Implementing the Standard on records management

This document is designed to assist public offices understand the requirements of the *Standard on records management*, obligations under the *State Records Act 1998*, and the relationship between the *Standard on records management* and the code of best practice.

There are three parts in this document:

Part 1: Understanding the requirements of the *Standard on records management*

Part 2: Meeting obligations under the *State Records Act 1998*

Part 3:*Standard on records management* and the code of best practice *AS ISO 15489.1: 2017 Information and documentation – Records Management, Part 1: Concepts and principles*

The *Standard on records management* was issued to public offices on 2 March 2015.

NSW State Archives and Records has reviewed the *Standard on records management* in light of Recommendation 8.4 of the Final Report of the Royal Commission into Institutional Responses to Child Sexual Abuse and the NSW Government Response to the Royal Commission into Institutional Responses to Child Sexual Abuse. We note that there are no changes or revisions to the minimum compliance requirements listed in the *Standard on records management.* However, our review identified that some minor amendments (additional text) were required to the "Examples of how a public office can demonstrate compliance with the requirement" component of the standard at minimum compliance requirements **3.2, 3.4,** and **3.5**. Additional text is highlighted in yellow in the amended *Standard on records management.*

An *amended Standard on records management* was issued to public offices on 30 November 2018 and is available from https://www.records.nsw.gov.au/recordkeeping/rules/standards/records-management

The *Standard on records management* covers records and information in all formats, including both digital and physical records. It has been designed to support digital recordkeeping as the NSW Government transitions to digital business processes.

Underpinning this standard is the need to ensure that business is supported by sound records and information management practices. Importantly, the standard has been framed and targeted to support good information practices in complex business and information environments.

This standard refers to both records and information and establishes requirements for the holistic management of records and information. Taking this approach to the management of records and information better reflects the way in which most organisations now manage their information resources in an integrated manner.

With the issue of the standard in 2015, a number of older standards were revoked and are no longer in use. Older standards can be consulted at www.opengov.nsw.gov.au.

Public offices should consult the *Standard on the physical storage of State records* for requirements for the storage of non-digital records and counter disaster requirements applicable to non-digital records.

Part 1: Understanding the requirements of the new standard

This part of the Guide is designed to assist public offices understand the requirements of the *Standard on records management*.

Following is a table for each principle which lists the minimum compliance requirements, an explanation for each requirement, and key guidance for implementing the requirements.

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. These include:

- policy directing how records and information shall be managed
- assigning responsibilities
- establishing provisions for records and information in outsourcing and service delivery arrangements
- monitoring records and information management activities, systems and processes.

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
1 Corporate records and information management is directed by policy and strategy.	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	Establishing effective information management What is information management? Records and information management policy checklist *NSW Information Management Responsibilities and Accountability Guidance* (September 2013) *AS ISO 15489.1: 2017*, *Information and documentation – Records management, Part 1: Concepts and principles*, see

	outsourcing and service delivery arrangements, and the monitoring of records and information activities, systems and processes.	*Section 6 Policies and responsibilities*
2 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.	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.	Key obligations under the State Records Act 1998 Resources for Chief Executives *NSW Information Management Responsibilities and Accountability Guidance* (September 2013) AS NZS ISO 30301-2012 *Information and documentation – Management systems for recordkeeping – Requirements* *AS ISO 15489.1: 2017*, *Information and documentation – Records management, Part 1: Concepts and principles*, see *Section 6 Policies and responsibilities*
3 Corporate responsibility for the oversight of records and information management is allocated to a designated individual (senior responsible officer).	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	Role of the senior responsible officer (online module) Framework for records and information management in NSW (online module) Checklist for the Senior Responsible Officer for records and information management *NSW Information Management Responsibilities and Accountability Guidance* (September 2013)

