The Records Management Assessment Tool (RMAT) enables NSW public offices to assess the maturity of records and information management in their organisation, or a part of the organisation (e.g. business unit or information system), or a group of public offices.

The questions in this assessment focus on the management of records, information and data in NSW public offices, and how these practices align with requirements in the *State Records Act 1998* and the standards issued under the Act. They highlight the links between records management and regulations for cyber security, privacy, data sharing, open data and information access (GIPAA). The results can be used for reporting on current status; planning for improvement; justifying investment and measuring progress.

|  |  |
| --- | --- |
| Introduction | Completing the Questions |
| Records Management Assessment Tool (RMAT) is a key part of State Records NSW’s regulatory framework allowing:* Public offices to self-assess and report their alignment with the regulatory framework.
* Public offices to identify areas for improvement; and possibly support a business case.
* State Records NSW to have an overview of regulatory alignment across the sector.
* State Records NSW to identify trends or key issues for targeted intervention, to support planning and the allocation of resources.

The results can be used for reporting on current status, planning for improvement, justifying investment and measuring progress.This Assessment Tool is also available in MS Excel spreadsheet format, which includes support for automated scoring and results graphs.If you have queries about the RMAT, please contact State Records NSW on govrec@staterecords.nsw.gov.au  | 1. Complete the assessment details on the next page.
2. Then complete each question on the following pages. For each question:
* Choose one response, which best describes your current situation. The number in brackets indicates how many points apply when scoring this response. e.g. (1)
* Look at the types of evidence required to demonstrate this level of maturity, and ensure you can justify the response you’ve chosen.
* Refer to some of the Guidance material if you need more help understanding the requirements, or for considering your next steps to improve maturity in this area.

We recommend that the questions should be completed by the person/team responsible for overseeing records and information management, or in collaboration with key staff, such as a system owner, data custodian or business manager.The assessment includes some technical terms that may require explanation from a records professional (or reference to the [Glossary of Recordkeeping Terms](https://staterecords.nsw.gov.au/recordkeeping/resources/glossary-recordkeeping-terms)) if the questions are being answered by a system owner, data custodian or business manager.Detailed instructions for the assessment are provided in a separate document. |

| Overview: Records and information management actions |
| --- |
| Q.1 Has your organisation identified high risk and high value areas of business and the systems, records and information needed to support these business areas?  |
| Q.2 Are the information risks that could impact high risk and high value areas of business identified and addressed? |
| Q.3 Is records and information management the responsibility of senior management, who provide direction and support, in accordance with business requirements, relevant laws & regulations? |
| Q.4 Is there a defined strategic direction for records and information management, aligned with the goals of broader organisational strategy? |
| Q.5 Does the organisation have an up-to-date, approved and communicated policy for records and information management? |
| Q.6 Are staff across the organisation aware of their records and information management responsibilities? |
| Q.7 Is the organisation's information management capability and capacity sufficient to support and develop good information management? |
| Q.8 Are partners, contractors and other external parties aware of their responsibilities for records and information management? |
| Q.9 Does your organisation monitor the performance of records and information management? |
| Q.10 Do security and access controls protect digital and hard copy records and information from unauthorised or unlawful access, destruction, loss, deletion or alteration? |
| Q.11 How easy is it for staff and contractors to find the information and records they are looking for? |
| Q.12 Are the business needs and user expectations for information being met, in terms of strategic importance, quality and availability? |
| Q.13 How usable and re-usable is the information being created or collected by the organisation, both now and in the future? |
| Q.14 How are records and information requirements addressed in the design and management of IT systems and services for the organisation? |
| Q.15 Are records and appropriate metadata created, collected and captured across the organisation? |
| Q.16 Has the organisation considered how best to store its digital and hard copy records and information? |
| Q.17 Has the organisation identified the records and information required to meet short, medium and long term needs, so they can be effectively managed throughout their "lifetime"? |
| Q.18 Has the organisation considered requirements to transfer records and information? |
| Q.19 Has the organisation made Access Directions to enable public access to the State records for which it is responsible? |

# ASSESSMENT DETAILS / TITLE PAGE

|  |  |  |
| --- | --- | --- |
| Assessment Details | Responses | Guidance Notes |
| Date of Assessment: | e.g. 5 July 2021 | Date when this assessment is completed. |
| Cluster: | e.g. Premier and Cabinet  | Enter the Cluster for this public office.Enter "Councils" for local government or “Universities” for a university. |
| Public Office: | e.g. NSW Electoral Commission | Enter the name of public office responsible for this assessment. |
| Business Units or Information Systems: | [Free text] | Where only part of a public office is being assessed, list the business units or information systems included in the assessment. Please leave the box blank if this does not apply. |
| Other Public Offices: | [Free text] | List any other public offices included in the assessment. Please leave the box blank if this does not apply. |
| Contact name: | [Free text] | Name of the public office employee responsible for this assessment |
| Role/job title: | [Free text] | Position and title of the person completing this assessment. |
| Email: | [Free text] | Email address of the person completing this assessment. |
| External assessor: | [Free text] | Name, organisation and title of a consultant or other external person completing this assessment. Please leave the box blank if this does not apply. |
| Assessment approach: | [Free text] | Techniques used to complete the assessment. For example: workshops, interviews, meetings, document analysis. |
| Organisation context:(optional) | [Free text] | Information about the organisation's operating environment, where relevant to the assessment. For example:No. of sites, staff, business units/statutory authorities or Ministers covered by the assessment.Types of services the organisation delivers (e.g. corporate, citizen services).Records and information environment. (e.g. primarily paper, digital, hybrid; off-site storage; primary software or systems).Other key legislation impacting records, information and data management (e.g. Environmental Planning & Assessment Act). |

|  |
| --- |
| RIM ACTION 1: HIGH RISK / HIGH VALUE BUSINESS AND SYSTEMSHas your organisation identified high risk and high value areas of business and the systems, records and information (referred to as information assets) needed to support these business areas?HOW THIS ACTION SUPPORTS THE DEVELOPMENT OF RECORDS AND INFORMATION MANAGEMENT MATURITY:**Principle 2**: Records and information management support businessThe core role of records and information management is to ensure the creation, maintenance, useability and sustainability of the records and information needed for short- and long-term business operations. (*Standard on records management* requirements 2.2)**Asset Governance:** With good leadership and management, Information Asset management policies and other instruments will be effectively implemented and used. |
| Responses (points) (tick one response that applies) | Examples of evidence to justify your response | Key guidance about this topic |
| [ ]  There is no identification of the information assets needed to support high risk / high value areas of business. (1) | [ ]  Documents identifying high risk and high value areas of business and systems.e.g. risk registers; cyber security plans; business continuity plans; audit reports; IT plans; open data plans; information asset register. | 1. [Identifying and managing high value and high-risk records, information and data](https://staterecords.nsw.gov.au/recordkeeping/identifying-and-managing-high-value-and-high-risk-records-information-and-data)
2. [Identifying information risks that might be impacting on high-risk business](https://staterecords.nsw.gov.au/recordkeeping/identifying-information-risks-might-be-impacting-high-risk-business)
 |
| [ ]  There is some identification of the information assets needed to support high risk / high value areas of business - but the organisation does not have a complete, single view (e.g. different information assets identified in various plans or registers). (2) |  |  |
| [ ]  The organisation has formally identified its high risk / high value information assets. There is a complete, single view of high risk / high value information assets (e.g. in a specific document, spreadsheet, or register). (3) |  |  |
| [ ]  The organisation has an inventory of all information assets (physical and digital), including current and legacy systems. There is a process in place to update and maintain the register of high risk / high value information assets. (4) |  |  |
| [x]  The organisation recognises records and information as real business assets. Information asset management is considered at a strategic level within the organisation and actively plans to manage them according to their purpose and risk profile. (5) |  |  |
| Your comments:Use this space to add information about observations, gaps, potential corrective actions; or information about the stakeholders who were consulted in relation to this question. This information is for use by public offices for internal planning and development. |

|  |
| --- |
| RIM ACTION 2: Information RiskAre the information risks that could impact high risk and high value areas of business identified and addressed?HOW THIS ACTION SUPPORTS THE DEVELOPMENT OF RECORDS AND INFORMATION MANAGEMENT MATURITY:**Principle 2**: Records and information management support businessThe core role of records and information management is to ensure the creation, maintenance, useability and sustainability of the records and information needed for short and long term business operations. (Standard on records management requirement 2.2)**Asset Governance:** With good leadership and management, Information Asset management policies and other instruments will be effectively implemented and used. |
| Responses (points) (tick one response that applies) | Examples of evidence to justify your response | Key guidance about this topic |
| [x]  There is no formal identification of information risks that could impact high risk / high value areas of business. (1) | [ ]  Documents indicating records and information risks are actively identified and managed.e.g. risk registers; cyber security plans; business continuity plans; information asset register; assigned responsibilities (e.g. system owner; data steward); policies, business rules and procedures; system design and acquisition documents; data migration strategy; data portability addressed in service contracts. | 1. [Identifying and managing high value and high-risk records, information, and data](https://staterecords.nsw.gov.au/recordkeeping/identifying-and-managing-high-value-and-high-risk-records-information-and-data)
2. [Identifying information risks that might be impacting on high-risk business](https://staterecords.nsw.gov.au/recordkeeping/identifying-information-risks-might-be-impacting-high-risk-business)
 |
| [ ]  There is some analysis of the information risks that could impact high risk / high value areas of business - but the organisation does not have a complete, single view (e.g. different information risks identified in various plans or registers). (2) |  |  |
| [ ]  The organisation has formally identified its high risk / high value information assets. There is a complete, single view of the information risks that could impact high risk / high value areas of the business (e.g. in a specific document, spreadsheet, or register). (3) |  |  |
| [ ]  The organisation has formally identified the information risks that could impact high risk / high value areas of the business. Risk mitigation for high risk / high value information assets is addressed through planned initiatives. (4) |  |  |
| [ ]  The organisation recognises records and information as real business assets. Information risk management is integrated into all new organisation-wide (or business unit-wide) initiatives and plans. e.g. IT projects, business transformation initiatives. (5) |  |  |
| Your comments:Use this space to add information about observations, gaps, potential corrective actions; or information about the stakeholders who were consulted in relation to this question. This information is for use by public offices for internal planning and development. |

|  |
| --- |
| RIM ACTION 3: SENIOR RESPONSIBLE OFFICERIs records and information management the responsibility of senior management, who provide direction and support, in accordance with business requirements, relevant laws and regulations? (NOTE: At the organisational level, this question relates to the organisation's Senior Responsible Officer or SRO. At the business unit level, it relates to a senior manager responsible for a defined group of activities and systems.)HOW THIS ACTION SUPPORTS THE DEVELOPMENT OF RECORDS AND INFORMATION MANAGEMENT MATURITY:**Principle 1**: Organisations take responsibility for records and information management.To ensure records and information are able to support all corporate business operations, organisations should establish governance frameworks. (Standard on records management requirements 1.2, 1.3)**Business Environment**: If the executives are aware of the benefits and are interested in managing Information Assets well, they will impose accountability. |
| Responses (points) (tick one response that applies) | Examples of evidence to justify your response | Key guidance about this topic |
| [x]  There is no senior executive oversight of the records and information management function. (1) | [ ]  Responsibility assigned in corporate policy on IM/RM.[ ]  Policy reflects Chief Executive's responsibility to ensure compliance with State Records Act (section 10).[ ]  Directives or reports that indicate the extent of SRO oversight of RM performance.[ ]  Reports to the senior manager, SRO or RIM governance group[ ]  Reports or directions from the senior manager, SRO or RIM governance group | 1. [Key obligations under the State Records Act 1998](https://staterecords.nsw.gov.au/recordkeeping/key-obligations-under-the-state-records-act-1998)
2. [NSW Information Management Responsibilities and Accountability Guidance (September 2013)](https://www.digital.nsw.gov.au/sites/default/files/Information%20Management%20Responsibilities%20guidance%20v1.pdf)
3. [Checklist for the Senior Responsible Officer for records and information management](https://staterecords.nsw.gov.au/recordkeeping/guidance-and-resources/resources-senior-responsible-officers)
 |
| [ ]  Responsibility for the oversight of records and information management is allocated to a designated senior manager, but this individual has little awareness or minimal visibility of RIM practices and performance in the business processes and systems for which they are responsible. (2) |  |  |
| [ ]  Responsibility for the oversight of records and information management is allocated to a designated senior manager. This individual understands and supports RIM practices and performance in the high risk / high value information assets for which they are responsible. (3) |  |  |
| [ ]  The designated senior manager directs RIM practices and monitors performance across all the business processes and systems for which they are responsible. The organisation has established a high-level, inter-disciplinary governance group that oversees all aspects of records and information management in a coordinated way. (4) |  |  |
| [ ]  The RIM governance group regularly reports to the Executive on RIM practices and performance to drive continuous improvement; identifies information risks and opportunities aligned with strategic objectives; and champions the value of records and information to all areas of the business. (5) |  |  |
| Your comments:Use this space to add information about observations, gaps, potential corrective actions; or information about the stakeholders who were consulted in relation to this question. This information is for use by public offices for internal planning and development. |

