that uniquely identifies the dataset within a metadata register document.
Data Flow Identifier	Unique identifier that applies to the scripts/workflows between two IT assets.
Data Source Name	As noted in the Data Naming Standards (D16/96439), a short name for each dataset is determined by business users and based on the Bank's systems and third party sources. These names, which are displayed in the business glossary, do not need to be unique.
Source Provider/System/Application	IT asset name. *Example : ABS*
Source Contact	System owner or authorised delegate
Target System/Application	IT asset name. *Example : BI Sandpit*
Target Contact	System owner or authorised delegate
Control	Name of control points that are in place. If there is more than one type of control, add them separated by a comma. *Example: Data Validation on load.*

Field Name	Description
Data Flow Type	Categorisation of data flows: • Replicate • Transform • Aggregate

8.3 Level 2 Data Lineage

The following table lists the metadata that must be captured and maintained for the Level 2 Data Lineage:

Field Name	Description
Dataset Identifier	A unique reference identifier for the dataset. The identifier could be a system generated key or a manually created identifier that uniquely identifies the dataset within a metadata register document.
Data Flow identifier	Unique identifier that applies to the scripts/workflows between two IT assets.
Data Flow mechanism	Type of the scripts/jobs/workflows that move data from one IT asset to the other *Example: R Scripts, DataStage Jobs, SSIS Jobs*
Script/Job Location	Script/job location in TRIM, code repository or within the integration tool.
Source Dataset Type	Type of dataset: • *File* • *Database/Table* • *Application* • *Other*
Target Dataset Type	Type of dataset: • *File* • *Database/Table* • *Application* • *Other*
Transfer Frequency	Element to identify the frequency of the dataset transfer/refresh *Example : Every 5 minutes, Daily, Weekly, Monthly etc.*

The following table lists the Metadata that must be captured if '**File**' is selected under Source or Target Dataset Type:

Field Name	Description
Data Flow identifier	Unique identifier that applies to the scripts/workflows between two IT assets.
Source File name	Name of the file from where the scripts/workflows are moved
Source File format	File format

Field Name	Description
	Example: csv, txt, JSON, parquet etc.
Target File name	Name of the file to which scripts/workflows are to be moved
Target File format	File format *Example: csv, txt, JSON, parquet etc.*

The following table lists the Metadata that must be captured if '**Database/Table**' is selected under Source or Target Dataset Type:

Field Name	Description
Data Flow identifier	Unique identifier that applies to the scripts/workflows between two IT assets.
Source Database Name	The name of database which contains the source table.
Source Schema	The name of the schema which contains the source table.
Source Table Name	The name of source table
Target Database Name	The name of database which contains the target table.
Target Schema	The name of the schema which contains the target table.
Target Table Name	The name of target table

The following table lists the Metadata that must be captured if '**Application**' is selected under Source or Target Dataset Type:

Field Name	Description
Data Flow Identifier	Unique identifier that applies to the scripts/workflows between two IT assets.
Source Application Name	The name of application which contains the source dataset.
Source Application Gateway	The application URL.
Target Application Name	The name of application which contains the target dataset.
Target Application Gateway	The application URL.

8.4 Level 3 Data Lineage

The following table lists the Metadata that must be captured and maintained for Level 3 Data Lineage:

Field Name	Description
Dataset Identifier	A unique reference identifier for the dataset. The identifier could be a system generated key or a manually created identifier that uniquely identifies the Dataset within a metadata register document.
Data Flow Identifier	Unique identifier that applies to the scripts/workflows between two IT assets.

Field Name	Description
Data Element Identifier	A unique reference identifier for the data element. The identifier could be a system generated surrogate key or a manually created identifier that uniquely identifies an element within a metadata register document.
Source Field / Column	The field name from the source table/file.
Source Format	Source data type.
Target Field / Column	The field name in the target table/file.
Target Format	Target data type.
Transformation Rule	Textual description of transformations implemented by the script/jobs. Do not include the actual transformation code here.
Filters / Constraints	What filters are applied to the Data Element • **Filter Condition**: The filter condition used to restrict data *Example: Where record creation date is within the last one week.* • **Literal / Hardcoded Value**: Any constant value used to populate field *Example: If Country code is not available default it to 'Australia'*

8.5 Information Governance Catalog examples

The following screen shot present a part of the business metadata described in section 3.2

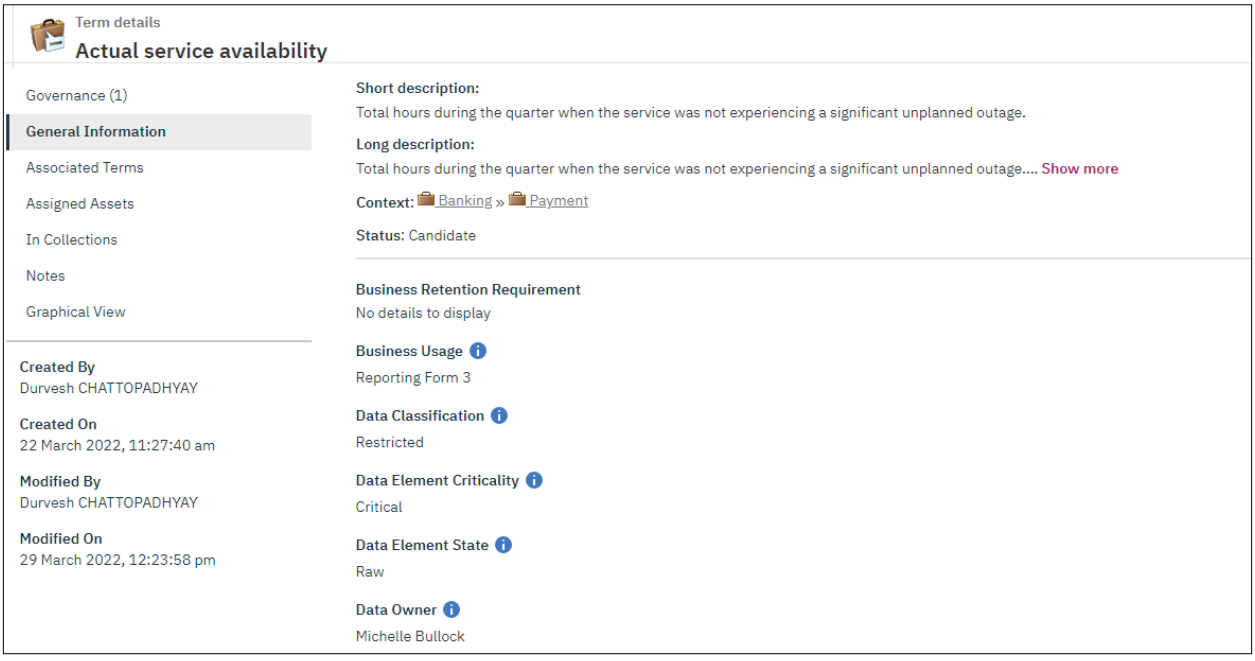


Figure 2 - Business metadata

The following screen shot of IBM Information Governance catalog presents a graphical view of a business term ("Member RITS Code"), and where this term is implemented in the BI Platform.

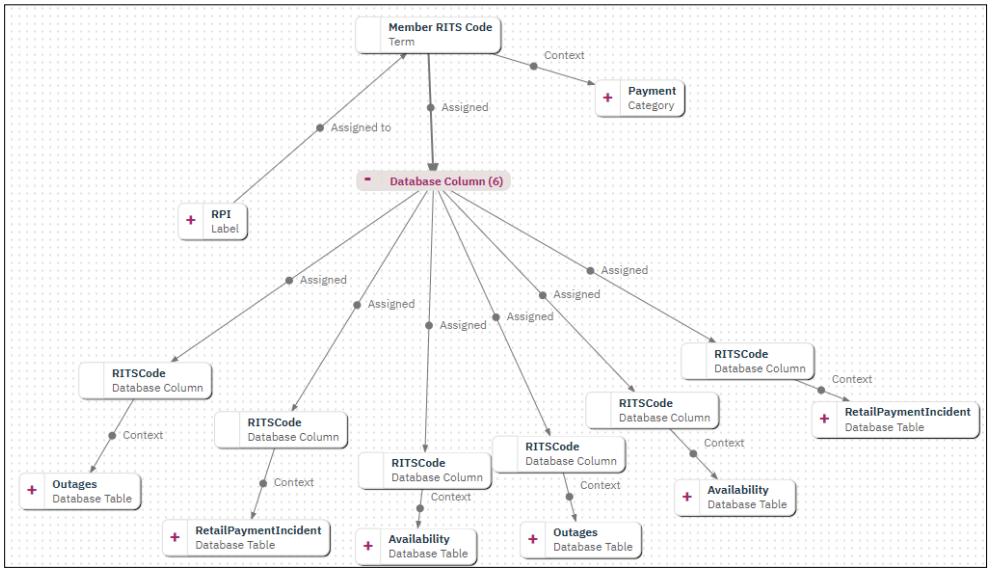


Figure 3 - IGC Screen shot - Search function

RESERVE BANK OF AUSTRALIA

Information Classification Policy

December 2024

Version Control

Version	5.0
Date	13 December 2024
Document Approver	Risk Management Committee
Document Administrator	Knowledge Management Department
Document Control ID	D16/84750
Date Next Review Due	November 2027 for RMC approval December 2027

Contents

1. Key Requirements

The Bank expects that its information assets will be safeguarded. This means that special care is taken when handling, sharing, storing, copying or disposing of Bank information. There are four key elements for ensuring information assets are safeguarded:

- Bank information is assigned a classification according to its sensitivity and the impact its disclosure might cause;
- Classification markers (labels) are applied to all electronic and hard copy records to clearly identify the classification;
- Access privileges are applied based on the classification and sensitivity of the information; and
- Information is handled (stored, distributed and disposed) according to guidelines associated with its classification.

2. Purpose

The purpose of this policy is to ensure the Bank's information assets are classified, secured and handled appropriately, regardless of their format or where the information resides.

By classifying information and specifying appropriate access to it, this policy is intended to help prevent unauthorised access while facilitating information sharing.

This policy complements others that relate to the security of information systems and acceptable use of technology and should be read in conjunction with the Information Management Policy and the Information System Security and Acceptable Use Policy.

3. What does this Policy apply to?

This policy applies to the information assets created, shared and used by the Bank, irrespective of format or location including:

- all records created in the course of work, including emails, documents and Microsoft Office files;
- information stored in TRIM (Content Manager) – the central repository for the Bank's corporate records and metadata about them;
- information (new or active) that resides in network drives;
- information that resides in business and collaborative systems, e.g. Microsoft 365, RBA Box, SharePoint and Power BI Platform;
- selected output from business systems that is shared (e.g. reports).[1]

[1] See the characteristics of this output in Section 5.2(c).

4. Who does this Policy apply to?

This policy applies to you if you:

- are an employee of the Bank; or
- occupy a position (as a contractor, consultant, agency employee or otherwise) within the organisational structure of the Bank; or
- have access to the Bank's information and communications technology systems (ICT Assets) and have been informed that you are required to comply with some or all of this policy; or
- are a contractor, consultant, or visitor to the Bank and have been informed that you are required to comply with some or all of this policy.

5. The Classifications and their Application

5.1 Choosing a classification

The information owner decides the information classification. The decision should be informed by the nature of the content and the intended audience.

Most information produced by the Bank is classified 'General'. This means that all staff could view its content or metadata without posing any significant risks to the Bank. Other information will need varying degrees of safeguarding and require higher information security classifications. Care should be taken to ensure that information is not over-classified.

You should use the following guidelines when applying security classifications to information.

Table 1: Choosing a Classification

Classification	Description	Access	Examples
General	• Information that relates to the general business of the Bank and is widely distributed. • Public knowledge of its existence carries little reputational or operational risk.	Metadata and/or content that can be viewable and searchable by large groups, up to and includingall Bank staff.	• Articles published on the intranet • Bank-wide email communications or newsletters Corporate policies • Staff appointments or movements • Routine enquiries or requests sent to a service desk
	Most records should be classified General		
Restricted	• Information that is not widely distributed for reasons of market, commercial, political or legal sensitivity. • Unauthorised access could cause some reputational damage or operational risk	Metadata and/or content is confined to: • those who work directly with it and have been provided access by the information owner • KM-IM Support staff [(a)]	• Employee records • Contract documents • Committee reports • Confidential analytical notes

	to the Bank and/or to other parties.		
	Many records will be Restricted because it is not appropriate for them to be available to all Bank staff		
Highly Restricted	• Information that is not widely distributed because unauthorised access could seriously damage the Bank's reputation, damage physical or financial assets, disrupt markets, endanger Bank staff, adversely affect external relationships and impede investigations.	Metadata and/or content is confined to: • those who work directly with it and have been provided access by the information owner • KM staff in the TRIM Secure Access Group (SAG)[b]	• Economic forecasts • Monetary policy decisions • Market-sensitive policy advice • Security arrangements • Contentious legal matters
	To be used sparingly and decided by Assistant Governors or their delegates		
Extremely Restricted	• Information where knowledge of its existence could threaten life directly, jeopardise national interests, damage external relationships, including with other governments.	Metadata and/or content is confined to: • those who work directly with it and have been provided access by the information owner • TRIM (Content Manager)) Administrators	• Details of cash distribution • Aspects of banknote security and operations
	To be used with the utmost restraint and decided by Governor, Deputy Governor, or Chief Operating Officer		

(a) Knowledge Management Department (KM) staff who manage a record through its life cycle and are in the TRIM (Content Manager) access group KM - IM Support.
(b) The Secure Access Group comprises the subset of IM Support who require access to higher security classifications to support users and conduct essential lifecycle maintenance of records.

The information security classifications can also be accompanied by conventional 'dissemination limiting markers' (DLMs). These are:

- Official use only
- Personal
- Legal
- Commercial.

These DLMs are used in addition to an information security classification and assist to further identify disclosure and/or special handling requirements. For example, a document might be classified 'Restricted: Legal' or 'Restricted: Personal'.

5.2 Applying a classification

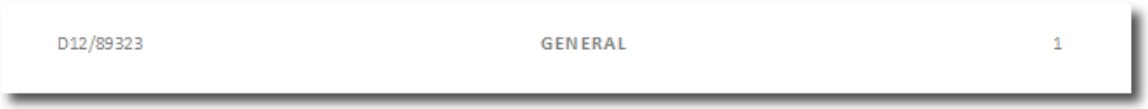
(a) Using Microsoft Purview

When creating new documents, editing existing documents, or sending an email staff are obliged to select a sensitivity label using the Microsoft Purview tool. Staff need to choose the correct classification label that appears in Microsoft applications when:

- sending an email;
- creating and saving a new document;
- editing an existing document that does not already have a label applied.