	respond to monitoring/reporting requests from NSW State Archives and Records. 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 NSW State Archives and Records of their organisation’s SRO and keep NSW State Archives and Records updated with any changes to personnel undertaking this role.	AS NZS ISO 30301-2012 *Information and documentation – Management systems for recordkeeping – Requirements* *AS ISO 15489.1: 2017*, *Information and documentation – Records management, Part 1: Concepts and principles*, see *Section 6 Policies and responsibilities*
4 Organisations have skilled records and information management staff or access to appropriate skills.	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.	Education and training opportunities in records and archives Framework for records and information management in NSW (online module) *NSW Information Management Responsibilities and Accountability Guidance* (September 2013) AS NZS ISO 30301-2012 *Information and documentation – Management systems for recordkeeping – Requirements* *AS ISO 15489.1: 2017*, *Information and documentation – Records management, Part 1: Concepts and principles*, see *Section 6 Policies and responsibilities*
5 Responsibility for ensuring that records and information	This requirement places RM/IM responsibilities more broadly within the organisation. It	Developing systems – information

management is integrated into work processes, systems, and services is allocated to business owners and business units.	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.	management considerations *NSW Data & Information Custodianship Policy* (June 2013) AS NZS ISO 30301-2012 *Information and documentation – Management systems for recordkeeping – Requirements* *AS ISO 15489.1: 2017*, *Information and documentation – Records management, Part 1: Concepts and principles*, see *Section 6 Policies and responsibilities*
6 **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.**	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	Recordkeeping and you: supervisors and managers (online module) Recordkeeping and you (online module) Your responsibilities for managing email

	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.	(online module) *NSW Information Management Responsibilities and Accountability Guidance* (September 2013) *AS ISO 15489.1: 2017, Information and documentation – Records management, Part 1: Concepts and principles*, see *Section 6 Policies and responsibilities*
7 **Records and information management responsibilities are identified and addressed in outsourced, cloud and similar service arrangements**.	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	Accountable outsourcing: managing the records and information management considerations of outsourcing NSW Government business Using cloud computing services - implications for information and records management Using shared services for records and information management Cloud Email Implementation *NSW Information Management Responsibilities and Accountability Guidance* (September 2013) *NSW Data & Information Custodianship Policy* (June 2013) *NSW Government Cloud Services Policy and Guidelines* (August 2015)

	outsourced, cloud and similar service arrangements.	AS NZS ISO 30301-2012 *Information and documentation – Management systems for recordkeeping – Requirements* *AS ISO 15489.1: 2017, Information and documentation – Records management, Part 1: Concepts and principles*, see *Section 6 Policies and responsibilities*
8 Records and information management is monitored and reviewed to ensure that it is performed, accountable and meets business needs.	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 of high risk/high value systems.	Monitoring Records Management Assessment Tool (revised tool will be available later in 2018) *NSW Information Management Responsibilities and Accountability Guidance* (September 2013) *AS ISO 15489.1: 2017, Information and documentation – Records management, Part 1: Concepts and principles*, see *Section 6 Policies and responsibilities*

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.

By undertaking an assessment of records and information needs, public offices can define their key business information. Public offices should use this assessment to design records and information management into processes and systems. This will ensure that records and information support business operations and accountability requirements, and sustain records and information needed for the short and long term.

Taking a planned approach to records and information management means all operating environments are considered. It also means that the creation and management of records and information needed to support business are considered in all system and service arrangements.

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
1. Records and information required to meet short and long term needs are identified.	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	Strategies for documenting government business: DIRKS Manual Minimum requirements for metadata for authoritative records and information General retention and disposal authorities Functional retention and disposal authorities *AS ISO 15489.1: 2017, Information and documentation – Records management, Part 1: Concepts and principles*, see *Section 4 Principles for managing records*, *Section 5 Records and records systems*, *Section 7 Appraisal*, and *Section 8 Records controls*

	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.	
2. High risk and high value areas of business and the systems, records and information needed to support these business areas are identified.	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 Digital Information Security Policy* also covers business processes and continuity. By identifying high value records and information at	Identifying and managing high value and high risk records and information *Standard on the physical storage of State records* Counter disaster strategies for records and recordkeeping systems Identifying information risks that might be impacting on high risk business *NSW Government Digital Information Security Policy* (April 2015) *NSW Government Information Classification Labelling and Handling Guidelines* (July 2015) *NSW Data & Information Custodianship*