|  |
| --- |
| RIM ACTION 4: Records & Information StrategyIs there a defined strategic direction for records and information management, aligned with the goals of broader organisational strategy? (NOTE: RIM Strategy may be established for the whole organisation and then referenced in business unit plans, policies or procedures; or it could be established separately by business units. This will depend on the size of the organisation and whether records and information is centrally managed or devolved.)HOW THIS ACTION SUPPORTS THE DEVELOPMENT OF RECORDS AND INFORMATION MANAGEMENT MATURITY:**Principle 1**: Organisations take responsibility for records and information management. (Standard on records management requirements 1.2, 1.3)To ensure records and information are able to support all corporate business operations, organisations should establish governance frameworks. (Standard on records management requirement 1.1R)**Asset Governance:** With good leadership and management, Information Asset management policies and other instruments will be effectively implemented and used. |
| Responses (points) (tick one response that applies) | Examples of evidence to justify your response | Key guidance about this topic |
| [ ]  There is no RIM strategy or alignment of RIM to the organisation strategic direction. RIM issues are not recognised by senior management. (1) | [ ]  RIM strategy endorsed at Senior Executive level.[ ]  Business strategies reflect IM/RM goals and responsibilities | 1. [Establishing effective information management](https://staterecords.nsw.gov.au/recordkeeping/guidance-and-resources/establishing-effective-information-management)
2. [Records and information management policy checklist](https://staterecords.nsw.gov.au/recordkeeping/resources/records-and-information-management-policy-checklist)
3. [NSW Data and Information Custodianship Policy (June 2013)](https://data.nsw.gov.au/data-custodianship-policy)
 |
| [ ]  There is planning is underway to develop a RIM strategy and align RIM activities with the organisation strategic direction. There is some support from senior management. (2) |  |  |
| [ ]  There is an established RIM strategy, aligned with the organisation strategic direction. It includes a work program or initiatives to manage high risk / high value information assets as a priority. The strategy is endorsed by senior management and communicated to staff and contractors. (3) |  |  |
| [ ]  The RIM strategy influences or is referenced by other strategies and policies. The organisation considers records and information management impacts during long-term planning, major projects or risk management activities. There is regular reporting on RIM initiatives and senior management actively supports the RIM strategic direction. (4) |  |  |
| [ ]  The RIM strategy is regularly reviewed and updated to reflect changing business needs and direction. It is assessed to ensure the objectives are relevant, initiatives are resourced, and outcomes are measurable. The organisation seeks to align and coordinate with the strategic direction of related organisations. (5) |  |  |
| Your comments:Use this space to add information about observations, gaps, potential corrective actions; or information about the stakeholders who were consulted in relation to this question. This information is for use by public offices for internal planning and development. |

|  |
| --- |
| RIM ACTION 5: Records & Information PolicyDoes the organisation have an up-to-date, approved and communicated policy for records and information management? (NOTE: RIM Policy may be established for the whole organisation and then referenced in business unit plans, policies or procedures; or it could be established separately by business units. This will depend on the size of the organisation and whether records and information is centrally managed or devolved.) HOW THIS ACTION SUPPORTS THE DEVELOPMENT OF RECORDS AND INFORMATION MANAGEMENT MATURITY:**Principle 1**: Organisations take responsibility for records and information management.To ensure records and information are able to support all corporate business operations, organisations should establish governance frameworks. (Standard on records management requirements 1.1R)**Asset Governance:** With good leadership and management, Information Asset management policies and other instruments will be effectively implemented and used. |
| Responses (points) (tick one response that applies) | Examples of evidence to justify your response | Key guidance about this topic |
| ☐ There is no policy for records and information management; or the policy has not been updated within the past 3 years; or there is no staff awareness of the policy. (1) | [ ]  RIM policy endorsed at Senior Executive level.[ ]  Policy and RIM responsibilities are referenced in procedure documents.[ ]  System procurement, design or management documentation references RIM policy.[ ]  Performance monitoring (e.g. survey, audit, system logs) indicate staff awareness of the policy and policy requirements are reflected in practice | 1. [Establishing effective information management](https://www.records.nsw.gov.au/recordkeeping/advice/establishing-effective-information-management)
2. [Records and information management policy checklist](https://staterecords.nsw.gov.au/recordkeeping/resources/records-and-information-management-policy-checklist)
3. [NSW Data & Information Custodianship Policy (June 2013)](https://data.nsw.gov.au/data-custodianship-policy)
 |
| [ ]  The RIM policy is being developed or updated. Some teams or systems have documented procedures or business rules. (2) |
| [ ]  The organisation has a RIM Policy, endorsed by senior management. It is consistent with the RIM Strategy, the State Records Act and State Records NSW's standards. The policy requirements are supported by documented procedures for managing high risk / high value information assets. The policy is communicated and available to all staff and contractors. (3) |
| [ ]  The RIM Policy is linked to other policies and strategies. e.g. security, privacy and risk management. Breaches of the policy or procedures are actively addressed. Capabilities that support RIM policy requirements have been built into some business processes and systems. (4) |
| [ ]  RIM policy and processes are regularly reviewed and adjusted to align with business needs and strategy. They are championed and integrated across the organisation. Capabilities that support RIM policy requirements are actively built into information systems and business processes. (5) |
| Your comments:Use this space to add information about observations, gaps, potential corrective actions; or information about the stakeholders who were consulted in relation to this question. This information is for use by public offices for internal planning and development. |

|  |
| --- |
| RIM ACTION 6: RIM ResponsibilitiesAre staff across the organisation aware of their records and information management responsibilities?HOW THIS ACTION SUPPORTS THE DEVELOPMENT OF RECORDS AND INFORMATION MANAGEMENT MATURITY:**Principle 1**: Organisations take responsibility for records and information management.To ensure records and information are able to support all corporate business operations, organisations should establish governance frameworks. (Standard on records management requirements 1.5R. 1.6R, 1.7R)**Information Behaviours:** With efficient and effective information systems, good information management behaviours will be enabled and encouraged. |
| Responses (points) (tick one response that applies) | Examples of evidence to justify your response | Key guidance about this topic |
| [ ]  Awareness of records and information requirements is limited to specialist staff. Roles and responsibilities are not explicitly identified or documented – they are communicated ad hoc. Training needs have not been identified. (1) | [ ]  RIM Policy documents roles and responsibilities.[ ]  Responsibility for ensuring records and information management is addressed in systems and processes, is assigned to owners of systems.[ ]  Documentation identifies owners of systems.[ ]  Roles and responsibilities for IM are documented in job descriptions, performance plans or codes of conduct for staff and contractors. [ ]  Evidence of performance monitoring or interventions for non-compliance. | 1. [Leaflet for CEOS: Why is Recordkeeping Important?](https://www.staterecords.nsw.gov.au/recordkeeping/resources/leaflets-list)
2. [Recordkeeping Reminders](https://www.staterecords.nsw.gov.au/recordkeeping/resources/reminders)
3. [Recordkeeping and you (online course)](https://www.staterecords.nsw.gov.au/recordkeeping/recordkeeping-online-modules)
4. [Create and capture](https://www.staterecords.nsw.gov.au/recordkeeping/create-and-capture)
5. [Records Management Fundamentals](https://www.staterecords.nsw.gov.au/recordkeeping/records-management-fundamentals-presentations)
 |
| [ ]  There is some awareness of RIM requirements across the organisation. Roles and responsibilities are documented in some job descriptions and performance plans. RIM induction training is provided to some staff and contractors. Training needs have been identified and there is a plan to deliver RIM training more broadly. (2) |  |  |
| [ ]  Staff and contractors understand the RIM requirements of their role. They are familiar with the relevant policies and procedures. Roles and responsibilities are documented in all job descriptions, performance plans and codes of conduct. All staff receive RIM induction training as part of their on-boarding. A further program of RIM training is available to all staff and contractors. (3) |  |  |
| [ ]  RIM responsibilities are regularly promoted as part of normal business practice. Senior management understand their responsibilities and are exemplars of good practice. Job descriptions, performance plans and codes of conduct are reviewed and updated to ensure they reflect current RIM requirements and business needs. There is targeted RIM training available to staff and contractors in response to business needs and issues. (4) |  |  |
| [ ]  Records and information management requirements are embedded in the organisation’s business activities, work processes, systems and services. RIM expertise is available to provide targeted training when issues are identified through regular RIM reporting. The value of RIM training is understood and championed by senior management to support improved business practices. (5) |  |  |
| Your comments:Use this space to add information about observations, gaps, potential corrective actions; or information about the stakeholders who were consulted in relation to this question. This information is for use by public offices for internal planning and development. |

|  |
| --- |
| RIM ACTION 7: Capability & CapacityIs the organisation's information management capability and capacity sufficient to support and develop good information management?HOW THIS ACTION SUPPORTS THE DEVELOPMENT OF RECORDS AND INFORMATION MANAGEMENT MATURITY:**Principle 1**: Organisations take responsibility for records and information management. (Standard on records management requirements 1.4R)To ensure records and information are able to support all corporate business operations, organisations should establish governance frameworks.**Information Behaviours**:With efficient and effective information systems, good information management behaviours will be enabled and encouraged. |
| Responses (points) (tick one response that applies) | Examples of evidence to justify your response | Key guidance about this topic |
| [ ]  The organisation has taken no steps to address RIM capability and capacity. There is limited access to appropriate RIM expertise to support good practice. (1) | [ ]  Skills and capabilities reflected in relevant role descriptions.[ ]  Skills, capabilities and responsibilities are reflected in performance plans and/or service agreements. | 1. [Recordkeeping and you (online module)](https://www.staterecords.nsw.gov.au/recordkeeping/recordkeeping-online-modules)
2. [Framework for records and information management in NSW (online module)](https://www.staterecords.nsw.gov.au/recordkeeping/recordkeeping-online-modules)
3. [NSW Data & Information Custodianship Policy (June 2013)](https://data.nsw.gov.au/data-custodianship-policy)
 |
|  [ ]  Staff responsible for records and information management have limited professional development opportunities. There is a plan to improve RIM capability and capacity. (2) |  |  |
| [ ]  The organisation has skilled records and information management staff or access to appropriate skills to support good practice across the organisation. They have regular access to professional development opportunities. RIM capability and capacity is regularly assessed and monitored against business needs. (3) |  |  |
|  [ ]  RIM capability development is aligned to current and future business needs – job descriptions for skilled staff are regularly reviewed and updated accordingly. RIM capacity is included in workforce planning. (4) |  |  |
| [ ]  Records and information management staff are engaged across the business supporting a variety of initiatives. There is sufficient capacity to target continuous improvement in RIM practices. (5) |  |  |
| Your comments:Use this space to add information about observations, gaps, potential corrective actions; or information about the stakeholders who were consulted in relation to this question. This information is for use by public offices for internal planning and development. |