(b) In TRIM (Content Manager

For information stored in TRIM (Content Manager), information security classifications are applied to each folder. A record automatically inherits the security characteristics of its folder and users can apply additional security as needed. Furthermore, where the information type contains a cover page or footer, you should ensure the security classification is added to records as shown:



(c) In other repositories

For information (new and active) stored in repositories other than TRIM (Content Manager), you must identify the security classification relevant to that information. Where the information type contains a footer or cover page, a security classification marker (as above) should be added to the record as follows:

- to the footer (e.g. for Microsoft Word documents)
- to the cover sheet (e.g. for PowerPoint presentations)

This also applies to the outputs of business systems (e.g. reports) which contain footers where such markers can easily be applied without application system changes.

6. Monitoring access to information

For information stored in TRIM (Content Manager), a full audit trail and audit logs are accessible to information owners and users to identify any unauthorised access including: when a breach occurred; what occurred; and who accessed the information.

In the case of Highly Restricted and Extremely Restricted information, the Governors, Chief Operating Officer, and Heads of Departments can request specific access reports to monitor the integrity of access arrangements.

For information stored outside TRIM (Content Manager), information owners must specify access and IT Department will assist them to identify any unauthorised access to applications, files and infrastructure.

7. Declassification

The information owner remains responsible for controlling the declassification of the information if it no longer needs to remain safeguarded.

When creating a record and assigning an information security classification, the information owner should consider including a future date at which time the record could be declassified to assist with the lifecycle management of information assets. (This future date may be, for example, when public release of the information is scheduled.)

8. Relationship to the Protective Security Policy Framework

This policy provides for an access-based model of managing safeguarded information. In contrast, the Australian Government's Protective Security Policy Framework (PSPF) is based on the security clearances of personnel. This means that the Bank's information security classifications differ from those used in the PSPF.

However, both approaches provide for the classification and protective control of information assets (in electronic and paper-based formats)based on their sensitivity and importance.

While most staff will only be exposed to Bank information, some will be exposed to Australian Government information and will need to ensure that it is handled according to the PSPF. For more information refer to the PSPF – Classification and Handling Guidelines.

9. Policy Management

9.1 Administration

This policy is administered by Knowledge Management Department.

9.2 Implementation

The Senior Manager, Information Solutions, Knowledge Management Department is responsible for the implementation of this policy.

9.3 Compliance

Knowledge Management Department is responsible for monitoring compliance with this policy. Compliance is supported through monitoring completions of the e-learning module, 'Managing Information' and also reporting to the Risk Management Committee.

9.4 Monitoring and review

This policy is reviewed by Knowledge Management Department at least every three years or more frequently if there is a major change. All changes to the policy must be approved by Risk Management Committee.

9.5 Communication

This policy is published on the intranet and is also communicated via the 'Managing Information' e-learning module as part of the compliance pathway.

10. Resources

10.1 Related internal documents

D13/91827	ICP – RBA Classification and Handling Guidelines
D20/26538	PSPF – Classifications and Handling Guidelines
D11/24451	Information Management Policy
D18/320100	Information Systems Security and Acceptable Use Policy
Intranet	Classifying Information (sharepoint.com)

10.2 Enquiries

Contact the KM-Engagement and Training team with any handling of information queries.

RESERVE BANK OF AUSTRALIA

Email Management Guidelines

November 2025

Version Control

Version	3.1
Date	12 March 2025
Document Approver	Head of Knowledge Management
Document Administrator	Knowledge Management Department
Document Control ID	D21/324310
Date Next Review Due	March 2028

Contents

1. Purpose

Email is a well-established communications channel that has become the most common form of corporate correspondence. These guidelines outline the acceptable use and handling of email, management of email accounts, and the role Bank staff have in managing and classifying their emails as a corporate record.

2. Responsibilities

Every staff member is responsible for managing their use of email and email accounts to ensure compliance with the RBA's use of technology, records management and classification requirements. Staff should familiarise themselves with:

- the Information Systems Security and Acceptable Use Policy
- the Information Management Policy; and
- the Information Classification Policy.

The Bank views breaches of its policies seriously and breaches will be assessed in terms of the requirements of the Code of Conduct and relevant laws to the extent they apply.

Information Technology (IT) Department is responsible for monitoring and surveillance of email accounts, providing secure email channels for external communications and alternative communication channels for emails that exceed the maximum size limit. Currently the size limits are 50MB for internal email or 20MB for external emails.

Knowledge Management Department (KM) is responsible for providing training and support services to Bank staff, and monitoring high-level email activities to ensure email management and handling practices are consistent with the Bank's Information Governance Framework.

3. Acceptable Use of Email

Acceptable use of Bank email accounts includes:

- Using Bank email accounts for all work-related communication.
- Using Bank email accounts on Bank-approved MDM devices or technologies.
- Capturing emails as corporate records when they provide evidence of work.
- Reporting any suspicious emails or attachments to IT via the 'Report Phishing' add-in.
- Ensuring emails and meeting invites are classified and handled appropriately.
- Emailing information up to RESTRICTED classification to external parties.
- Using links (i.e. TRIM links) when sharing information internally.
- Sharing information externally using the TRIM 'Email PDF copy' function, when practical.
- Using approved collaborative platforms (i.e. RBA Box) when sharing HIGHLY RESTRICTED information externally or if you need to share large files.

Unacceptable use of Bank email accounts includes:

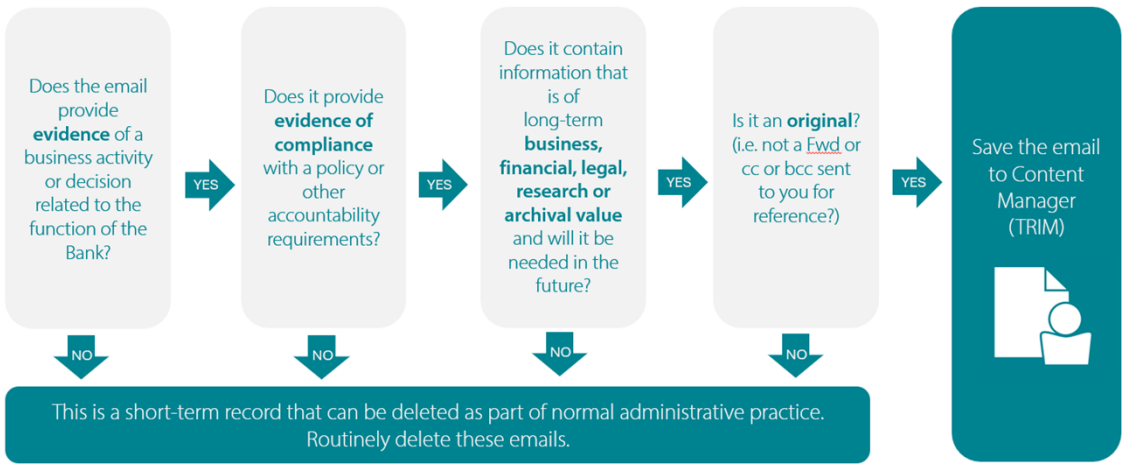
- Sending emails that do not comply with the Code of Conduct, e.g. sending a personal email using the Bank's email system in your professional capacity as Bank staff.
- Treating Bank email accounts as personal accounts.
- Sending any Bank information to personal email accounts on external systems.[1]
- Clicking on links or open attachments from senders that you suspect to be phishing or lack credible features.
- Sending attachments to internal recipients when links should be used.
- Encrypting emails unless required as part of an approved exempted business process. e.g. when sharing EXTREMELY RESTRICTED information.
- Providing information classified as RESTRICTED or above in Out of Office notifications for outside the organisation.

4. Capturing Corporate Records

4.1 Which emails are corporate records?

An email that provides evidence related to the Bank's functions, business, or transactions is a corporate record and must be captured in Content Manager (TRIM). It is especially important that such information is captured if it provides evidence of an instruction, decision, approval or a change in Bank policy. Figure 1 provides a decision tree diagram to help staff determine which emails need to be captured as corporate records.

Figure 1: Decision Tree - Capturing Email as Corporate Records[2]



1 The guidelines allow for sending private or staff-specific information to a personal email account, e.g. forwarding your personal tax form or payslip.

2 Figure 1 is sourced from D21/347973 Email Management – TRIM or Delete.

4.2 Which emails are not corporate records?

All emails that are of short-term value, duplicate or not original, do not need to be captured in TRIM and can be disposed at the discretion of the staff member using Normal Administrative Practice.

4.3 Who should capture emails as corporate records?

In general, staff members are responsible for capturing their own corporate records. However, there are two exceptions. The first exception is when staff are part of a team that uses a shared email box. The team needs to specify who is responsible for capturing corporate records; this can be individual staff members or a designated member on behalf of the team. The second exception is when senior Bank staff have an assistant who works directly to them; the assistant can be designated to capture corporate records on their behalf.

4.4 When should I capture emails as corporate records?

The recommended time to capture an email as a corporate record is at the completion of the work task or when a decision has been made. If staff send or receive subsequent emails on the same subject they have two options. The first option requires staff to create a new record with additional text in the title field e.g. 'reply from XXXX'. The second option allows staff to create a new revision of the initial record using the 'Attach to the record' field in Content Manager (TRIM).

Staff should be aware that sometimes, the important part of the email, is an attachment received from external parties. Staff should capture the attachment separately using the 'Check in attachments' option in MS Outlook.

4.5 How should I title emails that are corporate records?

When capturing an email or attachment in Content Manager (TRIM) staff need to ensure the record has a meaningful title. Emails without meaningful titles can be difficult to find and their value in recording a decision or outcome is potentially lost. To make the title meaningful, staff should include the following details: subject – matter - parties – date. An example of a meaningful title is: "Travel Approval – Switzerland – John Smith – March 2025".

4.6 TRIM guides for managing emails

For more information on how to manage emails as corporate records see:

- Email Management – TRIM or Delete
- Saving Emails from Outlook
- Saving Email Attachments from Outlook
- Email Integration with TRIM
- Document Naming Standard

5. Classifying Emails and Calendar Invites

The Bank requires that all internal and external emails are classified using Microsoft Purview. This tool requires staff to select a label when sending an email or calendar invite. Security classification labels should accurately reflect the sensitivity of the information that is mentioned in the email or the content to be discussed in the meeting. More information about how to apply security classifications is available on the intranet and within Microsoft Outlook when a pop-up appears before sending emails and calendar invites.

6. Guideline Management

6.1 Administration

This Guideline is administered by Knowledge Management.

6.2 Implementation

The Head of Information and Data Governance, Knowledge Management Department is responsible for the implementation of this Guideline.

6.3 Monitoring and review

This Guideline is reviewed by Knowledge Management Department every three years. All changes to the Guideline must be approved by the Head of Knowledge Management Department.

6.4 Communication

This Guideline is published on the Bank's Policies + Intranet page and referenced throughout KM's information governance documentation.

7. Resources

D11/24451	Information Management Policy
D12/89323	Information Classification Policy
D09/227086	Code of Conduct
D18/320100	Information Systems Security and Acceptable Use Policy
D21/32507	Normal Administrative Practice
Intranet	Managing Information - Home (sharepoint.com)
Intranet	Classifying Information

7.1 Enquiries

Contact the KM-Information Governance team with any queries.

RESERVE BANK OF AUSTRALIA

Risk & Compliance Operating Model Proposal

Employee Briefing

12 May 2025

D25/110074
RESTRICTED

CONFIDENTIAL

Why are we changing?

# of incidents which is outside our risk appetite

Internal and external reviews, plus audit findings, a need to strengthen Line 2

Pulse Surveys reveals workload pressures affecting employee engagement

Opportunity to refocus, strengthen Line 2

Alignment to Best Practices

CRO 'Voice of risk'

Clear roles and accountabilities

What are we aiming for?

Our North Star

Clear accountabilities for managing risk
Our people are clear on their roles in owning and managing risk

Healthy tension between Line 1 and Line 2
Departments demand and value an independent perspective to inform their decision-making

Capacity and capability
Departments have sufficient resources and skills to manage current and emerging risks

Highly resilient central bank
Confidence that processes are robust and adequate controls are in place to address risk

Strong risk culture
Our people are empowered to raise risk and opportunities for improvement

Consistency and focus
Frameworks, policies and standards are consistently applied, allowing focus on material risk

Reliable risk reporting
Accurate information and reporting enabling confident and timely decision-making

Current State vs Future State

From

Broad roles and responsibilities
Roles currently include a mix of line 1, frameworks and line 2 review and challenge

Lack of clarity around line 1 and line 2 responsibilities
Sometime assumed that risk management is RM's responsibility

Insufficient capacity to effectively review and challenge line 1
Mixture of responsibilities weakens ability to effectively challenge

Limited controls assurance undermines resilience
Controls assurance is immature and fairly 'stand-alone' withing RM and maturity levels in line 1 are low

Limited line 2 oversight leads to inconsistent application of risk frameworks

Risk reporting not leading to effective decision making
Risk reporting is currently done on top of other responsibilities

To

Clearly defined roles and accountabilities
Teams structured for specific purposes, with senior level capability to drive transformation and improvement in line 1 responsibilities.

Clearly defined line 2 purpose
Brings line 2 responsibilities to the forefront, especially in relation to review and challenge.