	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.	*Policy* (June 2013) AS/NZS 5050: Business continuity: Managing disruption-related risk HB 221: 2004, Business Continuity Management *AS ISO 15489.1: 2017, Information and documentation – Records management, Part 1: Concepts and principles*, see *Section 4 Principles for managing records*, *Section 5 Records and records systems*, *Section 7 Appraisal*, *Section 8 Records controls, Section 9 Processes for creating, capturing and managing records*
3. Records and information management is a designed component of all systems and service environments where high risk and/or high value business is undertaken.	In the complex business and systems environments in organisations, it is important to design records and information management upfront rather than trying to integrate or develop solutions after a system has been developed and implemented. 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	Designing, implementing and managing systems Metadata for managing records and information Minimum requirements for metadata for authoritative records and information Information management by design Decommissioning systems NSW Disaster Recovery Guidelines *AS ISO 15489.1: 2017, Information and documentation – Records management, Part 1: Concepts and principles*, see *Section 4 Principles for managing records*, *Section 5 Records and records systems*, *Section 6 Policy and responsibilities*, *Section 7 Appraisal*, *Section 8 Records*

	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. 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.	*controls*, *Section 9 Processes for creating, capturing and managing records*
4. Records and information are managed across all operating environments.	If an organisation knows what records and information assets they have, where they are located and managed, then they can better control them in the short and long term. By maintaining visibility of records and information regardless of the system or storage location, the organisation can better protect these assets. Records and information assets can be held in diverse systems environments, in third party systems in the cloud, by service providers and in a range of physical locations. By identifying where records and information are	Accountable outsourcing: managing the records and information management considerations of outsourcing NSW Government business *Standard on the physical storage of State records* (see particularly Principle 2: Location and buildings) Information management by design The complexity of digital transitions

	held, organisations can better manage records and information in diverse system environments, diverse storage environments and physical locations, including providing access to records and information when required. To help with this requirement, organisations will also be able to leverage off the inventory of information assets undertaken for the *NSW Government's Digital Information Security Policy*.	*NSW Government Digital Information Security Policy* (April 2015) *NSW Government Information Classification Labelling and Handling Guidelines* (July 2015) *NSW Data & Information Custodianship Policy* (June 2013) *NSW Government Mobile Device and Application Framework* *NSW Government End User Computing Standard* *AS ISO 15489.1: 2017, Information and documentation – Records management, Part 1: Concepts and principles*, see *Section 4 Principles for managing records, Section 5 Records and records systems, Section 9 Processes for creating, capturing, and managing records*
5. Records and information management is designed to safeguard records and information with long term value.	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.* 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	Identifying and managing high value and high risk records and information Decommissioning systems *Standard on the physical storage of State records* (see particularly Principle 7: Security) Information security Back up systems are not a long-term information strategy Effectively manage the migration of your

	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*.	digital records Deep Time – perspectives on managing long term value digital information *NSW Government Digital Information Security Policy* (April 2015) *NSW Government Information Classification Labelling and Handling Guidelines* (July 2015) *NSW Data & Information Custodianship Policy* (June 2013) *Transition Guidelines: Managing legacy data and information* (November 2013) *AS ISO 15489.1: 2017*, *Information and documentation – Records management, Part 1: Concepts and principles*, see *Section 5 Records and records systems*, *Section 7 Appraisal*, and *Section 9 Processes for creating, capturing, and managing records*
6. Records and information are sustained through system and service transitions by strategies and processes specifically designed to support business and accountability.	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	Effectively manage the migration of your digital records Decommissioning systems Back up systems are not a long-term information strategy Using cloud computing services - implications for information and records management

	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* 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.	The complexity of digital transitions *General retention and disposal authority: Source records that have been migrated* (GA 48) *General retention and disposal authority: original or source records that have been copied* (GA 45) *AS ISO 15489.1: 2017*, *Information and documentation – Records management, Part 1: Concepts and principles, see Section 5 Records and records systems, Section 7 Appraisal, Section 8 Records controls, Section 9 Processes for creating, capturing, and managing records*

Principle 3: Records and information are well managed

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.