|  |
| --- |
| RIM ACTION 8: Outsourcing & ContractsAre partners, service providers, contractors and other external parties aware of their responsibilities for records and information management?HOW THIS ACTION SUPPORTS THE DEVELOPMENT OF RECORDS AND INFORMATION MANAGEMENT MATURITY:**Principle 1**: Organisations take responsibility for records and information management. (Records Management Standard requirements 1.4R)To ensure records and information are able to support all corporate business operations, organisations should establish governance frameworks.**Information Behaviours**: With efficient and effective information systems, good information management behaviours will be enabled and encouraged. |
| Responses (points) (tick one response that applies) | Examples of evidence to justify your response | Key guidance about this topic |
| [ ]  Roles, responsibilities and requirements for records and information management are not identified in contracts for outsourced functions and collaborative arrangements. There is no recognition of the State records status of records created or maintained by contracted providers or external parties. (1) | [ ]  Contracts for outsourced functions and collaborative arrangements specify details covering the creation, management, retention, portability and security of the information.[ ]  The risks of non-compliance by any party are identified. [ ]  Demonstrate that records and information management is assessed in outsourced and service contracts and instruments and included where required.[ ]  Portability of records and information is assessed in outsourced, cloud and similar service arrangements. | 1. [Accountable outsourcing: managing the records and information management considerations of outsourcing NSW Government business](https://www.staterecords.nsw.gov.au/recordkeeping/advice/accountable-outsourcing)
2. [NSW Government Cloud Policy (2020)](https://www.digital.nsw.gov.au/policy/cloud-strategy-and-policy/cloud-policy)
3. [NSW Data & Information Custodianship Policy (June 2013)](https://data.nsw.gov.au/data-custodianship-policy)
4. [Using cloud computing services - implications for information and records management](https://www.staterecords.nsw.gov.au/recordkeeping/advice/using-cloud-computing-services)
5. [Transition to the cloud: Managing your agency's privacy risks May 2021](https://www.ipc.nsw.gov.au/guide-transition-cloud-managing-your-agencys-privacy-risks-may-2021)
 |
| [ ]  Roles, responsibilities and requirements for records and information management are identified in some contracts for outsourced functions and collaborative arrangements. There is some monitoring of external parties to assess whether requirements are met. All parties are aware of the State records status of the records they hold. (2) |  |  |
| [ ]  Requirements for records and information management are identified in contracts for outsourced functions and collaborative arrangements that involve high risk / high value information assets. The responsibilities are clearly identified and monitored. (3) |  |  |
| [ ]  All contracts for outsourced functions and collaborative arrangements identify roles, responsibilities and requirements for records and information management (including creation, management, retention, portability and security). The responsibilities are clearly identified and monitored. (4) |  |  |
| [ ]  RIM requirements outlined in contractual arrangements are routinely performed as part of contracted services. RIM requirements are regularly reviewed and updated to remain current with good practice. Non-compliance by any party is addressed. (5) |  |  |
| Your comments:Use this space to add information about observations, gaps, potential corrective actions; or information about the stakeholders who were consulted in relation to this question. This information is for use by public offices for internal planning and development. |

|  |
| --- |
| RIM ACTION 9: Performance MonitoringDoes your organisation monitor the performance of records and information management?HOW THIS ACTION SUPPORTS THE DEVELOPMENT OF RECORDS AND INFORMATION MANAGEMENT MATURITY:**Principle 1**: Organisations take responsibility for records and information management. (Standard on records management requirements 1.8R)To ensure records and information are able to support all corporate business operations, organisations should establish governance frameworks.**Benefits Realisation**: The ability to measure information performance enables the articulation of business benefits and the justification for investment.**Executive Awareness**: If the benefits of good information management are understood, the executive will be interested and supportive. |
| Responses (points) (tick one response that applies) | Examples of evidence to justify your response | Key guidance about this topic |
| [ ]  Records and information management is not regularly audited for compliance; RM performance is not regularly monitored or reported. (1) | [ ]  Documented monitoring or auditing of activities, systems and processes, and corrective actions undertaken to address issues, e.g. could include monthly performance reporting on the number of new documents added to systems, or reports on usage of EDRMS. | 1. [Monitoring Overview](https://www.staterecords.nsw.gov.au/recordkeeping/advice/monitoring)
2. [Monitoring Recordkeeping Performance](https://www.staterecords.nsw.gov.au/recordkeeping/advice/monitoring/recordkeeping-performance)
3. [Records Management Assessment Tool](https://www.staterecords.nsw.gov.au/recordkeeping/advice/monitoring/records-management-assessment-tool)
4. [NSW Data & Information Custodianship Policy (June 2013)](https://data.nsw.gov.au/data-custodianship-policy)
 |
| [ ]  The organisation reports compliance with NSW Government requirements (including *State Records Act 1998*) and internal RM policies across some information systems or business units. Corrective actions to address non-compliance are inconsistent. (2) |  |  |
| [ ]  Records and information management across information systems and business processes that have been identified as high risk or high value is monitored and reviewed to ensure that it is performed, accountable and meets business needs. There is a structured approach to addressing non-compliance issues. (3) |  |  |
| [ ]  RM performance is regularly monitored and reported across all information systems and business processes. Corrective actions to address non-compliance are systemic. Opportunities to improve performance are explored and implemented. (4) |  |  |
| [ ]  The maturity, value and benefits of records and information management are regularly measured, reported and acknowledged by the Executive. Investment in information quality is done on the basis of continuous improvement and corporate alignment. (5) |  |  |
| Your comments:Use this space to add information about observations, gaps, potential corrective actions; or information about the stakeholders who were consulted in relation to this question. This information is for use by public offices for internal planning and development. |

|  |
| --- |
| RIM ACTION 10: Security & ProtectionDo security and access controls protect digital and hard copy records and information from unauthorised or unlawful access, destruction, loss, deletion or alteration? (NOTE: This question covers both digital and physical / hard copy records.)HOW THIS ACTION SUPPORTS THE DEVELOPMENT OF RECORDS AND INFORMATION MANAGEMENT MATURITY:**Principle 3**: Records and information are well managed (Standard on records management requirements 3.4, 3.5)Effective management of records and information underpins trustworthy, useful and accountable records and information which are accessible and retained for as long as they are needed. This management extends to records and information in all formats, in all business environments, and in all types of systems.**Principle 6**: Records are protected against theft, misuse, unauthorised access or modification (Standard on the physical storage of State records requirements 6.1S, 6.2S, 6.3S)All records in all formats require a basic level of security to prevent misuse and unauthorised access and ensure their authenticity and integrity. Records with security classifications (e.g. protected, secret, top secret), or containing sensitive information, should be handled, protected, stored and disposed of according to NSW Government requirements and the Australian Government Protective Security Policy Framework.**Information Quality**: Good information behaviours create high quality information. |
| Responses (points) (tick one response that applies) | Examples of evidence to justify your response | Key guidance about this topic |
| [ ]  There are limited security, access and quality controls in place. There are inadequate protections in place for physical and digital records and information. (1) | [ ]  Access, security and user permissions for systems managing records and information are documented and implemented.[ ]  System audits are able to test that access controls are implemented.[ ]  Policy, business rules and procedures identify how access to records and information is managed.[ ]  Assessments confirm that access is in accordance with the organisation’s policy, business rules and procedures.[ ]  Cybersecurity Attestation; audits or annual reports under the Privacy and Personal Information Protection Act 1998 ('PPIP Act'), the Government Information (Public Access) Act 2009 ('GIPA Act') and the State Records Act 1998.[ ]  Incident reports regarding any unauthorised access or theft of records.[ ]  Information security procedures and reporting[ ]  Data breach procedures and reporting[ ]  Effective identification, protection and management of sensitive classified information as well as security classified | 1. [Information security](https://www.staterecords.nsw.gov.au/recordkeeping/advice/faqs-information-security)
2. [Information classification, labelling and handling](https://www.digital.nsw.gov.au/policy/managing-data-information/information-classification-labelling-and-handling-guidelines)
3. [NSW Cyber Security Policy](https://www.digital.nsw.gov.au/policy/cyber-security-policy)
4. [Standard on the physical storage of State records](https://www.staterecords.nsw.gov.au/recordkeeping/standard-the-physical-storage-state-records)
5. [Public access to the records of NSW Government](https://www.staterecords.nsw.gov.au/recordkeeping/advice/public-access-to-records-of-nsw-government)
 |
| [x]  Controls are ad hoc or only applied in a few business processes or systems. Protections and security are in place for some physical and digital records and information. (2) |  |  |
| [ ]  Standard processes and controls are established and monitored across business processes and systems that have been identified as high risk or high value. There are appropriate protections in place for high risk / high value information assets (including third party storage providers and in transit). Security processes and controls are regularly tested. (3) |  |  |
| [ ]  Staff and contractors understand protection and security requirements. Incidents of unauthorised access to physical and digital records and information are monitored and addressed. Unauthorised destruction, loss or deletion is reported to the RIM governance group and to State Records NSW. Information security risks are reported to the RIM governance group for remediation. (4) |  |  |
| [ ]  RIM planning and reporting is consistent with privacy and security management. Policies and controls are integrated to minimise effort, costs and risks to records and information. (5) |  |  |
| Your comments:Use this space to add information about observations, gaps, potential corrective actions; or information about the stakeholders who were consulted in relation to this question. This information is for use by public offices for internal planning and development. |

|  |
| --- |
| RIM ACTION 11: Search & DiscoveryHow easy is it for staff and contractors to find the information and records they are looking for?HOW THIS ACTION SUPPORTS THE DEVELOPMENT OF RECORDS AND INFORMATION MANAGEMENT MATURITY:**Principle 3**: Records and information are well managed (Standard on records management requirements 3.3R)Effective management of records and information underpins trustworthy, useful and accountable records and information which are accessible and retained for as long as they are needed. This management extends to records and information in all formats, in all business environments, and in all types of systems.**Storage Principle 5**: Records are controlled in a system so that they can be identified, located and retrieved. (Standard on physical storage of State records requirements 5.1S, 5.2S, 5.3S, 5.4S)**Information Behaviours**: With efficient and effective information systems, good information management behaviours will be enabled and encouraged. |
| Responses (points) (tick one response that applies) | Examples of evidence to justify your response | Key guidance about this topic |
| [ ]  The organisation is unaware or has taken no steps to specifically address information accessibility and discoverability. Statistics and reports may indicate staff and contractors have difficulty searching and retrieving relevant and information and records. (1) | [ ]  System testing is able to verify that systems can locate and produce records which are viewable and understandable.[ ]  Adequate metadata to ensure that records are identifiable and accessible.[ ]  Statistics and reports on information requests (GIPA, PPIPA, HRIPA, SO52, subpoenas, commissions of inquiry, Chapter 16A) or complaints[ ]  The plan for the storage area/facility includes information on the physical and intellectual control of records.[ ]  Documented and implemented systems and metadata for the physical and intellectual control of records in storage areas/facilities which allows for the effective identification, retrieval and tracking of records.[ ]  Recordkeeping system includes information on the location of records within storage areas and the tracking of the movement of records.[ ]  Contracts with service providers include clauses requiring the tracking of movement and location of records, and the capture of appropriate metadata about the records and containers.[ ]  Procedures for identification and tracking of record locations.[ ]  Procedures include the retrieval, handling, safe transport of records, and the return of records to storage.[ ]  Inspection logs/documentation confirm that records are being retrieved from storage and handled correctly. | 1. [Mitigating common digital information management challenges](https://www.staterecords.nsw.gov.au/recordkeeping/advice/mitigating-digital-information-management-challenges)
2. [Metadata for managing records and information](https://staterecords.nsw.gov.au/recordkeeping/guidance-and-resources/metadata-records-and-information)
3. [(Suggested in the above) Minimum requirements for metadata for authoritative records and information](https://staterecords.nsw.gov.au/recordkeeping/guidance-and-resources/minimum-requirements-metadata-authoritative-records-and)
4. [Standard on the physical storage of State records](https://www.staterecords.nsw.gov.au/recordkeeping/standard-the-physical-storage-state-records)
 |
| [ ]  Search and retrieval have been addressed across some business processes or systems. Statistics and reports may indicate staff and contractors have variable experiences when trying to find and retrieve information and records. (2) |  |  |
| [ ]  Search and retrieval have been addressed for business processes and systems that are identified as high risk or high value. Statistics and reports indicate records and information are identifiable, retrievable and easily accessible. Staff and contractors have a consistent experience when finding and retrieving information and records that they create and manage. (3) |  |  |
| [ ]  Management controls are in place and regularly tested to maintain search and retrieval capability. Definitions, metadata and standards are used to increase the utility of information. User-experience issues with finding and retrieving information and records are identified and addressed. Staff and contractors have a reliable and repeatable experience when using information from across the organisation. (4) |  |  |
| [ ]  Records and information are collected and stored with access and discoverability in mind. Sufficient metadata is provided to correctly identify and locate information. Remediation processes are in place to address issues identified by the testing of management controls. The organisation (or business unit) is developing business intelligence to proactively deliver insights. Records have remained viewable and understandable regardless of format conversion or system migration over time. (5) |  |  |
| Your comments:Use this space to add information about observations, gaps, potential corrective actions; or information about the stakeholders who were consulted in relation to this question. This information is for use by public offices for internal planning and development. |