Capacity and capability to effectively review and challenge
More specialised teams for risk will drive improvement in risk management practices

Highly resilient central bank
Leveraging insights from reporting team and business oversight will enable a more integrated controls assurance program, also leveraging business oversight and line 1 teams for execution

Consistency and focus
Standards provide consistency for more effective oversight of line 1 risk management (delivered through additional capacity and capability in business oversight)

Reliable risk reporting
More robustness in risk data (through standards and additional line 1 capacity), and insights leveraged through business oversight will enable more accurate information and reporting, which in turn, will enable confident and timely decision-making

RESERVE BANK OF AUSTRALIA

What's Changing? Proposed Service Offering

Chief Risk Officer

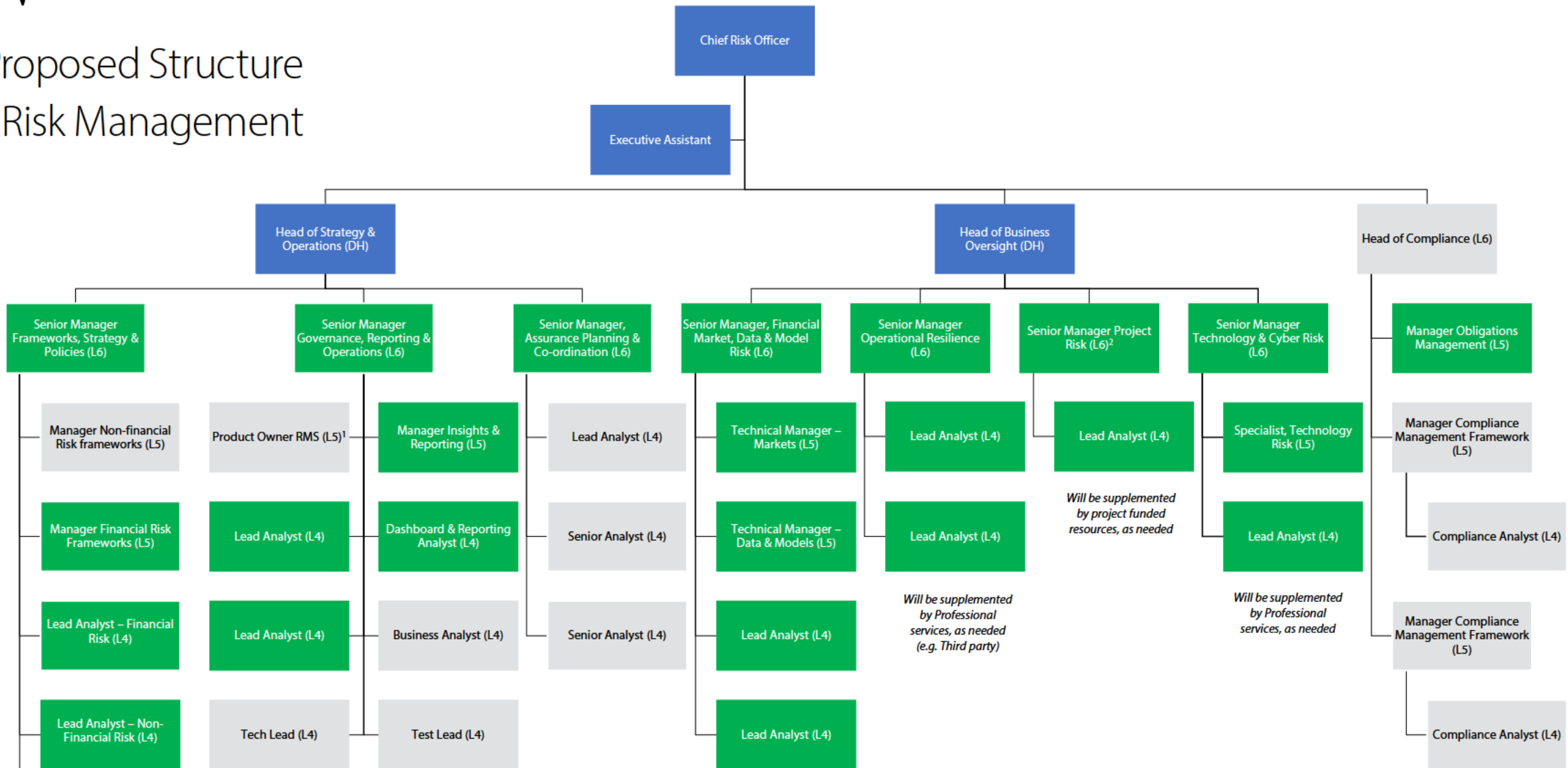
New Team *- new Deputy Head, re-alignment and re-focussing of service offering*	***New Team*** *- new Deputy Head and new service offerings*	***Existing Team***
Strategy & Operations	**Business Oversight**	**Compliance**
Build, deliver and maintain best practice risk management frameworks, policies and tools that are impactful, valued and contribute to the Bank's management of risk and effective decision making, ensuring consistent application across the Bank.	Drive independent challenge and oversight into the Line 1 operations, elevating the CRO's ability to lead the 'Voice of Risk' at a department level. Independent challenge contributes to effective management of the Bank's most critical risk exposures.	Drive a strong compliance culture across the Bank, provide accurate compliance and regulatory support to better enable the Bank to identify, treat and mitigate exposure.

What does this mean for me?

- ✓ As a **team**, we will have clearly defined roles and responsibilities. This clarity will help **you** understand **your purpose and empower** you to drive improvements confidently. **You** will also be able to clearly communicate our roles and the value we provide to our stakeholders.
- ✓ As a **team**, we will emphasise the importance of reviewing and challenging processes. This gives **you** the **power** to ensure things are done correctly and to suggest improvements, fostering a culture of accountability. **You'll** play a **key role** in maintaining high standards and driving positive change.
- ✓ You will have the **support and development opportunities** to be part of a specialised team focused on improving risk management practices. This will not only **enhance your skills** but also contribute to the overall success of the RBA corporate plan. **You'll** be part of a team that makes a real difference.

RESERVE BANK OF AUSTRALIA

Proposed Structure - Risk Management



NOTES

1. *Product Owner RM is a temporary role funded by FutureHub through to 03/2026.*
2. *Temporary role - Fixed term (12 months).*

The following additional changes are proposed

Effective 23 June

The **Project Risk team** led by Manager - Project Risk will repoint to Head of Strategy, Architecture Transformation & Governance in IT.

The **Portfolio Risk & Compliance (PRC)** team will be led by Senior Manager - Portfolio Risk & Compliance.

The following roles will repoint to the Senior Manager – Portfolio Risk & Compliance:

- Manager, Domestic Portfolio
- Manager, Foreign Portfolio
- Manager Documentation & Regulation

By 30 September

The **Portfolio Risk & Compliance (PRC)** team led by Senior Manager - Portfolio Risk & Compliance will repoint to the Deputy Head, FMG.

The **Data Analysts, Senior Data Analysts and EDM BAU support team in Risk Business Operations** will repoint to FMG. Once the new Deputy Head FMG role has commenced we will be able to determine the most appropriate reporting line for these roles in FMG.

Consultation about the Proposed Structure

- As a first step, and before finalising the proposed structure, we will open up for consultation and **invite your feedback**.
- We encourage feedback from **everyone in Risk Management** and ask that you send this via email **to Keith Drayton** and/or **by 5pm Thursday 15 May 2025**.
- All feedback and comments will be considered continuously throughout the feedback period, prior to finalising the proposed structure.
- Please feel free to **speak to Keith** and/or (in person or by phone) if you have any questions.
- At our next briefing on **Friday, 16 May 2025**, we will aim to confirm our structure.

RESERVE BANK OF AUSTRALIA

Consultation Timeline

Proposed Structure Announced	Consultation Period	Confirm Outcome of Consultation & Individual Outcomes	Proposed Structure Commences
12th May	From 12th to 27th May	By 28th May	23rd June
• Employees are advised of the proposed changes and how they impact your role. Employees are also provided with the anticipated organisational structure for feedback. • Consultation commences.	• This is a period where employees are able to provide feedback on the proposed change. • During this time employees will be invited to attend information sessions about the proposed structure and proposed new roles. • Employees have until COB 15th May to submit written feedback on the proposed structure. • The business will consider feedback received during this period. • On 16th May the CRO will report back on any changes that may be made as a result of consultation feedback, the confirmed structure and next steps. • From 19th to 22nd May impacted employees will have a 1:1 with the CRO and can use this opportunity to discuss their preferences for any new roles.	• From 26th to 28th May The CRO will have 1:1s with impacted employees to discuss individual consultation outcomes. • On 28th May the new structure is announced following confirmation of consultation outcomes with employees. *Note: more time may be required to fully consider all impacted employee's situations.*	• The new structure will commence.

Impact to Individual Roles – Redundancy and Redeployment

- If the changes proceed as proposed, we will then work with each impacted employee individually to understand their preference in relation to roles within the new structure.
- Our aim is to complete the role outcome discussions process by **28 May 2025**.
- Everyone will have access to the job profiles for each of the proposed roles and we will hold 'drop-in sessions' where you can come and find out more about the proposed roles and the new ways of working.
- If your role is impacted you can also share with us if your preference is to find employment elsewhere in the Bank or have your employment end by reason of redundancy.

New Job Profiles and Roles

The **job profiles** for the Risk Management job family have been reviewed align ensure alignment to the 3 Lines of Accountability model.

We have introduced separate job profiles that are specific to Deputy Head, Senior Manager, Manager and Lead Analyst roles that sit in Line 1 and Line 2.

The new Risk Line 2 job profiles can be viewed here D25/137707.

Role (Level)	#	New roles
Senior Manager (L6)	1	Senior Manager - Frameworks, Strategy & Policies (L6)
	1	Senior Manager - Governance, Reporting & Operations (L6)
	1	Senior Manager - Assurance Planning & Coordination (L6)
	1	Senior Manager - Financial Market, Data & Model Risk (L6)
	1	Senior Manager - Operational Resilience (L6)
	1	Senior Manager - Project Risk (L6) [*Fixed term for 12 months]*
	1	Senior Manager - Technology & Cyber Risk (L6)
Manager (L5)	1	Manager Financial Risk Frameworks (L5) - Frameworks, Strategy & Policies
	1	Manager Insights & Reporting (L5)– Governance, Reporting & Operations
	1	Technical Manager - Markets (L5) - Financial Market, Data & Model Risk
	1	Technical Manager – Data & Models (L5) - Financial Market, Data & Model Risk
	1	Specialist, Technology Risk (L5) - Technology & Cyber Risk
	1	Manager Obligations Management (L5) - Compliance
Lead Analyst (L4)	1	Lead Analyst – Financial Risk (L4) - Frameworks, Strategy & Policies
	1	Lead Analyst – Non-Financial Risk (L4) - Frameworks, Strategy & Policies
	1	Dashboard & reporting Analyst (L4) - Governance, Reporting & Operations
	2	Lead Analyst (L4) - Governance, Reporting & Operations
	1	Dashboard & Reporting Analyst – Governance, Reporting & Operations
	2	Lead Analyst (L4) - Financial Market, Data & Model Risk
	2	Lead Analyst (L4) – Operational Resilience
	1	Lead Analyst (L4) – Project Risk
	1	Lead Analyst (L4) - Technology & Cyber Risk

Our Ask

- I acknowledge that this is a lot to take in and the next couple of weeks might be challenging as you explore the various options.
- Everyone will remain in their current roles while we work through these changes; please continue with your business-as-usual work and let us know if you need any help or support.
- Everyone will received a copy of this pack.
- Please be respectful and considerate of colleagues during the consultation period.
- Ask and be curious about the changes and opportunities.

Who can I talk to?

- Chief Risk Officer – Keith Drayton
- People Partner, Strategic Partnering, People Department

Additional Support

As part of this process, you may also wish to share the materials with a representative (which may include a Union representative) and have them attend meetings as your support person.

The Bank's Employee Assistance Program

Provided our Employee Assistance Program (EAP) gives us all free and confidential access to a range of wellbeing services including:

- Psychological counselling
- Manager support coaching
- Wellbeing coaching
- Financial coaching

The services they offer can help us all to achieve lifestyle, work, personal and family goals and assist with managing work and life experiences, issues or concerns that arise from time to time.

For more information on the Bank's Employee Assistance Program see the dedicated intranet page here: Employee Assistance Program.

If you would like to speak to an EAP counsellor you can contact

and they will coordinate this for you.

Alternatively, to book a confidential appointment, please call

Appendices

Department Goals

Purpose	Goals / Objectives
Alignment of risk management to the Bank's strategy and objectives to maximise our chance of success	Develop risk management strategy to support the Bank's strategy, and operationalise it through frameworks, policies and standards
	Provide accurate, independent and critically assessed insights and information to our governance forums to enable effective decisions.
	Ensure the right risks get discussed and that effort is appropriately prioritised to the mitigation of the risks that matter most.
Provide effective line 2 oversight (independent review, challenge and insight) of the Bank's risk management and compliance activities	Drive the development and business acceptance of all risk and compliance frameworks across the Bank.
	Provide insights into business areas through development of strategic and trusted relationships and effective review and challenge of activities.
	Provide specialist advice to business areas to ensure consistent and quality adoption of the Risk Management Framework and effective management of compliance obligations
Equip employees to take appropriate risks in a way that contributes to a proactive risk culture	Raise awareness around potential risks among our employees, ensure everyone understands their role in mitigating risk and where to prioritise their effort through a shared understanding of what matters most.
	Foster an environment where our employees feel comfortable reporting risks and discussing potential issues without fear of retribution.
	Ensure consideration of risk is a fundamental part of our decision-making at all levels.

Goals - Strategy and Operations

Purpose	Goals / Objectives
Develop risk management strategy to support the Bank's strategy, and operationalise it through frameworks, policies and standards	Develop frameworks and policies to support corporate strategy - sufficiently responsive to emerging and changing risks and proportionate to key risks.
	Regularly assess our risk management maturity level and develop standards to drive consistency and improvement in risk management so executives have better information and visibility over our risks.
	With other teams, work to ensure frameworks, policies and standards are consistently applied, allowing focus on material risk and supporting strategic insights.
Provide accurate, independent and critically assessed insights and information to our governance forums to enable effective decisions	Support the establishment and continuous improvement of the Governance Board, manage governance arrangements for the Risk Management Committee and prepare bank-wide insights (based on risk data and leveraging insights from the business oversight function), reporting and monitoring for our key governance forums.
	Drive innovation in risk management processes and our supporting enterprise risk management system, leveraging the latest industry trends and technologies.
	Work with the business areas to enhance data, dashboards, and broader reporting to ensure timely, accurate, risk-based decision making.
	With input from the business oversight team, understand enterprise key risks, strategic risks and emerging risks and identify areas for more focused attention.
Ensure the right risks get discussed and that effort is appropriately prioritised to the mitigation of the risks that matter most	Identify areas of control where closer inspection is required, plan and co-ordinate control testing and assurance.
	Provide key insights (e.g. on the health of the control environment) to inform investment priorities
	Provide assurance to the Governance Board and other governance forums on the effectiveness of the Risk and Compliance Management Framework, and departmental compliance with the framework.

Goals - Business Oversight

Purpose	Goals / Objectives
Drive the business acceptance of all risk frameworks across the Bank	Gain executive and departments head commitment to the value of consistent and effective management of our risks and controls and gain organisational commitment to a proactive risk culture.
	Drive consistent understanding and adoption of our risk frameworks in departments by examining material risk classes across departments and encourage employees to escalate and drive appropriate responses where departments are not aligned to risk frameworks.
	Work with departments to validate risk frameworks are consistently applied and provide specialist knowledge to the 'Strategy and Operations' team to develop fit-for-purpose frameworks that enable the achievement of our business objectives.
Provide insights into business areas through development of strategic and trusted relationships and effective review and challenge of activities	Through teams structured teams to align to Bank's material risk classes, provide specialist advice on the breadth and complexity of the Bank's material risk classes.
	Effectively review and challenge departments on their management of our material risks, providing them with risk insights, through teams aligned to material risk classes with specialised domain knowledge and risk capability.
	Provide risk-specific insights to the Strategy and Operations team to incorporate into risk reporting, helping with the effective management of the Bank's material risk classes.
Provide specialist advice to business areas to ensure consistent and quality adoption of the Risk Management Framework	Provide leadership in relation to material risk classes by developing specialised risk class teams with dedicated capability and capacity to apply both domain knowledge and risk capability to their advice to departments and governance forums.
	Monitor and challenge the management of material risk classes in departments, validating compliance with the Risk Management Framework.
	As input into maturity assessments by the Strategy and Operations team, identify and report areas for improvement by undertaking thematic and targeted reviews of material risk classes, and benchmarking against best practice.