Minimum compliance requirements	Explanation	Key guidance for implementing this requirement
1. Records and information are routinely created and managed as part of normal business practice.	This requirement builds on the earlier principles in the standard. 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.	Records Management Assessment Tool (revised tool will be available later in 2018) Developing systems – information management considerations *AS ISO 15489.1: 2017*, *Information and documentation – Records management, Part 1: Concepts and principles*, see *Section 4 Principles for managing records*, *Section 5 Records and records systems*, *Section 7 Appraisal*, *Section 8 Records controls*, *Section 9 Processes for creating, capturing, and managing records*
2. Records and information are reliable and trustworthy.	This requirement builds on the earlier principles in the standard. Records and information need to be accurate, authentic, and reliable - as evidence of	Metadata for managing records and information Mitigating common digital information

	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.	management challenges Minimum requirements for metadata for authoritative records and information *NSW Government Digital Information Security Policy* (April 2015) *NSW Government Information Classification Labelling and Handling Guidelines* (July 2015) *AS ISO 15489.1: 2017, Information and documentation – Records management, Part 1: Concepts and principles*, see *Section 4 Principles for managing records, Section 5 Records and records systems, Section 8 Records controls, Section 9 Processes for creating, capturing, and managing records*
3. Records and information are identifiable, retrievable and accessible for as long as they are required.	This requirement builds on the earlier principles in the standard. 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 digital records and information are 'moved forward' through regular	Mitigating common digital information management challenges Metadata for managing records and information Minimum requirements for metadata for authoritative records and information *Standard on the physical storage of State records* *NSW Government Digital Information Security Policy* (April 2015) *NSW Government Information Classification Labelling and Handling*

	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* for further information.	*Guidelines* (July 2015) *AS ISO 15489.1: 2017, Information and documentation – Records management, Part 1: Concepts and principles*, see, *Section 5 Records and records systems, Section 8 Records controls, Section 9 Processes for creating, capturing, and managing records*
4. Records and information are protected from unauthorised or unlawful access, destruction, loss, deletion or alteration.	This requirement ensures that records and information are protected. 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.	Information security *Standard on the physical storage of State records* *NSW Government Digital Information Security Policy* (April 2015) *NSW Government Information Classification Labelling and Handling Guidelines* (July 2015) *AS ISO 15489.1: 2017, Information and documentation – Records management, Part 1: Concepts and principles*, see, *Section 5 Records and records systems, Section 8 Records controls, Section 9 Processes for creating, capturing, and managing records*
5. Access to records and information is managed appropriately in accordance with legal and business requirements.	This requirement builds on the requirements in Part 6 of the *State Records Act 1998*. 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 to the records of NSW Government *NSW Government Digital Information Security Policy* (April 2015) *NSW Government Information Classification Labelling and Handling*

	(Public Access) Act 2009, *Privacy and Personal Information Protection Act 1998*, *Health Records and Information Privacy Act 2002* and the *State Records Act 1998*. 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.	*Guidelines* (July 2015) Information access resources (Information and Privacy Commission) Privacy resources (Information and Privacy Commission) *AS ISO 15489.1: 2017, Information and documentation – Records management, Part 1: Concepts and principles, see, Section 5 Records and records systems, Section 8 Records controls, Section 9 Processes for creating, capturing, and managing records*
6. Records and information are kept for as long as they are needed for business, legal and accountability requirements.	This builds on the earlier principles in the standard. 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. 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	Making decisions about how long to keep digital information Information is maintained for as long as it needs to be kept for business, community and legislative purposes Retention and disposal authorities Implementing a retention and disposal authority Decommissioning systems Transferring custody of records as State archives Digital State archives Managing the risks of legacy ICT Disposal of digital information

	routinely transferred to NSW State Archives and Records when no longer in use for official purposes.	*AS ISO 15489.1: 2017, Information and documentation – Records management, Part 1: Concepts and principles, see, Section 5 Records and records systems, Section 8 Records controls, Section 9 Processes for creating, capturing, and managing records*
7. Records and information are systematically and accountably destroyed when legally appropriate to do so.	This requirement builds on the earlier principles in the standard. 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.	Retention and disposal authorities Implementing a retention and disposal authority Advice on retention and disposal Disposal of digital information Decommissioning systems Digital information management and digital disposal *AS ISO 15489.1: 2017, Information and documentation – Records management, Part 1: Concepts and principles, see, Section 5: Records and records systems, Section 8: Records controls*

Part 2: Meeting obligations under the State Records Act 1998

The *State Records Act 1998* conveys a number of obligations for public offices. This part of the Guide maps the requirements of the *Standard on records management* to the *State Records Act 1998*.