|  |
| --- |
| RIM ACTION 12: Quality Records and InformationAre the business needs and user expectations for records and information being met, in terms of strategic importance, quality and availability? Are records managed to ensure that they are reliable and trustworthy? HOW THIS ACTION SUPPORTS THE DEVELOPMENT OF RECORDS AND INFORMATION MANAGEMENT MATURITY:**Principle 3**: Records and information are well managed (Standard on records management requirements 3.2R)Effective management of records and information underpins trustworthy, useful and accountable records and information which are accessible and retained for as long as they are needed. This management extends to records and information in all formats, in all business environments, and in all types of systems.**Information Performance**: High quality information enables those assets to be effectively exploited and leveraged. |
| Responses (points) (tick one response that applies) | Examples of evidence to justify your response | Key guidance about this topic |
| [ ]  The organisation is unaware or has taken no steps to address business and user needs for records and information. RIM practices are ad hoc and do not support reliable and trustworthy records and information. (1) | [ ]  Adequate metadata to ensure meaning and context is associated with the record.[ ]  System audits are able to test management controls of systems, including information integrity.[ ]  Policies, business rules, procedures and other control mechanisms are in place to ensure accuracy and quality of records created, captured and managed.[ ]  Staff surveys and interviews[ ]  Time and motion studies of high risk or high value business processes | 1. [Mitigating common digital information management challenges](https://www.staterecords.nsw.gov.au/recordkeeping/advice/mitigating-digital-information-management-challenges)
2. [Metadata for managing records and information](https://staterecords.nsw.gov.au/recordkeeping/guidance-and-resources/metadata-records-and-information)
3. [(Suggested in the above) Minimum requirements for metadata for authoritative records and information](https://staterecords.nsw.gov.au/recordkeeping/guidance-and-resources/minimum-requirements-metadata-authoritative-records-and)
4. [NSW Cyber Security Policy](https://www.digital.nsw.gov.au/policy/cyber-security-policy)
 |
| [ ]  Policies, business rules and procedures have been implemented in some business processes or systems. Localised practices aim to ensure that records and information are reliable and trustworthy. System audits or anecdotal evidence indicate information quality is variable across the organisation. Some steps have been taken to address business and user needs for records and information. (2) |  |  |
| [ ]  Policies, business rules and procedures have been implemented for business processes and systems that are identified as high risk or high value. System audits or anecdotal evidence indicate these records and information are reliable and trustworthy. Business and user needs for high risk or high value records and information have been addressed. (3) |  |  |
| [ ]  Policies, business rules and procedures have been implemented for all business processes and systems across the organisation. Audits of management controls and anecdotal evidence indicate that records and information are reliable and trustworthy. Business and user needs for records and information have been identified and addressed. (4) |  |  |
| [ ]  An analysis of information assets has been conducted to determine if records and information meet business needs, usability, accountability requirements and community expectations. The organisation has established processes to remediate information quality issues as they arise. Audits and anecdotal evidence indicate information is fit for purpose. (5) |  |  |
| Your comments:Use this space to add information about observations, gaps, potential corrective actions; or information about the stakeholders who were consulted in relation to this question. This information is for use by public offices for internal planning and development. |

|  |
| --- |
| RIM ACTION 13: Use & Re-UseHow usable and re-usable is the information being created or collected by the organisation, both now and in the future?HOW THIS ACTION SUPPORTS THE DEVELOPMENT OF RECORDS AND INFORMATION MANAGEMENT MATURITY:**Principle 1**: Organisations take responsibility for records and information management. (Standard on records management requirements 3.2R)To ensure records and information are able to support all corporate business operations, organisations should establish governance frameworks.**Principle 2**: Records and information management support business. (Standard on records management requirements 3.5R)The core role of records and information management is to ensure the creation, maintenance, useability and sustainability of the records and information needed for short and long term business operations.**Information Quality**: Good information behaviours create high quality information. |
| Responses (points) (tick one response that applies) | Examples of evidence to justify your response | Key guidance about this topic |
| [ ]  The organisation is unaware, or has taken no steps to address information discovery, use and re-use. Information use and re-use is considered on an ad hoc basis in response to project needs or requests. Metadata for records and information is ad hoc. There is no systematic approach. (1) | [ ]  Annual reporting (GIPA, PPIPA, HRIPA)[ ]  Data quality statements[ ]  Adequate metadata to ensure meaning and context is associated with the record.[ ]  Standardised data sharing agreements | 1. [Minimum requirements for metadata for authoritative records and information](https://staterecords.nsw.gov.au/recordkeeping/guidance-and-resources/minimum-requirements-metadata-authoritative-records-and)
2. [NSW Information Management Framework](https://data.nsw.gov.au/information-management-framework)
3. [NSW Open Data Policy](https://data.nsw.gov.au/nsw-government-open-data-policy)
4. [NSW Data Quality Reporting Tool (and Standard)](https://data.nsw.gov.au/data-quality-reporting-tool)
5. [Reuse and repurpose design standard](https://www.digital.nsw.gov.au/delivery/digital-service-toolkit/design-standards)
 |
| [ ]  Localised RIM processes applied to some incoming and outgoing information and data shared with external parties. There is some application of State Records NSW’s minimum metadata requirements and other standards to support sharing and re-use. (2) |  |  |
| [ ]  Standard processes and controls for information use and re-use are established for information systems and business processes that have been identified as high risk or high value. Procedures for information collection, description and discovery support use and re-use, and minimise information duplication. (3) |  |  |
| [ ]  Information assets are routinely shared and re-used across the organisation or with external stakeholders as appropriate. RM requirements are addressed in data sharing agreements. Metadata is automatically applied where possible. Appropriate licences and quality statements are applied when sharing information. (4) |  |  |
| [ ]  The organisation identifies and engages with potential re-users of its information to support the design of RM capabilities and controls. Standard formats and metadata enable data exchange through common platforms, across organisations and jurisdictions. Information of known quality and provenance can be leveraged for business intelligence and analytics. (5) |  |  |
| Your comments:Use this space to add information about observations, gaps, potential corrective actions; or information about the stakeholders who were consulted in relation to this question. This information is for use by public offices for internal planning and development. |

|  |
| --- |
| RIM ACTION 14: Systems DesignHow are records and information requirements addressed in the design and management of IT systems and services for the organisation?HOW THIS ACTION SUPPORTS THE DEVELOPMENT OF RECORDS AND INFORMATION MANAGEMENT MATURITY:**Principle 2**: Records and information management support businessThe core role of records and information management is to ensure the creation, maintenance, useability and sustainability of the records and information needed for short and long term business operations. (Standard on records management requirements 2.3R, 2.4R, 2.6R).**Information Behaviours**: With efficient and effective information systems, good information management behaviours will be enabled and encouraged. |
| Responses (points) (tick one response that applies) | Examples of evidence to justify your response | Key guidance about this topic |
| ☐ The organisation is unaware or has taken no steps to address records and information management capabilities into new or existing business systems and tools. (1) | ☐ Systems managing high risk and/or high value records and information are protected by business continuity strategies and plans.☐ Documented policy, business rules and procedures for high risk and/or high value business processes include responsibilities for the creation and management of records and information.☐ Evidence that records and information management is assessed in system acquisition, system maintenance and decommissioning, and implemented where required.☐ Systems specifications for high risk and high value business include records and information management requirements.☐ Systems specifications include requirements for metadata needed to support records identification, useability, accessibility, and context.☐ Documentation of systems design and configuration maintained.☐ Identify and document where records and information are held across diverse system environments or physical locations.☐ Documented strategy for managing records and information in diverse system environments and physical locations.☐ Documented migration strategy.☐ Migrating records and metadata from one system to another is a managed process which results in trustworthy and accessible records.☐ Portability of records and information is assessed in cloud service or similar arrangements. | 1. [Designing, implementing and managing systems](https://www.staterecords.nsw.gov.au/recordkeeping/advice/designing%2C-implementing-%26-managing-systems)
2. [Backup systems are not a long-term information strategy](https://www.staterecords.nsw.gov.au/recordkeeping/advice/backup-systems)
3. [Identifying and managing high value and high-risk records and information](https://www.staterecords.nsw.gov.au/recordkeeping/advice/identifying-high-value-and-high-risk-information)
4. [Checklist for assessing business systems](https://www.staterecords.nsw.gov.au/recordkeeping/advice/checklist-for-assessing-business-systems)
5. [Cloud Computing Recordkeeping Requirements Checklist](https://www.staterecords.nsw.gov.au/recordkeeping/cloud-computing-recordkeeping-requirements-checklist)
6. [Decommissioning systems: records and information management considerations](https://www.staterecords.nsw.gov.au/recordkeeping/advice/decommissioning-systems)
7. AS/SNZ ISO 16175 – 1: 2021: *Information and documentation — Processes and functional requirements for software for managing records — Part 1: Functional requirements and associated guidance for any applications that manage digital records* [Available from Standards Australia]
 |
| [ ]  Records and information management capabilities are sometimes addressed in the design and management of new and upgraded IT systems or services, but there is no standard approach. Decisions about new and upgraded IT systems or services sometimes include RIM expertise. (2) |
| [ ]  Records and information management capabilities are often addressed in the design and management of new and upgraded IT systems or services – especially for high risk / high value information assets. RIM expertise is involved in decisions about systems that store, process or manage high risk / high value information assets. Standard RIM requirements for new and upgraded IT systems or services are documented. System design and configuration are fully documented for all IT systems and services. (3) |
| [ ]  Records and information management capabilities are routinely addressed in the design and management of new and upgraded IT systems or services. New and upgraded IT systems or services meet minimum metadata requirements where applicable. R&IM expertise is regularly involved in decisions about new and upgraded IT systems or services and during decommissioning to make sure RIM requirements are met. Risks are identified, where IT systems or services do not meet RIM requirements. (4) |
| [ ]  Records and information management capabilities and minimum metadata are implemented across all new and upgraded IT systems or services. RIM expertise is fully involved in design, management and decommissioning of IT systems or services. Risks relating to IT systems or services that do not meet RIM requirements are mitigated. (5) |
| Your comments:Use this space to add information about observations, gaps, potential corrective actions; or information about the stakeholders who were consulted in relation to this question. This information is for use by public offices for internal planning and development. |