Goals - Compliance

Purpose	Goals / Objectives
Drive the development and business acceptance of compliance frameworks across the Bank	Influence executives and departments heads on the value of consistent and effective management of our compliance obligations and controls.
	Work with departments to ensure that our compliance framework is fit-for-purpose and enables the achievement of our business objectives.
	Drive consistent understanding and adoption of our compliance framework in departments.
Provide insights into business areas through development of strategic and trusted relationships and effective review and challenge of activities	Identify our most significant compliance obligations and provide specialist advice to departments to enable effective management of our most significant compliance obligations.
	Working with the line 2 assurance team, effectively review and challenge departments on their management of compliance obligations.
	Provide insights to departments to help with the effective management of the Bank's compliance obligations.
Provide specialist advice to business areas to ensure consistent and quality adoption of the Compliance Framework and effective management of compliance obligations	Develop dedicated capability and capacity that can provide advice to departments on the Bank's most significant compliance obligations.
	Oversee the management of targeted compliance obligations, validating compliance with our Compliance management framework and Bank policies.
	Undertake thematic and targeted reviews of targeted compliance obligations and regular maturity assessments to identify areas for improvement.

RESERVE BANK OF AUSTRALIA

What's Changing? Proposed Service Offering

1. ***Strategic leadership*** *and board/senior executive engagement*
2. ***Enterprise approach*** *and* ***insights*** *on risk management, aligned to objectives and goals*
3. *Business area engagement (****review and challenge****) on management of our risks and controls, driving improvement in practices*
4. *Teams with clear delineation of responsibilities, designed to drive* ***consistent practice*** *and improve* ***quality*** *of* ***risk reporting***
5. *Dedicated capability and capacity to* ***review and challenge*** *line 1, aligned to risk classes*
6. *Strengthened approach to management of regulatory* ***obligations***

Chief Risk Officer (1)

Strategy & Operations (2)

Build, deliver and maintain best practice risk management frameworks, policies and tools that are impactful, valued and contribute to the Bank's management of risk and effective decision making, ensuring consistent application across the Bank

Frameworks, Strategy & Policies

Services

- Develop and maintain Risk Management Frameworks, policies, and standards.
- Define risk and control taxonomies to ensure a unified approach.
- Establish and enhance risk management learning pathways.
- Design and implement a methodology for assessing risk culture.
- Drive continual refinement of the Risk Appetite Statement (RAS), metrics, and tolerances.
- Strengthen the Bank's extreme event scenario and stress testing framework.
- Embed emerging risk management frameworks and scenario planning.
- Coordinate and support departmental risk management maturity and culture assessments.
- Deliver a comprehensive risk training strategy informed by capability assessments.

Governance, Reporting & Operations (4)

Services

- Innovate risk management frameworks, processes, and systems.
- Enhance data, dashboards, and broader reporting for better decision-making.
- Facilitate and improve governance arrangements for the RMC and Governance Board.
- Deliver bank-wide risk insights, reporting, and monitoring.
- Continuously improve the Bank's risk management system strategy and investment.
- Establish common metrics and tolerances for data quality and insights.
- Aggregate and challenge departmental risk profiles to build an RBA-wide view.
- Review and challenge Line 1 committee papers and outputs for accuracy.
- Support emerging risk identification and proactive attention.

Assurance, Planning & Coordination

Services

- Lead integrated assurance planning in collaboration with Line 1 and Line 3.
- Develop and execute an annual assurance plan endorsed by the Audit & Risk Committee.
- Define and obtain approval for the Line 2 assurance methodology.
- Execute thematic reviews, deep dives, and controls assurance with a focus on scope, fieldwork, and reporting.
- Undertake bank-wide thematic reviews on key risks (e.g. issue concentration or emerging risks).
- Leverage emerging technologies like AI and analytics tools for efficient assurance processes.
- Coordinate reporting on assurance plan status, key insights, and findings.
- Provide comprehensive reviews and challenge departmental risk registers for completeness.
- Monitor and report on departmental and enterprise-wide compliance with the risk framework.

Business Oversight (3)

Drive independent challenge and oversight into the Line 1 operations, elevating the CRO's ability to lead the 'Voice of Risk' at a department level. Independent challenge contributes to effective management of the Bank's most critical risk exposures

Financial Market, Data & Model Risk

Services

- Policy administrator/owner of the model risk framework, including supporting policies and standards.
- Guide executives and department heads on the effective management of financial market, data and model risk.
- Oversee the management of data and model risk within departments.
- Conduct independent review and challenge of market, model and data risk assessments at both department and Bank levels.
- Perform thematic reviews on market, data and model risk classes, such as issues, incident concentrations, and emerging risks.
- Undertake targeted reviews of RBA-wide and departmental action plans to ensure risks remain within appetite and tolerances.
- Prepare high-quality reports for departmental executives and risk governance committees.
- Drive innovation in market, model and data risk management processes and tools by leveraging the latest industry trends and technologies.

Operational Resilience (5)

Services

- Policy administrator/owner of the operational resilience framework, supporting policies and standards.
- Endorse and maintain the Service Provider Management (SPM) Policy.
- Influence executives and department heads on effective operational resilience risk management.
- Oversee the management of operational resilience risk within departments.
- Conduct independent review and challenge of resilience arrangements for critical operations and departmental business continuity plans.
- Perform thematic reviews of operational resilience risks, addressing issues, incident concentrations, and emerging risks.
- Undertake targeted reviews of RBA-wide and departmental action plans to ensure alignment with risk appetite and tolerances.
- Prepare high-quality reports for departmental executives and risk governance committees.
- Drive innovation in operational resilience processes and tools, leveraging the latest industry trends and technologies.
- Develop and deliver operational resilience training across the organisation.
- Monitor and report on the effectiveness of the operational resilience framework and adherence across Line 1 and departments.

Project Risk

Services

- Policy administrator/owner for the "risk in change" framework, supporting policies and standards.
- Influence executives and department heads on effective delivery and delivered risk management.
- Monitor and report on the effectiveness of the "risk in change" framework.
- Innovate project risk management processes and tools, leveraging industry trends and technologies.
- Provide insight, review, and challenge for portfolio-level and project-level delivery risks.
- Independently review and challenge prioritisation by the Investment Committee.
- Independently assess delivery risks at project and departmental levels, including aggregation to the RBA level.
- Provide insight, review, and challenge the quality of delivered risk management at portfolio and project levels.
- Independently review delivered risk assessments in department-level risk profiles and their aggregation to the RBA level.

Technology & Cyber Risk

Services

- Policy administrator/owner of the IT and cyber risk management framework, including supporting policies and standards.
- Influence executives and department heads on effective IT and cyber risk management practices.
- Oversee and monitor the management of IT and cyber risk across departments.
- Provide independent review and challenge of IT and cyber risk assessments at both departmental and RBA (Bank) levels.
- Conduct thematic reviews for technology and cyber risk classes, addressing issues, incident concentrations, and emerging risks.
- Perform targeted reviews of RBA-wide and departmental action plans to ensure risks are within appetite and tolerances.
- Prepare high-quality reports for departmental executives and risk governance committees.

Compliance

Drive a strong compliance culture across the Bank, provide accurate compliance and regulatory support to better enable the Bank to identify, treat and mitigate exposure

Compliance (6)

Services

- Policy administrator/owner of the Compliance Strategy, Compliance Management Framework, and supporting policies and standards.
- Influence executives and department heads on effective compliance risk management.
- Monitor and report on the effectiveness of the Compliance Management Framework.
- Conduct centralised scanning of the regulatory environment and communicate regulatory changes.
- Perform obligation breakdowns for prioritised legislation/regulation based on the consequence of non-compliance.
- Develop and roll out compliance training across the organisation.
- Oversee and monitor compliance risk management within departments.
- Provide high-quality reports to departmental executives and risk governance committees.
- Drive innovation in compliance management processes and tools, leveraging the latest industry trends and technologies.

From: DRAYTON, Keith
Sent: Monday, 12 May 2025 3:42 PM
To: Risk and Compliance - RM
Cc:
Subject: Consultation Information [SEC=OFFICIAL]

Good afternoon team,

Thank you for joining the meeting earlier today. I understand there was a lot to take in, and I appreciate you taking the time to listen and consider the information shared. Please find the pack here: D25/140585.

As mentioned in the meeting, I'm seeking your feedback on the proposed model and structure over the next two days. We're particularly interested in your thoughts on the proposed services, structure, and the roles outlined. I'll be holding drop-in sessions on Tuesday 13 May and Wednesday 14 May to answer any questions you may have about the structure. You will get a separate invite for these.

As a reminder, feedback on the proposed model is welcome by **end of day Thursday, 15 May 2025**. I would encourage you to submit your feedback via email so we can ensure that all feedback is captured and considered. You should also feel free to speak with us directly.

Once I've had the opportunity to review and consider all feedback, an outcome briefing will be scheduled for **Friday, 16 May**. I encourage you to attend in person if possible.

A gentle reminder – over the coming weeks, your kindness and support towards colleagues will be especially valued. Please continue to be mindful in your interactions.

We also want to make sure you feel supported throughout this process. If you'd like additional support, our Employee Assistance Program (EAP) is available, and you may schedule a session directly with via this link:

Our Health and Safety team is also available if you'd prefer a confidential conversation. You can reach to to arrange a one-on-one discussion.

Regards,

Keith Drayton | Chief Risk Officer
RESERVE BANK OF AUSTRALIA | 8 Chifley Square, Sydney NSW 2000
w: www.rba.gov.au

RESERVE BANK OF AUSTRALIA

Information Management Policy

June 2025

Version Control

Version	5.0
Date	16 June 2025
Document Approver	Risk Management Committee
Document Administrator	Knowledge Management Department
Document Control ID	D16/84458
Date of Next Review	June 2028

Contents

1. Key Requirements

- The RBA has legislative obligations to that ensure our information assets are authentic, reliable and usable.
- All staff are responsible for managing their information assets on behalf of the RBA.
- All information assets must be managed using the RBA's information management principles.

2. Purpose

Information is a valuable asset that is created and used by staff in the course of their work. This policy outlines information management principles that are applied to our information assets to ensure:

- they are capable of supporting the RBA's activities and obligations; and
- staff are able to create and manage records that are authentic, reliable and usable.

This policy is a key element of the RBA's Information Governance Framework and should be read in conjunction with the Information Classification Policy and the Data Management Policy.

3. Application

3.1 Who does this policy apply to?

This policy applies to:

- employees, the Governor and Deputy Governor;
- other workers at the RBA including contractors, consultants and agency employees who occupy a position within the organisational structure of the RBA; and
- others such as those with access to information and communication technology systems (ICT Assets) of the RBA, who have been informed they are required to comply with some or all of this policy.

3.2 What does this policy apply to?

This policy applies to all information assets[1] created or used by staff in the course of their work. A record is an information asset that provides evidence relating to any function, business activity or transaction of the RBA.[2]

1 The National Archives of Australia (NAA) policy that determines the information management obligations of Australian Government agencies and our approach to information management is Building Trust in the Public Record. This policy defines information assets to include 'all records, information and data'.

2 The Australian and International Standard for Records Management – AS ISO 15489 – 2016 defines a record as: Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.

A record can be any of the following things:

- information in hard copy or digital format (e.g. a publication, spreadsheet, email or social media post);
- a container for storing information (e.g. an electronic folder);
- metadata about an information asset (e.g. a catalogue entry or administrative data relating to an information object but not the object itself).

The RBA has three different categories of record:

- Category 1 –records that the National Archives of Australia requires the RBA to keep permanently (e.g. annual reports, Board papers, papers about charter functions) and are known as 'permanent records'.
- Category 2 –records that have specified legal retention periods (e.g. financial transaction records that are required to be retained for at least seven years) and are known as 'temporary records'.
- Category 3 –records of short-term value (e.g. drafts, duplicates, cc'd emails).

3.3 Where does this policy apply?

This policy applies to all information assets created and used by staff in the following locations:

- information stored in the RBA's central repository for corporate records, Content Manager (TRIM).
- information that, for operational reasons, does not reside in TRIM but in an approved business system (e.g. MyHR) or on a network drive or internal collaborative platform (e.g. SharePoint) and is formally managed according to the principles of this policy (e.g. files that are part of workflows or system files);
- information that is created and used by staff on external partner-provided collaborative platforms (e.g. GovTEAMs Official and GovTEAMs PROTECTED).

4. Compliance

The RBA is obliged to comply with legislation and standards that specify how our information assets must be managed.[3] To meet these obligations, we have a number of information practices and controls within the Information Governance Framework, including:

- internal monitoring and reporting to various governance working groups, the Risk Management Committee and departments; and
- annual external compliance reporting to the National Archives of Australia with the findings for all government agencies reported to the responsible Minister.

3 The National Archives of Australia is the Commonwealth body responsible for managing compliance with legislation and standards. The *Archives Act 1983* is the key legislation governing RBA records.

Deliberate and material breaches of this policy will be treated as a Code of Conduct breach, or breach of relevant laws to the extent they apply. This could include dismissal in situations involving serious breaches of this policy.

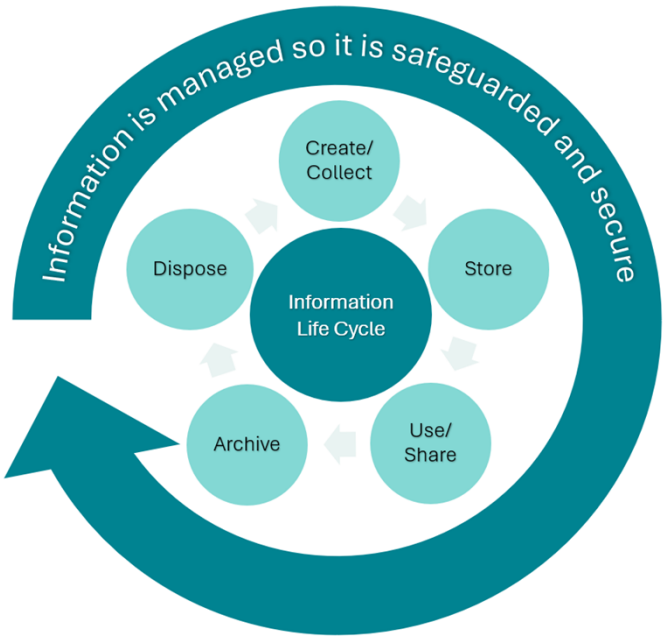
5. Managing information

5.1 Information management principles

The RBA's information assets are managed according to the following information management principles:

- Information is an asset and managed in a life cycle;
- All staff are responsible for and must manage the information they create and use;
- Only approved technologies and systems may be used to create and store information;
- Information management must meet legislative and compliance requirements;
- Information will be digital at the point of capture and/or creation;
- Information must be reliable and authentic and usable;
- Information that is AI generated must be clearly identified as 'AI Generated', with judgement exercised about its use;
- Information assets that are corporate records must be accessible in line with Commonwealth Government requirements and principles that they are be publicly available 20 years after creation; and
- Information must be safeguarded and managed in accordance with its sensitivity.