|  |
| --- |
| RIM ACTION 15: Create, Collect, CaptureAre records and appropriate metadata created, collected and captured across the organisation?HOW THIS ACTION SUPPORTS THE DEVELOPMENT OF RECORDS AND INFORMATION MANAGEMENT MATURITY:**Principle 3**: Records and information are well managed. (Standard on records management requirements 3.1R).Effective management of records and information underpins trustworthy, useful and accountable records and information which are accessible and retained for as long as they are needed. This management extends to records and information in all formats, in all business environments, and in all types of systems.**Information Quality**: Good information behaviours create high quality information. |
| Responses (points) (tick one response that applies) | Examples of evidence to justify your response | Key guidance about this topic |
| [ ]  Creation and capture of records and appropriate metadata is ad hoc. There is no systematic approach. Practices are determined by business units, teams or individual staff. (1) | [ ]  Policies, business rules and procedures articulate/document staff requirements and responsibilities for the creation, capture and management of records of business operations.[ ]  Assessments or audits demonstrate that systems operate routinely.[ ]  Exceptions to routine operations that affect information integrity, useability or accessibility are identified, resolved and documented. | 1. [Records Management Assessment Tool](https://www.staterecords.nsw.gov.au/recordkeeping/advice/monitoring/records-management-assessment-tool)
2. [Developing systems – information management considerations](https://www.staterecords.nsw.gov.au/recordkeeping/advice/developing-systems-considerations)
3. AS/SNZ ISO 16175-1: 2021: *Information and documentation — Processes and functional requirements for software for managing records — Part 1: Functional requirements and associated guidance for any applications that manage digital records* [Available from Standards Australia]
 |
| [ ]  Processes for records and metadata creation and capture are established across a few business processes or systems. (2) |  |  |
| [ ]  Records and metadata are routinely created and managed as part of normal business practice. There are standard processes to capture records of activity or decisions in areas of business that have been identified as high risk / high value. (3) |  |  |
| [ ]  Records and metadata are routinely created and managed as part of normal business practice. There are standard processes to capture records across all information systems and business processes. (4) |  |  |
| [ ]  Standard processes for creation, collection and capture of records and metadata are embedded in all information systems and business processes. The organisation explicitly recognises this will minimise information risks, while enhancing data quality, reliability and trustworthiness of records. (5) |  |  |
| Your comments:Use this space to add information about observations, gaps, potential corrective actions; or information about the stakeholders who were consulted in relation to this question. This information is for use by public offices for internal planning and development. |

|  |
| --- |
| RIM ACTION 16: StorageHas the organisation considered how best to store its digital and hard copy records and information?HOW THIS ACTION SUPPORTS THE DEVELOPMENT OF RECORDS AND INFORMATION MANAGEMENT MATURITY:**Principle 2**: Records and information management support business. The core role of records and information management is to ensure the creation, maintenance, useability and sustainability of the records and information needed for short and long term business operations. (Standard on records management requirements 2.5R).**Storage Principle 1**: Records are stored in appropriate storage areas and facilities and located away from known and unacceptable risk. (Standard on the physical storage of State records requirements 1.1S – 1.9S)**Storage Principle 2**: Records are stored in environmental conditions appropriate to their format and retention period. (Standard on the physical storage of State records requirements 2.1S – 2.8S)**Storage Principle 3**: Shelving, equipment and containers used for storing records are secure, accessible and protected from deterioration. (Standard on the physical storage of State records requirements 3.1S – 3.3S)**Storage Principle 4**: A regular maintenance and monitoring program for records storage areas has been implemented. (Standard on the physical storage of State records requirements 4.1S – 4.4S)**Information Behaviours**: With efficient and effective information systems, good information management behaviours will be enabled and encouraged. |
| Responses (points) (tick one response that applies) | Examples of evidence to justify your response | Key guidance about this topic |
| [ ]  The organisation is unaware or has taken no steps to address records and information storage requirements. (1) | [ ]  Identify and document which systems hold records of identified or potential permanent or long-term value.[ ]  Identify and document where records of identified or potential permanent or long-term value are located.[ ]  Records and information are kept for as long as they are needed for business, legal requirements (including in accordance with current authorised records retention and disposal authorities), accountability, and community expectations.[ ]  Decommissioning of systems takes into account retention and disposal requirements for records and information contained in the system.[ ]  Records survey or IT systems audit[ ]  Information asset register[ ]  Information Lifecycle Management policy, plan or strategy | 1. [Decommissioning systems](https://www.staterecords.nsw.gov.au/recordkeeping/advice/decommissioning-systems)
2. [Standard on the physical storage of State records](https://www.staterecords.nsw.gov.au/recordkeeping/standard-the-physical-storage-state-records)
3. [Effectively manage the migration of your digital records](https://www.staterecords.nsw.gov.au/recordkeeping/migrating-records%3A-managing-source-records-after-migration)
 |
| [ ]  The organisation has actively addressed safe and accessible storage for records and information in a few business units or information systems. There may be risks in other storage areas. (2) |  |  |
| [ ]  The organisation has actively addressed safe and accessible storage, including storage areas, for records and information in systems and business processes that have been identified as high risk or high value. (3) |  |  |
| [ ]  The organisation has actively addressed safe and accessible storage across all business systems and information storage areas. (4) |  |  |
| [ ]  Records and information storage is directed by an Information Lifecycle Management approach. The organisation considers security, accessibility and quality – and how these requirements change during the retention period. It balances cost-effective storage with performance to meet business needs for information until final disposition. (5) |  |  |
| Your comments:Use this space to add information about observations, gaps, potential corrective actions; or information about the stakeholders who were consulted in relation to this question. This information is for use by public offices for internal planning and development. |

|  |
| --- |
| RIM ACTION 17: Retention & DisposalHas the organisation identified the records and information required to meet short, medium and long term needs, so they can be effectively managed throughout their "lifetime"? (NOTE: Retention and disposal requirements are driven by business needs for information, community expectations and various accountability requirements - e.g. State Records Act, GIPAA, privacy, environmental protection and many more. These requirements are documented in an approved disposal authority. The disposal authority can be used to plan for storage, migration, security etc.)HOW THIS ACTION SUPPORTS THE DEVELOPMENT OF RECORDS AND INFORMATION MANAGEMENT MATURITY:**Principle 2**: Records and information management support business. (Standard on records management requirements 2.1R)The core role of records and information management is to ensure the creation, maintenance, useability and sustainability of the records and information needed for short and long term business operations.**Principle 3**: Records and information are well managed. (Standard on records management requirements 3.6R, 3.7R)Effective management of records and information underpins trustworthy, useful and accountable records and information which are accessible and retained for as long as they are needed. This management extends to records and information in all formats, in all business environments, and in all types of systems.**Information Quality**: Good information behaviours create high quality information. |
| Responses (points) (tick one response that applies) | Examples of evidence to justify your response | Key guidance about this topic |
| [ ]  No processes are in place to manage the retention or disposal of records and information as identified in authorised disposal authorities. No disposal takes place; OR disposal of physical and digital information is ad hoc. Disposal actions may not be documented. (1) | [ ]  Documented decisions, policy, business rules or procedures on what records and information are required to meet or support business and identified recordkeeping requirements, including accountability and community expectations.[ ]  Policy, business rules and procedures identify:- how the retention and disposal of records and information is managed.- how the destruction of records and information is managed, including deletion of data.[ ]  Current, comprehensive and authorised records retention and disposal authorities are in place.[ ]  Documents or system logs confirm that records and information have been sentenced or disposed according to current authorised retention and disposal authorities.[ ]  Documented internal approval to keep, destroy or transfer records. Internal approval considers other legislative obligations, business needs and stakeholder expectations. | 1. [Advice on retention and disposal](https://www.staterecords.nsw.gov.au/recordkeeping/advice/retention-and-disposal)
2. [Implementing a retention and disposal authority](https://www.staterecords.nsw.gov.au/recordkeeping/advice/retention-and-disposal/implementing-a-retention-and-disposal-authority)
3. [Decommissioning systems](https://www.staterecords.nsw.gov.au/recordkeeping/advice/decommissioning-systems)
 |
| [ ]  Processes manage some records and information according to authorised disposal authorities. Disposal actions are implemented across some repositories and formats and are sometimes documented. The destruction of some physical or digital information is secure, complete and irreversible. (2) |  |  |
| [ ]  Processes ensure records and information are retained for as long as required for business use and as identified in authorised disposal authorities. Disposal actions are routinely planned and carried out for information assets identified as high risk / high value. These disposal actions are fully documented. Destruction (where applicable) is secure, complete and irreversible. (3) |  |  |
|  [ ]  Processes for authorised disposal are monitored to ensure their ongoing effectiveness. Disposal actions are routinely planned and carried out across most repositories and formats. e.g. EDRMS, paper files, M365, Teams, email, shared drives, other business systems. Issues relating to internal approvals for disposal are escalated to the RIM governance group for action. Staff and contractors know where to get guidance on disposal policies and processes. Destruction (where applicable) is secure, complete and irreversible (4) |  |  |
|  [ ]  The organisation proactively reviews and improves its disposal processes and capability to support regular disposal. Disposal functionality is provided in all new and upgraded business systems. Disposal actions are routinely implemented across all repositories, systems and formats. Application of disposal rules are facilitated by auto-classification tools. The RIM governance group promotes regular and routine disposal of information. (5) |  |  |
| Your comments:Use this space to add information about observations, gaps, potential corrective actions; or information about the stakeholders who were consulted in relation to this question. This information is for use by public offices for internal planning and development. |

|  |
| --- |
| RIM ACTION 18: TransferHas the organisation considered requirements to transfer records and information? Public offices may need to transfer records and information due to organisation restructure, machinery of government changes, merger, privatisation; or when transitioning between IT systems and service environments. Public offices are required to transfer State archives to Museums of History NSW. (NOTE: This question excludes transfers to offsite or temporary storage, such as the Government Records Repository or commercial providers.)HOW THIS ACTION SUPPORTS THE DEVELOPMENT OF RECORDS AND INFORMATION MANAGEMENT MATURITY:Museums of History NSW’s entitlement to State records no longer in use. Once a State record is no longer in use for official purposes in the public office responsible for the record, the Museums of History NSW is entitled to control of the record and the public office ceases to be entitled to control of it.Records required to be made available to Museums of History NSW. A public office that has control of a record that the Museums of History NSW is entitled to control of under this Act is required to make the record available to the Museums of History NSW (to enable the Museums of History NSW to take control of the record). The Museums of History NSW may issue guidelines to public offices from time to time as to how State records are to be made available to the Museums of History NSW and public offices are to comply with those guidelines. (*State Records Act 1998*, Part 4, section 27 and section 29)**Information Behaviours:** With efficient and effective information systems, good information management behaviours will be enabled and encouraged. |
| Responses (points) (tick one response that applies) | Examples of evidence to justify your response | Key guidance about this topic |
| [ ]  The organisation is unaware or has not taken any steps or given explicit consideration to the transfer of records and information. (1) | [ ]  Policy, business rules and procedures identify how the retention and disposal of records and information is managed.[ ]  Records and information are sentenced according to current authorised retention and disposal authorities.[ ]  Records required as State archives are routinely transferred to Museums of History NSW (or other approved arrangements) when no longer in use for official purposes.[ ]  Specification for information systems and service environments[ ]  Evidence that records and information management is assessed in system acquisition, system maintenance and decommissioning, and implemented where required. | 1. [Transferring digital records to our custody](https://mhnsw.au/transferring-digital-records-to-our-custody/)
2. [Transferring physical format records to our custody](https://mhnsw.au/transferring-physical-format-records-to-our-custody/)
3. [Procedures for disposal authorisation](https://www.staterecords.nsw.gov.au/recordkeeping/rules/procedures/disposal-authorisation)
 |
| [ ]  Records and information transfer is done on an ad hoc basis, e.g. in response to organisation restructure, office relocation or IT system / service decommissioning. (2) |  |  |
| [ ]  Records required as State archives in the applicable general or functional retention and disposal authorities have been identified. Physical records are routinely transferred to Museums of History NSW (or other approved arrangements) when no longer in use for official purposes. Digital records are transferred to Museums of History NSW on an ad hoc basis. (3) |  |  |
| [ ]  Records required as State archives in the applicable general or functional retention and disposal authorities have been identified. Physical and digital records are routinely transferred to Museums of History NSW (or other approved arrangements) when no longer in use for official purposes. (4) |  |  |
| [ ]  Records and information transfer capabilities are addressed proactively in the design and management of IT systems or service environments. They support both routine transfer of records to Museums of History NSW (or other approved arrangements) and incidental transfers driven by changes in organisation structure or operational needs. (5) |  |  |
| Your comments:Use this space to add information about observations, gaps, potential corrective actions; or information about the stakeholders who were consulted in relation to this question. This information is for use by public offices for internal planning and development. |