Figure 1: Life Cycle Management of Information



5.2 Roles and responsibilities

The following roles and responsibilities are involved in the management of the RBA's information assets:

Table 1: Roles and Responsibilities

Role	Responsibility
All staff (including contractors)	Managing information assets they have created or used on behalf of the RBA.
Business Information Owners (BIOs)	Being able to make decisions on managing information (including legacy information) stored on drives and in business and collaborative systems on behalf of their department.
Business System Owners	Managing the information assets contained within the systems they own.
Chief Information Governance Officer (CIGO)	Building a culture that is focussed on good information management practices. The role of the CIGO is fulfilled by the KM - Senior Manager, Information and Data Governance.
Governor, Reserve Bank of Australia	Head of agency sign-off of the National Archives of Australia annual compliance report.
Head of Department, Knowledge Management	Implementing this policy and other documents supporting the Information Governance Framework.
Information Technology Department (IT)	Provisioning of ICT devices to access information and management of those devices to prevent unauthorised access or use.
Knowledge Management Department (KM)	Providing the framework, tools and support for staff to adopt effective information management practices.
Risk Management Committee (RMC)	Approving this policy every two years.
TRIM Super Users	Providing practical guidance and assistance in information management and the use of Content Manager (TRIM) to co-workers.

6. Policy Management

6.1 Administration

This policy is administered by Knowledge Management Department.

6.2 Implementation

The Head of Knowledge Management Department is responsible for the implementation of this policy.

6.3 Monitoring and review

This policy is reviewed by Knowledge Management Department at least every three years, or more frequently if there is a major change. All changes to the policy must be approved by the Risk Management Committee.

6.4 Communication

This policy is published on the RBA's intranet and an associated e-learning module is completed annually by all staff as part of the RBA's compliance suite.

7. Resources

7.1 Related internal documents

D15/92902	Information Governance Framework
D12/89323	Information Classification Policy
D19/156142	Data Management Policy
D09/227086	Code of Conduct
Intranet	Governance Framework

7.2 Related legislation

Archives Act 1983

Freedom of Information Act 1982

Privacy Act 1988

Evidence Act 1995

Electronic Transactions Act 1999

Crimes Act 1914

Public Governance, Performance and Accountability Act 2013

Building Trust in the Public Record Policy

Information Management Standard for Australian Government

7.3 Enquiries

Contact the KM - Information Governance team with any queries.

RESERVE BANK OF AUSTRALIA

Information Classification Policy – RBA Classifications & Handling Guidelines

December 2025

Version Control

Version	3.1
Date	16 December 2025
Document Approver	Head of Department
Document Administrator	Knowledge Management Department
Document Control ID	D22/26460
Date Next Review Due	December 2028

Contents

1. Key Requirements

- All staff are responsible for ensuring that RBA-created information assets have an information security classification applied.
- All staff are responsible for handling RBA information assets according to their format and the information security classification that has been applied.
- Staff need to be aware there is **no direct equivalence** between the RBA's Information Classification Policy (ICP) and the Australian Government's Protective Security Policy Framework (PSPF).

2. Purpose

These guidelines apply to all physical and digital information assets[1] created by RBA staff and support the implementation of the RBA's ICP by:

- helping staff choose an appropriate information security classification based on the sensitivity of the information asset;
- advising staff how to handle – create, label, store, share or dispose of - an information asset according to its sensitivity and its format.

RBA staff may also be recipients of physical or digital information assets created by other government agencies:

- In the case of 'protected information', RBA staff must handle this information in accordance with the Protected Information, Protected Documents and Maintaining Confidentiality instructions.
- In the case of information assets created by staff at other Australian Government agencies, RBA staff must consult the PSPF. Staff need to be aware that there is **no direct equivalence** and therefore they should consult the PSPF – Classification and Handling Guidelines and Handling Government Information on the intranet.

3. Classifying Information

3.1 Why do we use information security classifications?

The RBA's information assets should be safeguarded, meaning they warrant special protection from unauthorised access and use. To help staff be aware of how they must handle RBA information assets, an information security classification is applied. Using information security classifications reduces the risk of unauthorised access to sensitive information while still facilitating information sharing.

3.2 What are the information security classifications?

The RBA's Information Classification Policy sets out four information security classifications: GENERAL, RESTRICTED, HIGHLY RESTRICTED and EXTREMELY RESTRICTED.

1 The National Archives of Australia (NAA) policy that determines the information management obligations of Australian Government agencies and our approach to information management is Building Trust in the Public Record. This policy defines information assets to include 'all records, information and data'.

These information security classifications apply **only** to information assets created by RBA staff.

Table 1 provides a description of each of the RBA's information security classification, explains the level of sensitivity, confirms what can be viewed according to the classification and provides examples of different information assets.

Table 1: Description of the RBA's four information security classifications

Classification	Description	Sensitivity Level[2]	Access	Examples
GENERAL	• Information that relates to the general business of the RBA and can therefore be widely distributed internally.	• Reputational or operational risks from disclosure of this information, internally or externally, is **minor**. • This classification is used as a default within departments.	• Metadata and/or content can be accessed by all RBA staff.	• Material published on the intranet • Bank-wide email communications or newsletters • Corporate policies • Corporate publications • Exchange rates
RESTRICTED	• Information that is not widely distributed for reasons of market, commercial, political or legal sensitivity.	• Reputational or operational risks from consequential disclosure of this information, internally or externally, is **moderate**. • This classification should be used in moderation.	• Access is restricted to the information owner's department or RBA staff as needed. • KM Staff in the IM Support Group.	• Employee records • Contract documents • Committee reports • Project artefacts • Budget and cost forecasts • Housing data
HIGHLY RESTRICTED	• Information that is not widely distributed for reasons of market disruption, endangering RBA staff, impact to external relationships and impeding investigations.	• Reputational or operational risk from consequential disclosure of this information, internally or externally, is **major**. • This classification is used sparingly and is decided by Assistant Governors or their delegates.	• Access is restricted to senior RBA staff who need to know. • KM staff in the Content Manager (TRIM) Secure Access Group (SAG).	• Economic forecasts and models • Monetary policy decisions prior to announcement • Market-sensitive policy advice • Security arrangements • Contentious legal matters • Floor plans and drawings of RBA facilities • Over the counter derivatives data
EXTREMELY RESTRICTED	• Information where knowledge of its existence could threaten life directly, jeopardise national interests, damage external relationships, including with other governments.	• Reputational or operational risk from disclosure of this information, internally or externally, is **significant**. • This classification is used with the utmost restraint and decided by the Governor or Deputy Governor.	• Access is restricted to senior RBA staff who need to know. • KM Staff in the Content Manager (TRIM) Administrators group.	• Details of cash distribution • Aspects of banknote security and operations

2 The sensitivity level aligns to the consequence ratings in the RBA's Risk Matrix.

Most information assets produced by RBA staff are classified GENERAL. This means staff can view the metadata and/or content of an information asset with minor risk of it causing reputational or operational damage to the RBA if the information is disclosed.

The rest of the RBA's information assets have varying degrees of sensitivity and/or need for protection and therefore are classified with a higher information security classification. When applying an information security classification, care should be taken to ensure that information is not overclassified.

Information security classifications can be accompanied by four **optional** Dissemination Limiting Markers (DLMs) that allow the user to further classify and describe content. Use of a DLM is optional and includes:

- For Official Use Only – replaces the previous 'X-in-Confidence';
- Personal – used to identify personal information that may be sensitive or requires special handling;
- Legal – used to identify information that may be legally privileged or requires special handling; and
- Commercial – used to identify information that is commercial in nature e.g. financial or market related.

A DLM can be used in conjunction with any information security classification. Whilst the information security classification is capitalised, the DLM uses title case and is separated by a colon and a space, for example RESTRICTED: For Official Use Only.

3.3 Application of information security classifications

3.3.1 Where should labels be displayed?

Information security classification labels must be displayed in the metadata of an information asset and visible on both physical and digital files, e.g. in document footers, titles, covers or in the body of emails and meeting/calendar invitations.

3.3.2 How should labels be displayed?

When an information security classification label is applied to an information asset it must be capitalised, for example HIGHLY RESTRICTED. When it is requested by a system, such as MS Purview, it must be applied.

3.3.3 How are labels applied?

(a) MS Purview

MS Purview is used to apply information security classifications to all information assets that are compatible with Microsoft applications. Staff are required to choose an information security classification, also known as a 'sensitivity label', when creating a new information asset or when working with an existing information asset that does not yet have a label.

Staff are prompted to apply a relevant 'sensitivity label' when creating, using or sending Microsoft compatible documents, emails and calendar invites as per Figure 1.

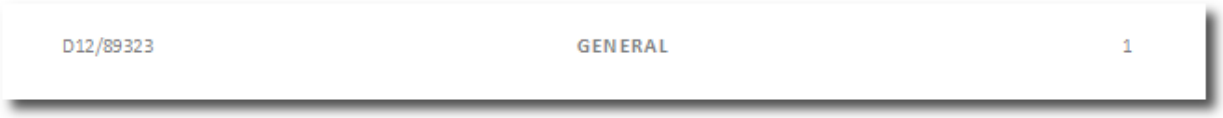
Figure 1: MS Purview Sensitivity Label Prompt

(b) Content Manager (TRIM)

For information stored in Content Manager (known as TRIM), information security classifications are applied to each folder. This means that when staff save an information asset to a folder, the information security classification of the folder is automatically applied to the information asset.

In addition, staff will also need to apply a MS Purview sensitivity label to any Microsoft compatible information assets stored in TRIM. Where the file type contains a cover page or footer, staff should ensure the sensitivity label is inserted as shown in Figure 2.

Figure 2: MS Purview Sensitivity Label in Document Footer



(c) In other repositories

For information (new and active) stored in repositories other than TRIM and that is not Microsoft Purview compatible, staff must identify the information security classification and ensure the label is visible:

- in the footer of an output from a business system e.g. reports
- in the title of a folder or file stored on a shared network G drive if it is RESTRICTED or HIGHLY RESTRICTED.

For audio recordings the information security classification should be spoken aloud at the start of the recording.

4. Handling Information

4.1 What does 'handling' information mean?

Whilst the information owner is responsible for choosing and applying an information security classification, all RBA staff are responsible for handling this information appropriately. This means that when labelling, storing, sharing or disposing of RBA information, staff need to consider the sensitivity of the information and manage it accordingly.

Most information produced by the RBA is classified GENERAL which means it can be used, shared, stored and disposed of without posing any significant risks to the RBA. However, information

classified as RESTRICTED, HIGHLY RESTRICTED and EXTREMELY RESTRICTED needs to be handled with increasing degrees of safeguarding. For example, if you print RESTRICTED information it cannot be left in the printer tray unattended because there is a risk that unauthorised access to this information could cause moderate reputational or operational damage to the RBA. It must be picked up immediately after release and used and disposed of according to Appendix B.

4.2 Handling information based on its format

Staff need to consider the format of their information and handle it accordingly. There are three formats to consider:

- electronic information assets;
- hard copy information assets; and
- removable storage devices.

Additional measures may also be required to prevent unauthorised access to information such as the use of physical security zones and/or physical security containers.

Staff should familiarise themselves with Appendices A, B or C when handling RBA information assets.

4.3 Changing information security classifications

Over the lifecycle of an information asset, its information security classification may change depending on whether it becomes more sensitive or less sensitive over time. For example, economic forecasts that are HIGHLY RESTRICTED will be declassified to GENERAL once the information is publicly available.

By their very nature, older information assets generally become less sensitive overtime and can be declassified in preparation for their potential release as part of the RBA's public access obligations.

At any time, however, the owner of an information asset should consider if the information security classification is appropriate and amend it if required. Prior to changing an information security classification, the user should confirm the change with the owner/s of the information asset.

Various tools can be used to assist with reclassifying or declassifying information assets including MS Purview Sensitivity ribbon, TRIM Security Helper or by manually updating titles of existing information assets and/or their container.

4.4 Using security zones and security containers

Security zones and security containers are managed by Workplace Department (WP). Security zones are identified in all premises owned and leased by the RBA and they provide a layer of physical protection from unauthorised or covert access to, and forcible attack on, people, physical assets and information. More information is available in the Standard for Location and Specification for Security Zones.

Security containers are used to store classified information, monetary assets and other valuables. Approved security containers are assessed based on their fitness for security purposes for Australian Government departments and agencies. More information is available in the Standard for Selection and Use of Safes and Security Containers.

5. Roles and Responsibilities

All staff are responsible for assessing the sensitivity of their information and applying an information security classification to the content. Staff are also expected to use the appropriate handling arrangements when labelling, storing, sharing and disposing of RBA information assets.

Table 2: Roles and Responsibilities

Role	Responsibility
All staff, including employees, contractors and consultants, with access to information and communications technology	• Applying information security classifications to information assets they have created or are using. • Handling information assets according to both the information security classification and the format. • Reassessing information assets and reclassifying or declassifying the information based on its current sensitivity. • Complying with all RBA policies and guidelines that provide advice on how information is handled e.g. staff cannot send RBA information to personal email accounts.
Knowledge Management Department	• Providing training, tools and support to staff so they are capable of creating and managing records well. • Ownership and technical support of the RBA's records management system, Content Manager (TRIM). • Preservation and management of the RBA's physical records stored in the Archives. • Monitors the RBA's information assets to ensure they are labelled with an information security classification and information is appropriately handled.
Information Technology Department	• Monitoring for compliance with relevant security policies and standards.
Senior Information and Data Governance Manager	• Implementing these guidelines and all related documents as part of the Information Governance Framework. • Fulfilling the role of Chief Information Governance Officer as per the National Archives requirements.
Workplace Department	• Providing staff with advice on the RBA's security zones and provisioning security containers to staff as required.

6. Guideline Management

6.1 Administration

This Guideline is administered by Knowledge Management Department.

6.2 Implementation

The Senior Manager, Information and Data Governance, Knowledge Management Department is responsible for the implementation of this guideline.

6.3 Monitoring and review

This Guideline is reviewed by Knowledge Management Department at least every three years or more frequently if there is a major change. All changes to the Guideline must be approved by Head of Knowledge Management Department.

6.4 Communication

This Guideline is published in the intranet on Policies + and referenced in online training modules.

7. Resources

7.1 Related internal documents

D12/89323	Information Classification Policy
D11/24451	Information Management Policy
D20/26538	Protective Security Policy Framework – Classifications and Handling Guidelines
D15/126367	Protective Security Framework
D19/156142	Data Management Policy
D21/355425	Risk and Compliance Management Framework
D19/406497	Metadata Management Guidelines
D14/28646	Standard for Location and Specification for Security Zones
D14/29384	Standards for Selection and Use of Safes and Security Containers
D16/429904	Protected Information, Protected Documents and Maintaining Confidentiality instructions
Intranet	Safeguarded Information (sharepoint.com)
Intranet	Classifying Information (sharepoint.com)
Intranet	Handling Bank Information (sharepoint.com)

7.2 Related external resources

Website	Protective Security Policy Framework

7.3 Enquiries

Contact KM - Information Handling with any queries regarding the application of information security classifications and how to handle both physical and digital information assets.

Contact IT Cybersecurity for questions about encryptions and security classification of systems.

Contact WP Security Operations for questions about security zones and security containers.