|  |
| --- |
| RIM ACTION 19: Access DirectionsHas the organisation made Access Directions to enable public access to the State records for which it is responsible?HOW THIS ACTION SUPPORTS THE DEVELOPMENT OF RECORDS AND INFORMATION MANAGEMENT MATURITY:Public access to State records after 30 years. Each public office must ensure that the State records for which it is responsible and that are in the open access period (at least 30 years old) are the subject of an access direction. This can be either an open to public access (OPA) direction or a closed to public access (CPA) direction. (*State Records Act 1998*, Part 6, section 51(1))**Information Quality:** Good information behaviours create high quality information. |
| Responses (points) (tick one response that applies) | Examples of evidence to justify your response | Key guidance about this topic |
| [ ]  There are no Access Directions in place. (1) | [ ]  Register of Access Directions[ ]  Information security attestation[ ]  Annual reporting (GIPA, PPIPA, HRIPA)[ ]  Privacy policy and procedures[ ]  Security policy and procedures | 1. [Procedures for making access directions](https://mhnsw.au/public-access-to-the-records/)
2. [Attorney General's Guidelines for making Access Directions](https://mhnsw.au/public-access-to-the-records/)
 |
| [ ]  There are some Access Directions in place. They are made on an ad hoc basis or in response to an application under s.54 of the Act. (2) |  |  |
| [ ]  There are Access Directions in place to manage public access for those records identified as State archives which have been transferred to Museums of History NSW. (3) |  |  |
| [ ]  There are Access Directions in place to manage public access for all records that are at least 30 years old, regardless of where they are held or their disposal status. (4) |  |  |
| [ ]  Access Directions are made proactively. They are linked to privacy and security controls; and are used to support IT planning and budgeting. Early Access Directions (or similar) have been made for records that can be authorised for public access in less than 30 years. (5) |  |  |
| Your comments:Use this space to add information about observations, gaps, potential corrective actions; or information about the stakeholders who were consulted in relation to this question. This information is for use by public offices for internal planning and development. |

# RESULTS

Review your responses to the preceding questions. For each response you selected, transcribe the corresponding points (the number in brackets after the response text) into the table below.

For example: For RIM Action 1 (High risk / high value records and information) – if you selected the first response “*There is no formal identification of high risk / high value records and information.*” enter a score of (1) into the Points column

# MATURITY SCORE

This number indicates your Maturity Score for each question.

Refer to the maturity levels described in a table on the following pages of this document – and write which level you are at for each RIM Action.

The questions have also been grouped into three themes or categories for a broader view of results.

* People & Governance (PG)
* Systems & Business (SB)
* Information Management (IM)

You can calculate a % result by adding up your scores for all the questions in a Category and dividing by the total possible score for that Category.

The table also indicates which regulatory requirements are associated with each RIM Action.

## Baseline Compliance

A maturity score of 3 is considered Baseline Compliance – meeting State Records NSW’s requirements for high risk / high value records and information.

This questionnaire is also available in **MS Excel spreadsheet format**, which includes support for automated scoring and results graphs.

Refer to the detailed **Instructions** document for an explanation of how to use the assessment results and suggestions for next steps.

# SCORING TABLE

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| CATEGORY | RIM ACTION | REQUIREMENTS | MATURITY SCORE | BASELINE COMPLIANCE | CATEGORY SCORE (%) |
| People and Governance | Q1. High Risk/High Value | 2.2R |  | 3 | % |
| People and Governance | Q2. Information Risk | 2.2R |  | 3 |
| People & Governance | Q3. Senior Responsible Officer | 1.2R, 1.3R |  | 3 |
| People & Governance | Q4. RIM Strategy | 1.1R |  | 3 |
| People & Governance | Q5. RIM Policy | 1.1R |  | 3 |
| People & Governance | Q6. RIM Responsibilities | 1.5R |  | 3 |
| People & Governance | Q7. Capability & Capacity  | 1.6R, 1.7R |  | 3 |
| People & Governance | Q8. Outsourcing | 1.4R |  | 3 |
| People & Governance | Q9. Performance Monitoring  | 1.8R |  | 3 |
| Systems & Business | Q10. Security & Protection | 3.4R, 3.5R, 6.1S-6.3S |  | 3 | % |
| Systems & Business | Q11. Search & Discovery  | 3.3R, 5.1S-5.4S |  | 3 |
| Systems & Business | Q12. Information Quality | 3.2R |  | 3 |
| Systems & Business | Q13. Use & Re-Use | 3.2R, 3.5R |  | 3 |
| Systems & Business | Q14. Systems Design  | 2.3R, 2.4R, 2.6R |  | 3 |
| Information Management | Q15. Create, Collect, Capture  | 3.1R |  | 3 | % |
| Information Management | Q16. Storage  | 2.5R, 1.1S-1.9S,2.1S-2.8S, 3.1S-3.3S, 4.1S-4.4S |  | 3 |
| Information Management | Q17. Retention & Disposal | 2.1R, 3.6R, 3.7R |  | 3 |
| Information Management | Q18. Transfer  | SR Act Pt.4 s.27 & s.29 |  | 3 |
| Information Management | Q19. Access Directions | SR Act Pt 6 s.51(1) |  | 3 |

# Information Domains

Consider the Information Domains below. These can help articulate how achieving maturity in one area of records and information management can support further development across the organisation – towards an environment where investment in the quality of information assets is driven by business benefits and value, rather than IT costs and efficiencies.





The information in these tables is Commercial in Confidence and Copyright © Experience Matters Pty Ltd. 2021

# Maturity Levels

|  |  |  |
| --- | --- | --- |
| 1 | Initial | The desirable processes are non-existent or ad hoc, with no organisational oversight. The organisation or senior responsible officer is unaware of whether a requirement is met. |
|  Ad hoc, unpredictable, poorly controlled, no processes, unaware. |
|  |
| 2 | Developing | Processes are becoming refined and repeatable, but only within the scope of individual teams or projects. There are no organisational standards. |
|  Aware, reactive, repeatable, documented processes. |
|  |
| Level 3 is considered Baseline Compliance– meeting State Records NSW requirements for high risk / high value records and information. |
| 3 | Defined | Processes are standardised within the organisation based on best practices identified internally or from external sources. Knowledge and best practices start to be shared internally. |
|  Controlled, established, standardised, followed processes. |
|  |
| 4 | Managed | The organisation has widely adopted the standard processes and begins monitoring them using defined metrics. |
|  Capable, proactive, measured and reported. |
|  |
| 5 | Optimising | The organisation is optimising, refining and using innovation to increase efficiency within the organisation and, more widely, within its business sector. |
|  Efficient, reviewed and audited, data-driven process improvement. |
|  |

# ANNEX A: FULL TEXT OF REGULATORY REQUIREMENTS:

Full text of the requirements reflected in the RMAT questions.

- R indicates a requirement from the [*Standard on records management*](https://www.records.nsw.gov.au/recordkeeping/rules/standards/records-management)
- S indicates a requirement from the [*Standard on the physical storage of State records*](https://www.records.nsw.gov.au/recordkeeping/standard-the-physical-storage-state-records)
- SRA indicates a requirement from the [*State Records Act 1998*](https://legislation.nsw.gov.au/view/html/inforce/current/act-1998-017)

| Qs | REQUIREMENTS |
| --- | --- |
| 4, 5 | 1.1R | Corporate records and information management is directed by policy and strategy. |
| 3 | 1.2R | Records and information management is the responsibility of senior management who provide direction and support for records and information management in accordance with business requirements and relevant laws and regulations. |
| 3 | 1.3R | Corporate responsibility for the oversight of records and information management is allocated to a designated individual (senior responsible officer). |
| 8 | 1.4R | Organisations have skilled records and information management staff or access to appropriate skills. |
| 6 | 1.5R | Responsibility for ensuring that records and information management is integrated into work processes, systems, and services is allocated to business owners and business units. |
| 7 | 1.6R | Staff and contractors understand the records management responsibilities of their role, the need to make and keep records, and are familiar with the relevant policies and procedures. |
| 7 | 1.7R | Records and information management responsibilities are identified and addressed in outsourced, cloud and similar service arrangements. |
| 9 | 1.8R | Records and information management is monitored and reviewed to ensure that it is performed, accountable and meets business needs. |
| 17 | 2.1R | Records and information required to meet short and long term needs are identified. |
| 1, 2 | 2.2R | High risk and high value areas of business and the systems, records and information needed to support these business areas are identified. |
| 14 | 2.3R | Records and information management is a designed component of all systems and service environments where high risk and/or high value business is undertaken. |
| 14 | 2.4R | Records and information are managed across all operating environments. |
| 16 | 2.5R | Records and information management is designed to safeguard records and information with long term value. |
| 14 | 2.6R | Records and information are sustained through system and service transitions by strategies and processes specifically designed to support business and accountability. |
| 15 | 3.1R | Records and information are routinely created and managed as part of normal business practice. |
| 12, 13 | 3.2R | Records and information are reliable and trustworthy. |
| 11 | 3.3R | Records and information are identifiable, retrievable and accessible for as long as they are required. |
| 10 | 3.4R | Records and information are protected from unauthorised or unlawful access, destruction, loss, deletion or alteration. |
| 10, 13 | 3.5R | Access to records and information is managed appropriately in accordance with legal and business requirements. |
| 17 | 3.6R | Records and information are kept for as long as they are needed for business, legal and accountability requirements. |
| 17 | 3.7R | Records and information are systematically and accountably destroyed when legally appropriate to do so. |
| 16 | 1.1S | The location of each records storage area and facility has been subject to risk assessment to identify and mitigate possible risks to records. |
| 16 | 1.2S | The Senior Responsible Officer or appropriate agency representative has approved all records storage areas and facilities. |
| 16 | 1.3S | The storage facilities have been assessed as being suitable for the storage of records. |
| 16 | 1.4S | Records storage facilities built since 2011 are compliant with the Building Code of Australia and associated codes at the time of construction. |
| 16 | 1.5S | Storage areas and facilities are weatherproof and have good drainage. |
| 16 | 1.6S | Storage areas and facilities are dedicated to either records or records/library materials storage. |
| 16 | 1.7S | Storage areas and facilities have appropriate and comprehensive fire detection and protection systems and equipment, in compliance with the Building Code of Australia and Australian Standards. |
| 16 | 1.8S | Each storage area and facility has a current disaster reaction and recovery plan which is regularly revised and equipment / supplies to assist in the recovery of records after a disaster. |
| 16 | 1.9S | Insurance for the recovery and restoration of records in the event of a disaster. |
| 16 | 2.1S | Short term records (to be retained for only 10 years or less) are stored in conditions which ensure preservation until they are no longer required. |
| 16 | 2.2S | Medium term records (to be retained for 10-30 years) are stored in conditions which ensure preservation until they are no longer required. |
| 16 | 2.3S | Long term records (to be retained for 30 years or longer) and those identified as State archives are stored in conditions which will ensure their preservation. |
| 16 | 2.4S | Temperature and humidity levels within storage areas and facilities are monitored for stability and action taken to minimise any significant fluctuations. |
| 16 | 2.5S | Records are stored away from direct light, including sunlight. |
| 16 | 2.6S | The air in records storage areas circulates freely and there is an intake of fresh air. |
| 16 | 2.7S | Magnetic media is protected from magnetic fields. |
| 16 | 2.8S | Records storage areas and facilities have an integrated pest management system. |
| 16 | 3.1S | Shelving and handling equipment is clean, in good condition and appropriate to the format and security requirements of the records. |
| 16 | 3.2S | Containers are clean, in good condition, and appropriate for the format, retention and security requirements of the records they hold. |
| 16 | 3.3S | Records storage facilities, shelving, equipment, and containers meet workplace health and safety requirements. |
| 16 | 4.1S | Records storage areas and facilities are clean and maintained. |
| 16 | 4.2S | Regular checks of records and containers in the storage facility to identify any signs of pest infestation, mould, or other deterioration. |
| 16 | 4.3S | Mould or pest infestation is treated promptly and appropriately. |
| 16 | 4.4S | Appropriate conservation action is undertaken as required but repairs to records do not damage the records further. |
| 11 | 5.1S | Records are controlled in a system which allows them to be identified, located, retrieved, and returned to storage after use. |
| 11 | 5.2S | Procedures for the appropriate handling and use of records are defined and communicated to all users. |
| 11 | 5.3S | Policies and procedures are implemented to ensure that records of long term value and archives are handled with care. |
| 11 | 5.4S | If a public office chooses to convert or digitise records, then records are converted or digitised according to recognised standards. |
| 10 | 6.1S | Storage areas and facilities are access controlled, restricted to authorised staff, intruder resistant, and monitored. |
| 10 | 6.2S | Security classified records are stored in appropriate containers and storage zones within the storage area. |
| 10 | 6.3S | Records in transit are protected. |
| 18 | SR Act Part.4 s.27 | Museums of History NSW’s entitlement to State records no longer in use. Once a State record is no longer in use for official purposes in the public office responsible for the record, the Museums of History NSW is entitled to control of the record and the public office ceases to be entitled to control of it. |
| 18 | SR Act Part.4 s.29 | Records required to be made available to Museums of History NSW> A public office that has control of a record that the Museums of History NSW is entitled to control of under this Act is required to make the record available to the Museums of History NSW (to enable the Museums of History NSW to take control of the record). The Museums of History NSW may issue guidelines to public offices from time to time as to how State records are to be made available to the Museums of History NSW and public offices are to comply with those guidelines. |
| 19 | SR Act Part 6 s.51(1) | Access direction must be given for records in the open access period. (1) Each public office must ensure that the State records for which it is responsible that are in the open access period are the subject of an access direction. Only the public office responsible for a record can give an access direction for the record. (1A) There is a presumption that State records in the open access period should be open to public access under this Act. |