8. Glossary

Term	Definition
Data	Data includes the dataset level in the data inventory and at the data element level in the data catalogue.
Information assets	Information assets include all information created, received and used by the RBA, including: • information stored in the RBA's central repository for corporate records, Content Manager (Content Manager (TRIM). • information that, for operational reasons, does not reside in Content Manager (TRIM) but in an approved business system (e.g. MyHR) or on a network drive or internal collaborative platform (e.g. SharePoint) and is formally managed according to the principles of this policy (e.g. files that are part of workflows or system files); • information that is created and used by staff on external partner-provided collaborative platforms (e.g. GovTEAMs OFFICIAL)
Information owner	The information owner is the individual or department responsible for commissioning, approving, releasing and managing the content during its lifecycle. If an information asset does not have a formal business owner, the information owner is also the creator.
Protective Security Policy Framework (PSPF)	The Commonwealth Government's PSPF governs management of information issued by Commonwealth agencies. When the RBA receives or sends information classified under the PSPF (e.g. classified as PROTECTED, SECRET or TOP SECRET), the information must be managed according to the PSPF.
Corporate records	The Australian and International Standard for Records Management – AS ISO 15489 – 2016 defines a record as: Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.
Protected information	'Protected information' is a term defined in section 79A of the *Reserve Bank Act*. It means information that has not been made publicly available that has been disclosed (to the RBA) or obtained (by the RBA).
Safeguarded information	Safeguarded information is an umbrella term for all information that should be afforded special care when being handled, disseminated, stored, copied or disposed of. It is information that the RBA receives, produces or otherwise uses that is either personal, privileged, confidential, protected or government classified or a combination of these categories.

Appendix A Handling electronic information assets

Electronic information assets	Action	Information Security Classification			
		GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
Includes: • Any electronic information asset in any format, in any repository (e.g. Content Manager (TRIM), shared drives, SharePoint). Includes: ○ MS Word and PDF documents ○ Excel spreadsheets (except where treated as business systems) ○ PowerPoint presentations ○ Multimedia files (digital image, video, audio) ○ Data ○ Graphics files ○ Web files ○ Any other electronic file types • Information sent electronically by: ○ Email ○ Facsimile ○ Collaboration systems	**Storing**				
		• In authorised repository (e.g. Content Manager (TRIM) or Shared Drive).	• In authorised repository (e.g. Content Manager (TRIM) or Shared Drive).	• In authorised repository (e.g. Content Manager (TRIM) or Shared Drive).	• In authorised repository such as Content Manager (TRIM). • Contact KM - Information Handling for guidance.
	Duplication/printing/copying				
		• No restrictions.	• May only be printed/copied by or for those authorised to view the information.	• May only be printed/copied by or for those authorised to view the information.	• May only be printed/copied with permission of information owner or in accordance with agreed business processes.
	Internal Distribution				
	Email	• Use links to circulate information via email (not attachments).	• Use links to circulate information via email (not attachments) to those authorised to view the information.	• Use links to circulate information via email (not attachments) to those authorised to view the information. • Assume that emails can be read by others and avoid the inclusion of sensitive content in the body of an email.	• Contact KM - Information Handling for guidance.
	Collaborative systems (e.g. SharePoint, M365, Confluence, intranet)	• No restrictions.	• Access is limited to those authorised to view the information.	• Ensure that access is limited to those authorised to view the information. • Ensure User Access Reviews are conducted regularly to remove/add members to the access group.	• Ensure that access is limited to those authorised to view the information. • Ensure User Access Reviews are conducted regularly to remove/add members to the access group. • Ensure that EXTREMELY RESTRICTED content resides only in approved business system. • Contact KM - Information Handling for guidance.

Electronic information assets	Action	Information Security Classification			
		GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
Includes: • Any electronic information asset in any format, in any repository (e.g. Content Manager (TRIM), network drives, SharePoint). Includes: ○ MS Word and PDF documents ○ Excel spreadsheets (except where treated as business systems) ○ PowerPoint presentations ○ Multimedia files (digital image, video, audio) ○ Graphics files ○ Web files ○ Any other electronic file types • Information sent electronically by: ○ Email ○ Collaboration systems ○ Facsimile	**External distribution**				
	Email	• No restrictions.	• No restrictions on receiving or sending of emails to work email accounts. • Attachments should be PDF, if possible. • Optional – Nominate any handling requirements.	• Discuss with IT Cybersecurity the provision of encryption services for your email. • Use encrypted email channels as per exemption received. • Provide instructions for secure handling to the recipient.	• Do not email EXTREMELY RESTRICTED information. • Contact KM Information Handling for guidance.
	Facsimiles	• No restrictions.	• No restrictions on sending of facsimiles. • Optional – Nominate any handling requirements.	• Use a secure (encrypted) facsimile line. • Include the information security on the cover sheet. • Provide instructions for secure handling to the recipient.	• Do not send EXTREMELY RESTRICTED information in the body of a facsimile.
	Collaborative systems (e.g. GovTeams, RBA Box)	• No restrictions.	• No restrictions on participation. • Optional – Nominate any handling requirements	• Ensure that membership/access is appropriate for the information being shared. • Provide instructions for secure handling to participants.	• Only use a collaborative system considered by IT Cybersecurity to be appropriately secure. • Provide instructions for secure handling to participants. • Consult KM Information Handling for more guidance.
	Disposing				
		• Use the Disposal of Records under Normal Administrative Practice Guidelines.	• Use the Disposal of Records under Normal Administrative Practice Guidelines.	• Use the Disposal of Records under Normal Administrative Practice Guidelines. • Ensure that temporary or cached copies are also deleted.	• Use the Disposal of Records under Normal Administrative Practice Guidelines. • Ensure that temporary or cached copies are also deleted.

Appendix B Handling hard copy information assets

Hard copy records	Action	Information Security Classification			
		GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
Includes: • Hard copy information assets (documents, folders and objects) that are not digitised and are maintained as hard copy. • Printed copies of electronic information assets Note: *The RBA is a digital first agency. Born digital records are only to be printed as hard copy when unavoidable. Remote working arrangements are not reason enough for records marked HIGHLY RESTRICTED or EXTREMELY RESTRICTED to be printed.* • Official folders maintained by KM records staff will be marked and bear the colours corresponding to each of the security classifications: ○ GENERAL – buff ○ RESTRICTED – green ○ HIGHLY RESTRICTED – salmon ○ EXTREMELY RESTRICTED – red	**Storing (at the RBA)**				
		• No restrictions. • As needed, identify any hard copy location information in the metadata of the record in TRIM.	• Store in any lockable container. • Identify any hard copy location information in the metadata of the record in TRIM.	• Do not leave unattended. • Contact WP Security Operations for guidance. • Include a metadata entry in TRIM to identify the record and its physical location.	• Do not leave unattended. • Identify the physical location of the container in TRIM. • Include a metadata entry TRIM to identify the record and its physical location. • Contact WP Security Operations for guidance.
	Storing (when travelling or working from home)				
		• No restrictions.	• Avoid visibility to third parties.	• Take and store hard copy only when unavoidable. • Do not leave unattended. • Exercise care in physically securing records in a lockable bag, container or space.	• Take and store hard copy only when unavoidable. • Do not leave unattended. • Exercise extreme care in physically securing records in a lockable bag, container or space.
	Copying				
		• No restrictions.	• May only be copied by or for those authorised to view the information.	• May only be copied by or for those authorised to view the information. • Hard copies for distribution should be numbered and controlled (with description of hard copy distribution process recorded in TRIM).	• May only be copied with permission of information owner or in accordance with agreed business processes. • Hard copies for distribution should be numbered and controlled (with description of hard copy distribution process recorded in TRIM).

Hard copy information assets	Action	Information Security Classification			
		GENERAL	**RESTRICTED**	**HIGHLY RESTRICTED**	**EXTREMELY RESTRICTED**
Includes: • Hard copy information assets (documents, folders and objects) that are not digitised and are maintained as hard copy. • Printed copies of electronic records Note: *The RBA is a digital first agency. Born digital records are only to be printed as hard copy when unavoidable. Remote working arrangements are not reason enough for records marked HIGHLY RESTRICTED or EXTREMELY RESTRICTED to be printed.* • Official folders maintained by KM records staff will be marked and bear the colours corresponding to each of the security classifications: ○ GENERAL – buff ○ RESTRICTED – green ○ HIGHLY RESTRICTED – salmon ○ EXTREMELY RESTRICTED – red	**Internal distribution**				
		• No restrictions.	• Distribute only to those authorised to view the information.	• Hand deliver to the addressee or their delegate, in a folder or sealed non-transparent envelope. • Where multiples are distributed, they should be numbered and controlled (with description of hard copy distribution process recorded in TRIM). • Spot check audits are recommended on location/use of hard copies.	• Hand deliver in a sealed double envelope or tamper evident package directly to the addressee only. • Where multiples are distributed, they should be numbered and controlled (with description of hard copy distribution process recorded in TRIM). • Spot check audits are recommended on location/use of hard copies.
	External distribution				
		• Ensure information is directed to the intended audience.	• Ensure information is directed to the intended audience.	• Use secure courier or hand deliver in a sealed double envelope directly to the addressee. • Obtain confirmation of receipt. • Where multiples are distributed, hard copies should be numbered and controlled (with description of hard copy distribution process recorded in TRIM).	• Use a secure courier service and tamper evident device, or hand deliver in a sealed double envelope directly to the addressee (do not send by mail). • Obtain confirmation of receipt. • Where multiples are distributed, hard copies should be numbered and controlled (with description of hard copy distribution process recorded in TRIM). • Spot check audits are to be conducted on location/use of external hard copies.
	Disposing				
		• Use the Disposal of Records under Normal Administrative Practice Guidelines.	• Use the Disposal of Records under Normal Administrative Practice Guidelines.	• Use the Disposal of Records under Normal Administrative Practice Guidelines.	• Use the Disposal of Records under Normal Administrative Practice Guidelines.

Appendix C Handling Removable Storage Devices

Removable storage media	Action	Information Security Classification			
		GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
Covers the handling of physically removable storage media. Handling is relative to the level of sensitivity of the content held on the device. Devices include: • Ironkeys/USB flash drives • CDs, DVDs • Flash memory cards • Back-up tapes • Portable and removable hard drives	**Storing on RBA premises**				
		• No restriction on storing, beyond avoidance of theft or misplacement.	• Store in any lockable container.	• Ensure device is password protected or files are encrypted. • Store in an RBA authorised security container. • Contact WP Security Operations for guidance.	• Ensure device is password protected or files are encrypted. • Store in an RBA authorised security container. • Contact WP Security Operations for guidance.
	Storing outside of RBA premises				
		• No restriction on storing, beyond avoidance of theft or misplacement.	• No restriction on storing, beyond avoidance of theft or misplacement.	• Ensure device is password protected or files are encrypted. • Media must not be stored outside RBA premises without the permission of the information owner or in accordance with agreed business rules.	• Ensure device is password protected or files are encrypted. • Media must not be stored outside RBA premises without the permission of the information owner or in accordance with agreed business rules.
	Internal distribution				
		• Send via internal mail or carry by hand.	• Send via internal mail or carry by hand.	• Carry and deliver by hand. • Track and control distribution.	• Carry and deliver by hand. • Track and control distribution.

Removable storage media	Action	Information Security Classification			
		GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
Covers the handling of physically removable storage media. Handling is relative to the level of sensitivity of the content held on the device. Devices include: • Ironkeys/USB flash drives • CDs, DVDs • Flash memory cards • Back-up tapes • Portable and removable hard drives	**External distribution**				
		• Send by express/registered post, or by courier.	• Send by express/registered post, or by courier.	• When delivering in person, carry in a locked bag and hand deliver to addressee. • If sending by courier, use an approved secure courier and a tamper proof device, with instructions for the item to be opened by the addressee only. • If sending by courier, obtain confirmation of delivery. • Track and control distribution. • Optional – encrypt the device prior to carriage.	• When delivering in person, carry in a locked bag and hand deliver to addressee. • If sending by courier, use an approved secure courier and a tamper proof device, with instructions for the item to be opened by the addressee only. • Seek advice from IT Cybersecurity re encryption of the device prior to carriage. • If sending by courier, obtain confirmation of delivery. • Track and control distribution.
	Disposal				
	Removable hard drive; Ironkeys, USB and other flash drives; memory cards	• Delete information after use.	• Delete information after use.	• Reformat device after use. • Where required, destroy the device as advised by IT Service Desk.	• Reformat device after use. • Where required, destroy the device as advised by IT Service Desk.
	Optical media, including CDs, DVDs	• Disks should be shredded using KM's secure disposal service.	• Disks should be shredded using KM's secure disposal service.	• Disks should be shredded using KM's secure disposal service.	• Disks should be shredded using KM's secure disposal service.
	Back-up tapes	• Tapes should be shredded using KM's secure disposal service.	• Tapes should be shredded using KM's secure disposal service.	• Tapes should be shredded using KM's secure disposal service.	• Tapes should be shredded using KM's secure disposal service.

Classifying Information

Key understandings

- Information security classifications are labels that identify the sensitivity of an information asset.
- Using classifications reduces the risk of unauthorised access to sensitive information while still facilitating information sharing.
- All staff are responsible for ensuring the records we create or use have the classification clearly marked on the document.
- All staff are responsible for handling - creating, storing, sharing, disposing - of information according to its classification.

Need help labelling your emails and documents?

Visit Information Security Classifications (labels).

Understanding the different classifications

Safeguarded information is an umbrella term the Bank uses to describe all information that warrants special protection. It is information the Bank may receive, produce or otherwise use that is personal, privileged, confidential, protected or government classified.

Bank staff must use the Bank's information classifications as set out in the Information Classification Policy when creating information because we have not yet fully implemented the Protective Security Policy Framework (PSPF). However, Bank staff will receive and handle Australian Government classified information as part of their work activities and must handle this information according to the PSPF.

This effectively means there are two classification pathways: one for Bank information and another for Australian Government classified information. The pathway that staff need to follow depends on the source of the information they are using and its intended audience. Both pathways require the information to be safeguarded.

Pathway 1
Bank Information

Information that is created or used in the course of our work at the Bank and needs to be copied, stored, shared or disposed. To handle this information we need to refer to Handling Bank Information (sharepoint.com)

Pathway 2
Government Information

Information that is received from another government agency and needs to be carried, stored, shared, transmitted or disposed. To handle this information we need to refer to Handling Government Information (sharepoint.com).

On this page:

Get in touch

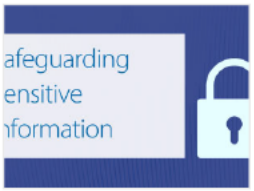
Any questions about classifying information email the KM Information Handling inbox.

Useful links

- RBA Classifications & Handling Guidelines
- PSPF Classifications & Handling Guidelines
- Safeguarded Information
- Protected Information
- Standard for Location and Specification of Security Zones
- Standard for Selection and Use of Safes and Security Containers

News

+ Add



News

Safeguarding Sensitive Information: Start the new year right

As we enter the new year, take a moment to refresh your understanding of the sensitive information you handle.

News

Information safeguarding starts with you

Everyone at the RBA is required to manage information well and safeguard it from unauthorised access or introduced vulnerabilities. Learn more here.

News

Understanding information security classifications

Learn more about the RBA's new information security classifications and how to use them here.

News

Collaborating securely

Learn more about the RBA's collaboration tools and how to collaborate securely here.