# ANNEX B: DETAILED EXPLANATORY NOTES:

These detailed explanatory notes are drawn from State Records NSW’s guidance to support implementation of the [Standard on records management](https://staterecords.nsw.gov.au/recordkeeping/guidance-and-resources/standard-records-management) and the [Standard on the physical storage of State records](https://staterecords.nsw.gov.au/recordkeeping/standard-the-physical-storage-state-records). They are provided here for easy reference in relation to each of the maturity assessment questions. Please refer to [State Records NSW’s website](https://staterecords.nsw.gov.au/) for the most current and comprehensive information.

## RIM ACTIONS 1 & 2: High Risk / High Value BUSINESS & SYSTEMS and Information RISK

High risk business areas in each organisation should be priorities for records and information management activity, to ensure that these records are created, captured, well managed and are allocated appropriate resources and strategies.

Information risks are related to but distinct from technology risks. Information risks are those risks which relate to the inherent characteristics and value of information. Information risks can hamper government business and accountability, particularly when these risks occur within high-risk areas of business operations.

Areas in your organisation that perform core, strategic, highly accountable or high value business operations are likely to be classed as high-risk business. Because these areas are likely to be performing key aspects of government business, it is critical that records are created and captured to account for and support these operations, in both the short and long term.

Other areas of high risk business that need to be identified and assessed are areas undergoing significant transition. In these areas, it is possible that traditional processes are changing, new technologies and services are being adopted and information itself is changing or disappearing, possibly placing your business at risk. To identify high risk areas of business you can:

* identify areas that perform core, strategic, highly accountable or high value business operations related to legislation that your organisation oversights
* use your organisation’s corporate risk register to flag existing areas of identified corporate risk
* look at business areas that are adopting a lot of new technologies and services
* focus on business areas under transition
* focus on areas adopting BYOD (bring your own device) approaches
* talk to managers and staff about any information-related concerns they may have in their specific business areas.

After identifying areas of high business risk, you should then identify what information is required to support these business areas. By identifying and documenting the high risk/high value areas of the organisation’s business, and the systems, records and information supporting these critical areas of the business, organisations can better prioritise the management, treatment, and protection of these critical systems and the records and information they contain.

Following the identification of high risk and high value records, information and systems, organisations should then identify the likely or potential information risks and manage or mitigate such risks. This also includes ensuring that systems managing high risk and/or high value records and information are protected from loss and disaster by appropriate security measures and business continuity strategies and plans. The [NSW Government Cyber Security Policy](https://www.digital.nsw.gov.au/policy/cyber-security-policy) also covers business processes and continuity. By identifying high value records and information at creation, the organisation can better manage and use this core asset. Better management can increase the value of information. Documented policy, business rules and procedures for high risk and/or high value business processes will also need to include responsibilities for the creation and management of records and information.

## RIM ACTION 3: Senior Responsible Officer

Responsibility for records and information management is cascaded down throughout the organisation, through various levels of management. Ultimate responsibility lies with the Chief Executive and senior management who provide direction and support for records and information management and ensure that it conforms to business requirements and relevant laws and regulations. This requirement mirrors obligations in the *State Records Act 1998* (see section 10) and reinforces the need for the Chief Executive and senior management to provide high-level direction and support (including ensuring adequate resourcing) for records and information management. Responsibilities are normally identified and assigned in organisational policy and strategy.

Another tier of responsibility is the oversight of records and information management at a corporate level. This requirement establishes the role of the *Senior Responsible Officer*. The *Senior Responsible Officer* (SRO) is a senior manager with organisation-wide influence and appropriate strategic and managerial skills. The SRO role is to provide oversight of records and information management within the organisation, including monitoring of records and information management to ensure that it meets the needs of the organisation and to respond to monitoring/reporting requests from State Records NSW. Responsibilities are normally identified and assigned in organisational policy and strategy. The role of SRO should also be incorporated into the performance plan for the individual designated as SRO. Each public office should advise State Records NSW of their organisation’s SRO and keep State Records NSW updated with any changes to personnel undertaking this role.

## RIM ACTIONS 4 & 5: RIM Strategy and Policy

Governance frameworks are critical to the achievement of good records and information management. This requirement establishes the importance of high level policy and strategy, adopted by the Senior Executive of the organisation, to ensure good records and information management practice in the organisation. Policy and strategy identify the value of corporate records and information, how records and information are managed, the various levels of responsibility and accountability for records and information within the organisation, requirements for records and information in outsourcing and service delivery arrangements, and the monitoring of records and information activities, systems and processes.

## RIM ACTION 6: Rim Responsibilities

This requirement places RM/IM responsibilities more broadly within the organisation. It acknowledges that business managers should have a detailed understanding of the information produced by and necessary to perform their function, and have responsibilities for ensuring its appropriate management. Cascading responsibility to different business areas of the organisation, allows for different skill groups (business unit staff and RM/IM staff) to work together to ensure that records and information management is integrated into work processes, systems and services across the organisation. Organisations should identify business owners (and system owners). Business owners are responsible for ensuring records and information management is considered and included in systems and processes used. Business units and business owners need to be aware that there are RM/IM requirements when they move to a new service environment, develop new work processes, systems or services, or improve on existing work processes, systems or services. In these types of scenarios, they will need to demonstrate that they have considered/addressed RM/IM and assessed risks as part of the development process. Responsibilities for business owners should be identified and assigned in organisation policy on IM/RM. These responsibilities may also be included in performance plans.

This requirement means that all staff of the organisation, including contractors, need to understand their records management responsibilities. Contractors are brought into organisations to perform specified tasks. Information and documentation required to be produced and managed in their performance of the contract needs to be clearly articulated. Contractors also need to know their records management responsibilities and be familiar with the relevant policies and procedures. Responsibilities are identified and assigned in organisational policy on IM/RM. Skills, capabilities and responsibilities are also assigned in role descriptions and/or performance plans. Policy, business rules or procedures will also articulate or document staff requirements for the creation and management of records.

This requirement ensures that records and information are addressed in all service arrangements that the organisation enters into. The corporate policy and strategy should include responsibilities for ensuring that records and information requirements are identified and addressed. Organisations should undertake risk assessments and have records and information management issues addressed in the contractual arrangements that the organisation agrees to. Service arrangements will include:

* Functions, activities or services of the organisation being outsourced to an external provider, and
* Functions, activities or services being moved to cloud services or other service providers (internal to Government or external to Government).

Organisations will also need to ensure that the portability of records and information is assessed and appropriately addressed in outsourced, cloud and similar service arrangements.

## RIM ACTION 7 & 8: Capability and Capacity; OUTSOURCING AND CONTRACTS

Access to skilled, capable, and qualified records and information staff is a core and important resource for the successful deployment of records and information management strategies. Within each organisation’s RM/IM strategy, there are likely to be a range of different levels of responsibility and skills required for the range of RM/IM roles and the various work being undertaken. These skills and capabilities will be reflected in relevant role descriptions. Qualifications for RM/IM roles will include TAFE and university qualifications, depending on the roles. Public offices should be able to access records and information management skills via recruitment, service providers, or through networking with other public offices. Responsibilities will be identified and assigned in organisational policy and strategy, performance plans and/or service agreements.

This requirement means that all staff of the organisation, including contractors, need to understand their records management responsibilities. Contractors are brought into organisations to perform specified tasks. Information and documentation required to be produced and managed in their performance of the contract needs to be clearly articulated. Contractors also need to know their records management responsibilities and be familiar with the relevant policies and procedures. Responsibilities are identified and assigned in organisational policy on IM/RM. Skills, capabilities and responsibilities are also assigned in role descriptions and/or performance plans. Policy, business rules or procedures will also articulate or document staff requirements for the creation and management of records.

## RIM ACTION 9: Performance Monitoring

Records and information management activities, systems and processes should be regularly monitored to ensure that they are meeting the needs of the organisation and are in conformity with requirements. If issues are identified though a monitoring process then these need to be addressed with a corrective action. Monitoring also includes activities such as process and system audits.

## RIM ACTION 10: Security and Protection

Organisations should implement an information security policy and appropriate security mechanisms. The policy should cover both physical and digital records and information. Appropriate security mechanisms include: access, security and user permissions in systems; processes to protect records and information wherever they are located including in transit and outside of the workplace; and appropriate secure physical storage facilities. Undertaking regular system audits will assist organisations verify that access controls have been implemented appropriately and are working.

Managing access to records and information should be in accordance with policy, business rules and procedures. Organisations should ensure that policy, business rules and procedures are in accordance with the requirements of the [Government Information (Public Access) Act 2009](https://legislation.nsw.gov.au/view/html/inforce/current/act-2009-052), [Privacy and Personal Information Protection Act 1998](https://legislation.nsw.gov.au/view/html/inforce/current/act-1998-133), [Health Records and Information Privacy Act 2002](https://legislation.nsw.gov.au/view/html/inforce/current/act-2002-071), and the [State Records Act 1998](https://legislation.nsw.gov.au/view/html/inforce/current/act-1998-017). Organisational policy should direct that information published by government organisation such as Annual Reports and open access information released under the GIPA Act should be uploaded to OpenGov. Undertaking regular assessments will assist organisations verify that access is managed in accordance with the organisation’s policy, business rules and procedures.

Security measures include but are not limited to:

* cyber security activities undertaken to comply with the [NSW Cyber Security Policy](https://www.digital.nsw.gov.au/policy/cyber-security-policy)
* access controls on storage areas and facilities to prevent intruders
* use of security zones for the storage of security classified or sensitive information
* restricting access to storage areas and facilities to authorised staff
* staff working in storage areas containing security classified or sensitive information have appropriate security clearances
* storing and protecting records according to [NSW Government Information classification, labelling and handling guidelines](https://www.digital.nsw.gov.au/policy/managing-data-information/information-classification-labelling-and-handling-guidelines) and the Australian Government Protective Security Policy Framework
* using secure processes for the disposal of records with security classifications or containing sensitive information according to [NSW Government Information classification, labelling and handling guidelines](https://www.digital.nsw.gov.au/policy/managing-data-information/information-classification-labelling-and-handling-guidelines) and the Australian Government Protective Security Policy Framework
* security monitoring of storage areas and facilities whereby access is trackable and auditable, and
* ensuring that records are not left unattended or unsecured when in transit.

Serious breaches (including those that may relate to personal information) should be reported to the Senior Responsible Officer and to the public office’s Chief Information Officer, and assessed to ensure rectification action is taken.

## RIM ACTION 11: Search and Discovery

This requirement ensures that records and information can be identified, retrieved from storage (physical or digital storage), and are accessible for as long as they are required. Adequate metadata should be used to ensure that records are identifiable and retrievable. Undertaking regular system testing will assist organisations verify that the systems can locate and produce records which are viewable and understandable. In order to maintain the accessibility to records and information in digital format, organisations will also need to ensure that they have plans and/or strategies to mitigate digital and technology obsolescence. This could include ‘moving forward’ digital records and information through regular processes of migration. In order to maintain accessibility to physical records, organisations will need to ensure that physical records are stored in appropriate storage areas and facilities. See the [Standard on the physical storage of State records](https://staterecords.nsw.gov.au/recordkeeping/standard-the-physical-storage-state-records) for further information.

## RIM ACTION 12: Quality RECORDS AND INFORMATION

Records and information need to be accurate, authentic, and reliable - as evidence of transactions, decisions and actions. This requirement ensures that records have adequate metadata to provide meaning and context and that the metadata remains associated with the record. Adequate and appropriate metadata enables a record to function as reliable and trusted evidence. Implementing policy, business rules, procedures and other control mechanisms work towards ensuring the accuracy and quality of records created, captured and managed. Undertaking regular system audits and assessments allows an organisation to demonstrate that the management controls of systems are operating correctly and provides assurity of the integrity of the information stored in the system.

## RIM ACTION 13: Use and Re-Use

Some indicators of maturity may include: whether the organisation release data through an open data platform; is core business system data captured in data lake, data hub or similar for reuse; does the organisation have information analytics or dashboards that are used in decision making or to support business processes. See also [Reuse and repurpose](https://www.digital.nsw.gov.au/delivery/digital-service-toolkit/design-standards) .

## RIM ACTION 14: Systems Design

In the complex business and systems environments in organisations, it is important to design records and information management upfront. This is particularly important for systems and service environments where high risk and/or high value business is undertaken. By designing upfront and including IM/RM into systems specification and acquisition, particularly for systems and service environments which are managing high risk and/or high value records and information, better control of IM/RM and improved outcomes can be achieved. ‘By design approaches’ mean that IM/RM is taken into account right from the start and that system maintenance, migrations and decommissioning are easier. Currently the migration and decommission of systems can be problematic as there is often insufficient information about the records and information held in the system, the configuration of the system, and the retention requirements for records and information held in the system. This often requires organisations to undertake considerable analysis in order to determine what to do with a system. By taking a ‘by design approach’, organisations can ensure:

* systems specifications for high risk and high value business include records and information management requirements
* systems specifications include requirements for metadata needed to support records identification, useability, accessibility, and context
* documentation of systems design and configuration is maintained.

Assess business systems against the [Checklist for assessing business systems](https://staterecords.nsw.gov.au/recordkeeping/guidance-and-resources/checklist-assessing-business-systems) or [Cloud Computing Recordkeeping Requirements Checklist](https://staterecords.nsw.gov.au/recordkeeping/cloud-computing-recordkeeping-requirements-checklist). The [Checklist for assessing business systems](https://staterecords.nsw.gov.au/recordkeeping/guidance-and-resources/checklist-assessing-business-systems) offers strategies on how to achieve records functionality either within the system design or by having a policy or a manual procedure in place.

Organisations also need to ensure that documentation of systems design and configuration (and changes made overtime) is maintained. Well managed, well planned and designed systems will better meet the organisation’s and Government’s needs for information.

This requirement ensures that records and information are managed appropriately through system migrations and service transitions, such as upgrades of systems and services offered in cloud environments. It is important that organisations have documented migration strategies, appropriate planning and testing processes and that these ensure that records and information are not ‘left behind’ or disposed of unlawfully. Migrating records and metadata from one system to another is a managed process which results in trustworthy and accessible records. Maintaining adequate system documentation will also assist successful migration strategies. Integral to the migration and decommissioning processes is the need to ensure that records and information are kept for as long as they are needed for business, legal requirements (including in accordance with authorised records retention and disposal authorities), accountability, and community expectations. Migration and decommissioning of systems must ensure that disposal of records and information takes into account the authorised retention and disposal requirements for the records and information contained in the system. Disposal of records includes not bringing across records, information, and metadata in migrations or deletion of records, information and metadata in decommissioning processes. This requirement also builds on Minimum Compliance Requirement 2.2 and Minimum Compliance Requirement 2.5 ([Standard on records management](https://staterecords.nsw.gov.au/recordkeeping/guidance-and-resources/standard-records-management)) that identified high risk/high value records and information are supported and migrated appropriately. It is important that the portability of records and information is assessed in cloud service or similar arrangements. It is also important that records and information are not “left behind” in outsourced arrangements and that adequate provision is made for records and information to be transferred back to the organisation or another service provider.

## RIM ACTION 15: Create, Collect, Capture

Policy, rules and processes articulate and inform the organisation and its staff of the requirements and responsibilities for the creation, capture and management of records of the business processes of the organisation. This requirement ensures that the organisation (including staff and contractors) is conforming with policies, rules and processes and that records and information are being routinely created and managed. Undertaking regular process and system audits and assessments allows an organisation to demonstrate that its processes and systems are operating routinely and that exceptions to routine operations that affect information creation, integrity, useability or accessibility are identified, resolved and documented.

## RIM ACTION 16: Storage

This requirement ensures that organisations identify and know which systems and service environments hold records and information with identified or potential permanent or long term value. This requirement builds on Minimum Compliance Requirements 2.1 and 2.2 ([Standard on records management](https://staterecords.nsw.gov.au/recordkeeping/guidance-and-resources/standard-records-management)). Once the organisation knows what records and information are required permanently or long term and where they are located, then these records and information assets can be safeguarded and managed appropriately over time. Records and information that are required permanently or for the long-term will outlive the systems in which they are currently managed. Permanent or long-term records and information will also outlive outsourcing arrangements and contracts with service providers. Organisation must ensure that they plan and manage the protection of permanent or long-term records and information through transitions of systems (system migrations and decommissioning systems processes) and changes to service arrangements (termination of services; new outsourcing arrangement). Permanent and long-term records must also be protected through administrative change and machinery of government changes. This includes where records are required to be transferred between organisations and also where records may remain with the creating organisation. To help with identifying long-term records and information organisations will be able to leverage off their approved retention and disposal authorities. They may also leverage off the inventory of information assets undertaken for the [*NSW Data & Information Custodianship Policy*](https://www.digital.nsw.gov.au/policy/managing-data-information/data-and-information-custodianship-policy)*.*

## RIM ACTION 17: Retention and Disposal

This requirement provides the foundation for the management of records and information in all environments, it is also particularly important for ensuring the management of records and information in the digital environment. By undertaking a documented assessment of the organisation’s functions and activities, the organisation can determine what records and information it requires to support business and meet identified recordkeeping requirements, including accountability and community expectations. This work provides the foundation for understanding the short and long term retention of records and determining what systems and business processes are high risk and/or high value for the organisation and the records and information which is required to support these. This work should also be incorporated into current, comprehensive and authorised records retention and disposal authorities for the organisation’s records. Decisions on what records and information are required should be documented in business rules, policy and procedure. These decisions should also be reflected in specifications for systems and metadata schema. Many organisations will have already undertaken some of this work in the development of a functional retention and disposal authority. Organisations should refer to the current, comprehensive and authorised records retention and disposal authorities used for disposal as a critical tool for determining what records and information it requires to support business and meet identified recordkeeping requirements, including accountability and community expectations.

Organisations should implement policy, business rules and procedures to ensure that records and information are kept for as long as they are required and identify how the retention and disposal of records and information is managed. The policy, business rules and procedures should be in accordance with the requirements of the *State Records Act 1998* and the authorised records retention and disposal authorities. Records and information need to be sentenced and disposed of according to current authorised retention and disposal authorities.

Organisations should implement policy, business rules and procedures which identify how the destruction of records and information is managed, including the deletion of data and the decommissioning of systems. This includes assigning responsibility for sentencing and disposal of records, disposal authorisation processes, the implementation of disposal actions, and documenting the disposal of records and information. Organisations must be able to account for their retention and disposal of records and information. This includes providing evidence that the disposal of records and information was permitted and authorised under legal obligations, including the State Records Act, and accountability requirements. Organisations must be able to demonstrate that the disposal of records and information is in accordance with current authorised records retention and disposal authorities.

This includes records and information located in business systems, in the cloud, or in physical records storage. Disposing of digital records and information may be part of a planned migration process or the decommissioning of systems. Records required as State archives should be routinely transferred to Museums of History NSW when no longer in use for official purposes.

## RIM ACTION 18: Transfer

Records that are to be kept as part of the State archives must be properly protected while they remain under the public office’s control. (Section 11(1)) Once a State record is no longer in use for official purposes in the public office responsible for the record, the Museums of History NSW is entitled to control of the record and the public office ceases to be entitled to control of it. (Section 27) A public office that has control of a record that the Museums of History NSW is entitled to control of is required to make the record available to the Museums of History NSW. A public office is to comply with the Museums of History NSW’s guidelines as to how records are to be made available. (Section 29)

A person must not dispose of a State record, transfer its possession or ownership, take or send it out of New South Wales, damage or alter them, or neglect it in a way that causes damage (Section 21(1)), unless it is done (Section 21(2)):

* with the permission, or in accordance with a practice or procedure approved by, the Board of the State Records Authority NSW
* in accordance with normal administrative practice in a public office
* as authorised or required under a provision of any other Act that is prescribed by the regulations
* pursuant to an order or determination of a court or tribunal
* in accordance with a resolution of a House of Parliament where the House is the responsible public office, or
* for the purpose of placing a record under the control of a public office.

## RIM ACTION 19: Access Directions \*

An access direction is a direction that a series, group or class of records is:

* open to public access (OPA) after 30 years or
* closed to public access (CPA) for a period of more than 30 years.

All records in the open access period (over 30 years of age) need to be covered by an access direction regardless of where they are held, or their disposal status. Each public office is responsible for making access directions to its own records.

This includes records created by:

* predecessor agencies where the function has been continued, and
* other public offices where the function the records document has been transferred.

Someone with an understanding of the known or likely contents of the records should make access directions. They may be records staff or action officers. The person who makes access directions should be familiar with the [Attorney General's Guidelines](https://www.records.nsw.gov.au/recordkeeping/advice/attorney-generals-guidelines).

The *State Records Act* requires that public offices ensure all their open access period records are covered by an access direction. There are also two additional triggers for the making of access directions if they have not already been made. 1) All records being transferred to Museums of History NSW must be covered by a current access direction. 2) If records are not covered by an access direction, anyone can apply, including Museums of History NSW, to have an access direction made for records in the open access period. A public office must make an access direction within 14 days and advise the applicant and Museums of History NSW in writing of the access direction. If no direction is made in 14 days, the records applied for are considered to be subject to an OPA direction.

A public office can authorise records that are less than 30 years of age to be open to public access. This authorisation is known as Early Access. Early Access does not permit the breaching of any duty or obligation (such as confidentiality) or other Acts prohibiting disclosure for records.

\* From 1 January 2024 due to changes to the *State Records Act 1998*, the open to public access (OPA) will change to after **20 years** and the closed to public access (CPA) for a period of more than **20 years**. See <https://mhnsw.au/public-access-to-the-records/>