Key understandings

- Information security classifications are displayed on Bank documents to indicate the sensitivity of the information.
- Using classifications reduces the risk of unauthorised access to sensitive information while still facilitating information sharing.
- All staff are responsible for ensuring the records we create or use have the classification clearly marked on the document.
- All staff are responsible for handling - creating, storing, sharing, disposing - of information according to its classification.
- The RBA Classifications & Handling Guidelines are complemented by physical containers and zones.

When handling Bank information staff are expected to comply with their obligations in regards to safeguarded information as well as the Code of Conduct and Information Systems Security and Acceptable Use Policy.

Understanding information security classifications

Expand All

What are information security classifications?

The Bank's information assets are safeguarded, meaning they warrant special protection from unauthorised access and use.

Information security classifications are labels identifying the level of sensitivity of an information asset. The classification levels indicate:

- how sensitive the information is
- precautions to take before accessing or sharing the information asset
- how that particular information asset should be handled - stored, shared or disposed - in order to reduce the risk of unauthorised access.

What information should be classified?

All information assets created and used by the Bank should have a classification. Information assets can be stored:

- in TRIM as an electronic or paper record
- on shared network drives
- in collaborative systems
- on removable storage media or
- as outputs from business systems.

What are the classification levels?

Classification	Description	Examples
GENERAL	Information that relates to the general business of the RBA and can therefore be widely distributed internally. Reputational or operational risks from disclosure of this information, internally or externally, is minor. Metadata and/or content can be accessed by all staff. Most information is classified GENERAL as a default.	• articles published on the intranet • Bank-wide email communications or newsletters • corporate policies • staff appointments or movements • routine enquiries or requests sent to a service desk

Classification	Description	Examples
		• exchange rates
RESTRICTED	Information that is not widely distributed for reasons of market, commercial, political or legal sensitivity. Reputational or operational risks from consequential disclosure of this information, internally or externally, is moderate. Access is restricted to those who need work directly with it and KM records staff. This classification is used in moderation.	• employee records • contracts • committee reports • sensitive analytical notes • project artefacts • budget and cost forecasts • housing data
HIGHLY RESTRICTED	Information that is not widely distributed for reasons of market disruption, endangering RBA staff, impact to external relationships and impeding investigations. Access is confined to those who work directly with the information and KM records staff in the TRIM Secure Access Group (SAG). This classification is used sparingly; decided by Assistant Governors or their delegates.	• economic forecasts and models • monetary policy decisions prior to public announcement • market-sensitive policyadvice • security arrangements • contentious legal matters • floor plans and drawings of RBA facilities • over the counter derivatives data
EXTREMELY RESTRICTED	Information where knowledge of its existence could threaten life directly, jeopardise national interests, damage external relationships, including with other governments.	• details of cash distribution

Classification	Description	Examples
	Access is restricted to senior RBA staff who need to know. This classification is used with the utmost restraint and decided by the Governor or Deputy Governor.	• aspects of banknote security and operations

The Bank also sometimes receives sensitive information from other government agencies that is classified according to the Protective Security Framework Policy with levels: PROTECTED, SECRET and TOP SECRET.

Only those with government security clearance corresponding to the security classification of the information can handle government classified information.

Government information that is not sensitive is generally marked as OFFICIAL.

If you handle Government classified information refer to the Guidelines for Handling Government Information or contact KM-Information Governance team with any questions..

How do I apply classification labels?

Choose one of the four security levels to best describe the sensitivity of your information. The classification should be clearly associated with the information and:

- Clearly visible in the footers of all Bank documents (Word, PowerPoint, Excel)
- Recorded in the metadata about the record

When creating infomation assets using Microsoft applications, staff are prompted to choose a classification by the MS Purview labelling tool. Using the MS Purview tool, staff are prompted to choose a 'sensitivity label'.

For information assets stored in TRIM they automatically inherit a classification form the TRIM folder they are stored in. This applies to all information assets that were created:

- prior to the introduction of MS Purview labelling tool (pre September 2024) or
- created using non-Microsoft applications,

For information stored in repositories other than TRIM, staff must choose an information security classification and ensure the marker is visible:

- in the footer of a an output from a business system e.g. reports
- on the cover page of a presentation e.g. PowerPoint or
- in the title of a folder or file stored on a network drive if it is RESTRICTED or HIGHLY RESTRICTED

For audio recordings and meeting transcripts the information security classification should be spoken aloud at the start of the recording.

The KM-Information Handling team can help you with questions about classifying information.

How should I handle classified information?

Information should be handled according to the classification that has been assigned to it and in line with the instructions outlined in RBA Classifications & Handling Guidelines. If you are unsure about the classification of an information asset contact the information owner.

Information classified as GENERAL can be used freely by Bank staff in the course of their daily work but a few common sense controls apply:

- TRIM links should always be used to email or circulate records internally to minimise the risk of accidental disclosure.

Information classified as RESTRICTED should have the following additional controls applied to its handling and use:

- Access to the digital information should be restricted to only those that require access to view the record.
- Access to physical copies should be controlled by ensuring copies are not left unattended at work, visible during transit or working from home.
- TRIM links should be used to circulate the information via email.
- The information should only be distributed to those authorised to view the record and in consultation with the information owner (particularly if being shared externally).

Information classified as HIGHLY RESTRICTED or EXTREMELY RESTRICTED requires specialised handling considerations. Refer to RBA Classifications & Handling Guidelines for more information or speak to a member of the KM-Information Handling team.

Can I change the classification of information?

Yes. The classification of information often changes over the course of the life of a record. For example, something that was HIGHLY RESTRICTED and embargoed due to sensitive economic forecasts might become GENERAL once the information is publicly available.

Various tools can be used to assist with reclassifying or declassifying information assets including MS Purview Sensitivity ribbon, TRIM Security Helper or by manually updating titles of existing information assets and/or their container.

Changes in classification should always be done in consultation with the owner of the information.

Which policies and guidelines should I be aware of? +

These policies and guidelines provide specific advice about how information is to be stored, copied, distributed internally and externally and disposed of once it is no longer of value.

Information Classification Policy

Ensures that the Bank's information assets are identified by their level of sensitivity and managed accordingly. The risk of unauthorised access to information can be reduced while facilitating information sharing.

As well as needing to comply with this policy for internal information we need to adhere to the Protective Security Policy Framework when handling Australian government information.

RBA Classifications & Handling Guidelines

The RBA Classifications & Handling Guidelines are designed to give staff practical guidance when they make decisions about how to create, store, copy, distribute or dispose of Bank information.

These decisions vary according to the medium of the information and its level of sensitivity. The RBA Classifications & Handling Guidelines are complemented by descriptions of physical containers and zones in the building along with supporting policies and services.

PSPF Classifications & Handling Guidelines

Australian Government information is managed under the Protective Security Policy Framework (PSPF). The Bank is required to adhere to the PSPF when it receives or handles classified information from other Australian Government agencies. The PSPF Classifications & Handling Guidelines give staff practical guidance on how to store, copy, distribute or dispose of Government information.

Where can I get help? +

For more help on information classification contact KM-Information Handling team.

Handling electronic records

Expand All

Types of electronic record —

Electronic Records include:

- Any electronic record in any format, in any repository (e.g. TRIM, network drives, SharePoint). Includes:
  - MS Word and PDF documents
  - Excel spreadsheets (except where treated as business systems)
  - PowerPoint presentations
  - Multimedia files (digital image, video, audio)
  - Data
  - Graphics files
  - Web files
  - Any other electronic file types
- Information sent electronically by:
  - Email
  - Facsimile

- Collaboration systems

Storing electronic records

GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
• In authorised repository (e.g. TRIM or shared drive).	• In authorised repository (e.g. TRIM or shared drive).	• In authorised repository (e.g. TRIM or shared drive).	• In authorised repository (e.g. TRIM). • Contact KM - Information Handling for guidance.

Duplication, printing, copying of electronic records

GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
• No restrictions.	• May only be printed/copied by or for those authorised to view the record.	• May only be printed/copied by or for those authorised to view the records.	• May only be printed/copied with permission of information owner or in accordance with agreed business processes.

Internal distribution of electronic records via email or collaborative systems

GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
Email			
• Use links to circulate information via email (not attachments).	• Use links to circulate information via email (not attachments).	• Use links to circulate information via email (not attachments) to those authorised to view the record. • Assume that emails can be read by others and avoid the inclusion of sensitive content in the body of an email.	• Contact KM - Information Handling for guidance.
Collaborative systems (e.g. SharePoint, M365, Confluence, Intranet)			
• No restrictions.	• Ensure that access is limited to those authorised to view the information.	• Ensure that access is limited to those authorised to view the information. • Ensure User Access Reviews are conducted regularly to remove/add members to the access group.	• Ensure that access is limited to those authorised to view the information. • Ensure User Access Reviews are conducted regularly to remove/add members to the access group. • Ensure that EXTREMEY RESTRICTED content resides only in approved business systems.

			• Contact KM - Information Handling for guidance.

External distribution of electronic records via email, facsimiles or collaborative systems +

GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
Email			
• No restrictions.	• No restrictions on receiving or sending of emails to work email accounts. • Attachments should be PDF if possible. • Optional – Nominate any handling requirements.	• Discuss with IT Cybersecurity the provision of encryption services for your email. • Discuss with KM - Information Handling using RBA Box for emails with attachment/s. • Provide instructions for secure handling to the recipient.	• Do not email EXTREMELY RESTRICTED information. • Contact KM - Information Handling for guidance.
Facsimiles			
• No restrictions.	• No restrictions on sending of facsimiles. • Optional – Nominate any handling requirements.	• Use a secure (encrypted) facsimile line. • Include the information security classification on the cover sheet. • Provide instructions for secure handling to the recipient.	• Do not send EXTREMELY RESTRICTED information in the body of a facsimile.
Collaborative systems (e.g. RBA Box)			
• No restrictions.	• No restrictions on participation. • Optional – Nominate any handling requirements.	• Ensure that membership/access is appropriate for the information being shared. • Provide instructions for secure handling to participants.	• Only use a collaborative system considered by IT Cybersecurity to be appropriately secure. • Provide instructions for secure handling to participants.

			• Contact KM - Information Handling for guidance.

Disposing of electronic records +

GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
• Use the Disposal of Records under Normal Administrative Practice Guidelines.	• Use the Disposal of Records under Normal Administrative Practice Guidelines.	• Use the Disposal of Records under Normal Administrative Practice Guidelines. • Ensure that temporary or cached copies are also deleted.	• Use the Disposal of Records under Normal Administrative Practice Guidelines. • Ensure that temporary or cached copies are also deleted.

Handling paper records

Expand All

Types of paper record —

Paper records include documents, folders and objects that are maintained as hardcopy.

Note: The Bank is a digital first agency. Born digital records are only to be printed as hardcopy when unavoidable. Remote working arrangements are not reason enough for records marked HIGHLY RESTRICTED or EXTREMELY RESTRICED to be printed.

Official folders maintained by KM records staff will be marked and bear the colours corresponding to each of the security classifications.

Storing paper records (at the Bank) +

GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
• No restrictions. • As needed, identify any hard copy location information in the metadata of the record in TRIM.	• Store in any lockable container. • Identify any hard copy location information in the metadata of the record in TRIM.	• Do not leave unattended. • Contact WP Security Operations for guidance. • Include a metadata entry in TRIM to identify the record and its physical location.	• Do not leave unattended. • Identify the physical location of the container in TRIM. • Include a metadata entry TRIM to identify the record and its physical location. • Contact WP Security Operations for guidance.

Storing paper records (when travelling or working from home) +

GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
• No restrictions.	• Avoid visibility to third parties.	• Take and store hard copy only when unavoidable. • Do not leave unattended. • Exercise care in physically securing records in a lockable bag, container or space.	• Take and store hard copy only when unavoidable. • Do not leave unattended. • Exercise extreme care in physically securing records in a lockable bag, container or space.

Copying paper records +

GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
• No restrictions.	• May only be copied by or for those authorised to view the information.	• May only be copied by or for those authorised to view the information. • Hard copies for distribution should be numbered and controlled (with description of hardcopy distribution process recorded in TRIM).	• May only be copied with permission of information owner or in accordance with agreed business processes. • Hard copies for distribution should be numbered and controlled (with description of hardcopy distribution process recorded in TRIM).

Internal distribution of paper records +

GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
• No restrictions.	• Distribute only to those authorised to view the information.	• Hand deliver to the addressee or their delegate, in a folder or sealed non-transparent envelope. • Where multiples are distributed, they should be numbered and controlled (with description of hard copy distribution process recorded in TRIM). • Spot check audits are recommended on location/use of hard copies.	• Hand deliver in a sealed double envelope or tamper evident package directly to the addressee only. • Where multiples are distributed, they should be numbered and controlled (with description of hard copy distribution process recorded in TRIM). • Spot check audits are recommended on location/use of hard copies.

External distribution of paper records +

GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
• Ensure information is directed to the intended audience.	• Ensure information is directed to the intended audience.	• Use secure courier or hand deliver in a sealed double envelope directly to the addressee. • Obtain confirmation of receipt. • Where multiples are distributed, hard copies should be numbered and controlled (with description of hard copy distribution process recorded in TRIM).	• Use a secure courier service and tamper evident device, or hand deliver in a sealed double envelope directly to the addressee (do not send by mail). • Obtain confirmation of receipt. • Where multiples are distributed, hard copies should be numbered and controlled (with description of hard copy distribution process recorded in TRIM). • Spot check audits are to be conducted on location/use of external hard copies.

Disposing of paper records +

GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
• Use the Disposal of Records under Normal Administrative Practice Guidelines.	• Use the Disposal of Records under Normal Administrative Practice Guidelines.	• Use the Disposal of Records under Normal Administrative Practice Guidelines.	• Use the Disposal of Records under Normal Administrative Practice Guidelines.

Handling removable storage media

Expand All

Types of removable storage media

Covers the handling of physically removable storage media. Handling is relative to the level of sensitivity of the content held on the device.

Devices include:

- Ironkeys/USB flash drives
- CDs, DVDs
- Flash memory cards
- Back-up tapes
- Portable and removable hard drives

Storing removable devices on Bank premises

GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
• No restriction on storing, beyond avoidance of theft or misplacement.	• Store in a lockable container.	• Ensure device is password protected or files are encrypted. • Store in an RBA authorised security container. • Contact WP Security Operations for guidance.	• Ensure device is password protected or files are encrypted. • Store in an RBA authorised security container. • Contact WP Security Operations for guidance.

Storing removable devices outside of Bank premises

GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
• No restriction on storing, beyond avoidance of theft or misplacement.	• No restriction on storing, beyond avoidance of theft or misplacement.	• Ensure device is password protected or files are encrypted. • Media **must not** be stored outside Bank premises without the permission of the information owner or in accordance with agreed business rules.	• Ensure device is password protected or files are encrypted. • Media **must not** be stored outside Bank premises without the permission of the information owner or in accordance with agreed business rules.

Internal distribution of removable devices

GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
• Send via internal mail or carry by hand.	• Send via internal mail or carry by hand.	• Carry and deliver by hand. • Track and control distribution.	• Carry and deliver by hand. • Track and control distribution.

External distribution of removable devices

GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
• Send by express/registered post, or by courier.	• Send by express/registered post, or by courier.	• When delivering in person, carry in a locked bag and hand deliver to addressee. • If sending by courier, use an approved secure courier and a tamper proof device, with instructions for the item to be opened by the addressee only. • If sending by courier, obtain confirmation of delivery. • Track and control distribution. • Optional – encrypt the device prior to carriage.	• When delivering in person, carry in a locked bag and hand deliver to addressee. • If sending by courier, use an approved secure courier and a tamper proof device, with instructions for the item to be opened by the addressee only. • Seek advice from IT Cybersecurityy re encryption of the device prior to carriage. • If sending by courier, obtain confirmation of delivery. • Track and control distribution.

Disposing of removable devices +

GENERAL	RESTRICTED	HIGHLY RESTRICTED	EXTREMELY RESTRICTED
Removable hard drive; Ironkeys, USB and other flash drives; memory cards			
• Delete information after use.	• Delete information after use.	• Reformat device after use. • Where required, destroy the device as advised by IT Service Desk.	• Reformat device after use. • Where required, destroy the device as advised by IT Service Desk.
Optical media, including CD Roms, DVDs)			
• Disks to be shredded using KM's secure disposal service.	• Disks to be shredded using KM's secure disposal service.	• Disks to be shredded using KM's secure disposal service.	• Disks to be shredded using KM's secure disposal service.
Back-up tapes			
• Tapes to be shredded using KM's secure disposal service.	• Tapes to be shredded using KM's secure disposal service.	• Tapes to be shredded using KM's secure disposal service.	• Tapes to be shredded using KM's secure disposal service.

Bank Security Zones

Security Zones, which are outlined in the Australian Government's physical security management guidelines, are nominated areas with a mix of security countermeasures that provide a layer of protection from unauthorised access or forcible attacks.

The RBA's Head Office is currently not aligned with the PSPF for physical security owing to features of the building that we temporarily occupy. Consequently, staff should consult the Location and Specification for Security Zones and liaise with Workplace Security Operations regarding their need for security zones.

Security Containers

Security containers provide a high level of tamper evidence of covert attack and significant delay from surreptitious attack, but limited protection from forcible attack. SCEC (Security Construction Equipment Committee, an interdepartmental standing committee that reports to the Attorney-General's Department) approved containers have been assessed based on their fitness for security purposes for Australian Government departments and agencies.

Lockable containers – Compared with safes and SCEC-approved security containers, lockable containers provide a low level of security and should be used to store information and assets of a relatively low-risk nature only.

Staff should consult the Selection and Use of Safes and Security Containers and liaise with Workplace Security Operations regarding their need for security containers.

On this page:

- Handling physical records
- Handling removable storage media
- Bank Security Zones
- Security Containers

Get in touch

Any questions about classifying information email the KM Information Handling inbox.

Useful links

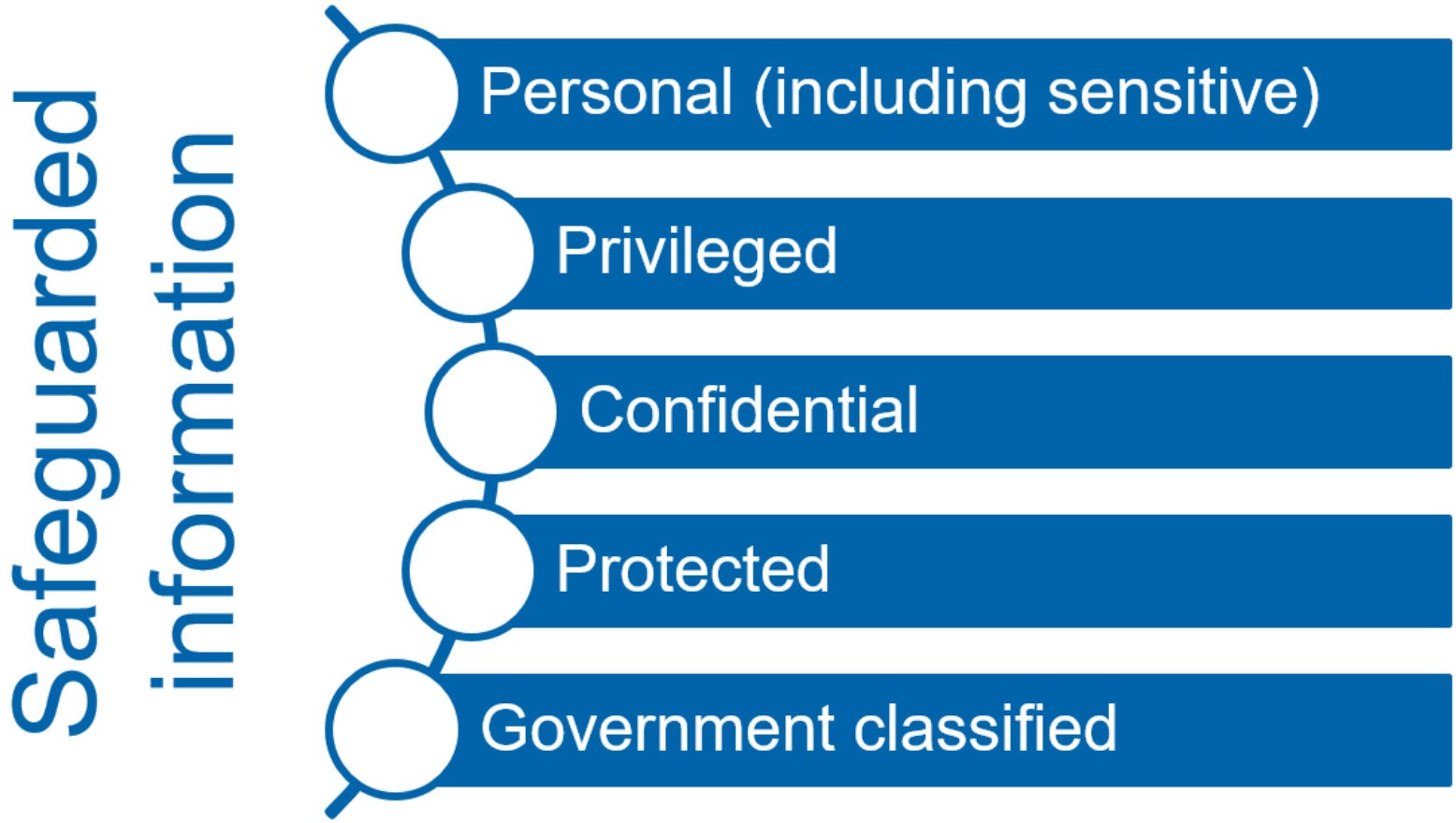
- RBA Classifications & Handling Guidelines
- PSPF Classifications & Handling Guidelines
- Managing Corporate Records

Overview

Safeguarded information is an umbrella term for all information that warrants special protection at the Bank.

> *Safeguarded information is information that should be afforded special care when being handled, disseminated, stored, copied or disposed of. It is information that the RBA receives, produces or otherwise uses that is personal, privileged, confidential, protected or government classified.*

Information may fall within more than one of the component categories.



Visual depiction of categories of information that require safeguarding

Personal Information

Definition

Personal information is any information or an opinion about an identified individual, or an individual who is

Examples

An individual's name, signature, address, telephone number, date of birth, bank account details,

reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.

employment details and commentary or opinion about a person.

Such records can be found in a wide range of Bank records including employee records, booking information, survey information, mailing lists and records relating to account signatories.

For a more comprehensive listing see the Personal Information Records Register.

Personal Sensitive Information

Definition

Personal sensitive information is a subset of personal information which has additional protection under the Privacy Act (for example, you need consent from the relevant individual to collect this information).

Examples

Information or an opinion about an identifiable individual's:

- racial or ethnic origin
- political opinions
- membership of a political association
- religious beliefs or affiliations
- philosophical beliefs
- membership of a professional or trade association
- membership of a trade union
- sexual orientation or practices
- criminal record or

- health, genetics and biometrics.

This information is most likely to be found in employee records, but will also be contained in other records (for example, dietary information in event booking records, biometric information held for security or access purposes and photographs taken for a variety of purposes).

(Legally) Privileged Information

Definition

Confidential communications and confidential documents made or exchanged between a lawyer (including an in-house lawyer) and a client for the dominant purpose of the lawyer providing legal advice or professional legal services to the client, or for use in current or anticipated litigation.

Examples

- Advice from Legal Section.
- Advice from a firm of solicitors or from a barrister.

Confidential Information

Definition

Examples

Information that Bank staff have an obligation not to disclose. This obligation may arise under the law, under a contract, under a Bank policy or because the information was obtained in other circumstances importing an obligation of confidence. Confidential information may be:

- confidential to the Bank, that is, not generally available outside of the Bank;
- confidential to a third party, that is, not generally available outside of that third party.

All Bank records that staff are not authorised to share or disclose outside the Bank, or which are only authorised to be shared or disclosed outside the Bank in specific or limited circumstances.

These include (but are not confined to) operational and security records, commercial agreements, analytical notes, embargoed information, committee papers, policy papers for the Bank's Boards and information that is not in the public domain supplied by government agency customers of Banking applicants for RITS membership or suppliers.

Protected Information

Definition

Protected information is a term defined in legislation and has a meaning in law. Protected information is defined differently in different Acts.

The protected information Bank staff are exposed to most commonly is:

- Protected relative to s79A of the Reserve Bank Act; and
- Protected relative to the s56 of the APRA Act.

The same term is also used in multiple other acts, which should be consulted depending on the context in which the term is used.

Protected documents are those that contain ‘protected information’.

Note: There is also a PROTECTED PSPF Government classification. See Handling Government Information for more information.

Application

Section 79A(2) of the Act states that a person who is an officer must not, unless permitted by section 79A of that Act, disclose any protected information or a protected document acquired by them in the course of their duties as an officer including to a court.

There are serious consequences including a potential prison term of up to two years for unauthorised disclosure of protected information and protected documents. Protected Information, Protected Documents and Maintaining Confidentiality instructions outlines the obligations of staff who have access to protected information and protected documents.

Circumstances allowing for disclosure of protected information outside the RBA

Disclosure of protected information and protected documents outside the RBA is only permitted for particular purposes or to particular categories of people. Refer to Sections 5, 6 and 7 of the Protected Information, Protected Documents and Maintaining Confidentiality instructions.

Senior Managers or above must approve disclosure of protected information or a protected document.

Consents for disclosure must be documented and recorded in a register maintained by the department or group. Use the Register template for this purpose.

Examples

Protected relative to s79A of the Reserve Bank Act

Protected information is a term defined in section 79A of the Reserve Bank Act. It means information that has not been made publicly available that has been disclosed (to the Bank) or obtained (by the Bank):

1. under or for the purposes of:
    a. the *Reserve Bank Act 1959*, the *Banking Act 1959,* the *Payment Systems (Regulation) Act 1998*, the *Payment Systems and Netting Act 1998* or the repealed Banks (Shareholdings) Act 1972; and
    b. that relates to the affairs of:
        i. a financial institution;
        ii. a body corporate that has at any time been, or is, related to a financial institution; or
        iii. a customer or proposed customer of a financial institution;
2. under or for the purposes of the performance or exercise of the Bank's functions or powers under Part 7.3 of the *Corporations Act 2001* dealing with licensing and regulation of clearing and settlement (CS) facilities; or
3. under or for the purposes of the performance or exercise of the Bank's functions or powers under Part 7.5A of the Corporations Act dealing with licensing and regulation of derivative trade repositories.

Protected relative to **s79A of the Reserve Bank Act** examples include:

- securitisations data required by the Bank to be reported to it in respect of asset backed securities;
- information collected by the Bank relating to payment system participants or their customers (such as through a payments survey or a consultation process)
- information provided by a CS facility licensee for the purpose of the Bank assessing compliance by that licensee with the Financial Stability Standards set by the Bank; and
- information collected about a CS facility licensee through participation in a supervisory cooperative arrangement for the CS facility licensee.

See the Protected Information, Protected Documents and Maintaining Confidentiality Instructions.

In general, if information is lawfully in the public domain from other sources (that is, it is readily available to others, either free or for a reasonable fee), it is 'publicly available' and therefore not protected information.

Disclosure of protected information or protected documents is only permitted under section 79A of the Reserve Bank Act for particular purposes or to particular categories of people and organisations.

Protected relative to s56 of the APRA Act

Information collected by the Australian Prudential Regulation Authority (APRA) under any one of a broad range of 'prudential regulation framework laws' including the *APRA Act 1998*, the Banking Act and the *Financial Sector (Collection of Data) Act 2001* (FSCOD Act).

When you are handling protected information or protected documents the Bank receives from APRA (for example, data used in the production of the systemic impact analysis), you must comply with section 56 of the APRA Act in addition to complying with s79A of the Reserve Bank Act.

Examples

Protected relative to **s56 of the APRA Act** examples include:

- Information collected by APRA under section 9 or 13 of the FSCOD Act and provided to the Bank.
- This includes, but is not limited to, SAFFI data.

Do these obligations apply to all staff?

The instructions apply if you:

- are a staff member of the Bank,
- occupy a position (whether as a contractor, consultant, agency staff, secondee or otherwise) within the organisational structure of the Bank,
- have access to the information and communications technology systems (ICT Assets) of the Bank and we have informed you that you are required to comply with these instructions.

If you are one of these people and because of your employment or engagement with the Bank, or in the course of that employment or engagement, you have or acquire protected information or protected documents then you are an officer to whom the important restrictions on disclosure of protected information and protected documents set out in the *Reserve Bank Act 1959* and in these instructions apply.

To help you determine your obligations check the other requirements section of your position description.

Government Classified Information

Definition

Information shared with the Bank by another Australian Government Agency, that has already been classified by that Government Agency as PROTECTED, SECRET or TOP SECRET, or is marked as having other special handling requirements.

Examples

Information shared with the Bank by an other government agency, that already carries a classification or other special handling marker.

Examples could include: Treasury briefings, intelligence and security operations details, information on

- TOP SECRET: Catastrophic business impact. Exceptionally grave damage to the national interest, organisations or individuals.
- SECRET: Extreme business impact. Serious damage to the national interest, organisations or individuals.
- PROTECTED: High business impact. Damage to the national interest, organisations or individuals.
- OFFICIAL: Sensitive: Low to medium business impact. Limited damage to an individual, organisation or government generally if compromised.
- OFFICIAL: Low business impact. No or insignificant damage. This is the majority of routine information.
- UNOFFICIAL: No business impact and no damage. This information does not form part of official duty.

management of counterfeit currency, prosecution of counterfeit currency related crimes, etc

See the Handling Government Information page.

On this page:

Get in touch

Any questions about safeguarding our information email the KM Information Handling inbox.

Any specific questions about protected information or protected documents please reach out to the Bank's Compliance team.

Useful links

- Creating and Managing Corporate Records
- Handling Bank Information
- Handling Government Classified Information
- Protected Information, Protected Documents and Maintaining Confidentiality Instructions