Obligation under the State Records Act	Requirement in Standard on records management
Obligation to ensure compliance with Act The chief executive of each public office has a duty to ensure that the public office complies with the requirements of this Act and the regulations… (Section 10)	Requirements 1.1, 1.2, 1.3
Obligation to protect records Each public office must ensure the safe custody and proper preservation of the State records that it has control of. (Section 11(1))	Requirements 2.5, 2.6, 3.3, 3.4
Full and accurate records Each public office must make and keep full and accurate records of the activities of the office. (Section 12(1))	Requirements 1.6, 2.1, 2.5, 2.6, 3.1, 3.2, 3.3, 3.4
Records management program Each public office must establish and maintain a records management program for the public office in conformity with standards and codes of best practice from time to time approved under section 13. (Section 12(2))	Requirements 1.1, 1.2, 1.3, 1.4, 1.8
Monitoring and reporting Each public office must make arrangements with the State Archives and Records Authority for the monitoring by the Authority of the public office's records management program and must report to the Authority, in accordance with arrangements made with the Authority, on the implementation of the public office's records management program. (Section 12(4))	Requirements 1.8

Equipment/technology dependent records If a record is in such a form that information can only be produced or made available from it by means of the use of particular equipment or information technology (such as computer software), the public office responsible for the record must take such action as may be necessary to ensure that the information remains able to be produced or made available. (Section 14(1))	Requirements 2.5, 2.6, 3.3, 3.4
Protection of State records 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 State Archives and Records Authority and its Board • 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.	Requirements 2.1, 3.3, 3.4, 3.6, 3.7 See also Procedures for disposal authorisation
Management of State archives 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 State Archives and Records Authority is entitled to control of the record and the public	Requirement 3.6, 3.7 See also Procedures for transferring custody of records as State archives and Digital archives migration methodology

office ceases to be entitled to control of it. (Section 27) A public office that has control of a record that the Authority is entitled to control of is required to make the record available to the Authority. A public office is to comply with the Authority's guidelines as to how records are to be made available. (Section 29)	
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. (Section 51(1))	Requirement 3.5 See also Making access directions

Part 3: *Standard on records management* and *AS ISO 15489.1: 2017 Information and documentation – Records Management, Part 1: Concepts and principles*

NSW State Archives and Records issues standards and codes of best practice under section 13 of the *State Records Act 1998* for use by NSW public offices.

Standards contain **minimum compliance requirements which are mandatory for public offices**. Codes of best practice are industry standards which codify and describe best practice, and are a **benchmark for processes, practices and systems**.

Codes of best practice underpin and support mandatory requirements in standards and will assist a public office in understanding and implementing requirements contained in standards issued by NSW State Archives and Records. Codes of best practice are not designed for a formal auditing framework. Nonetheless, failure to comply with a code of best practice would leave a public office open to criticism in an investigation where recordkeeping practices were an issue.

This part of the Guide includes a mapping demonstrating the relationship between requirements in the *Standard on records management* and *AS ISO 15489.1: 2017 Information and documentation – Records Management, Part 1: Concepts and principles*, issued as a code of best practice in June 2018.

Standard on records management	AS ISO 15489.1: 2017
Principle 1: Organisations take responsibility for records and information management	
1.1 Corporate records and information management is directed by policy and strategy	*Section 6 Policies and Responsibilities*, see 6.1 and 6.2
1.2 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.	*Section 6 Policies and Responsibilities*, see 6.3
1.3 Corporate responsibility for the oversight of records and information management is allocated to a designated individual (senior responsible officer).	*Section 6 Policies and Responsibilities*, see 6.3
1.4 Organisations have skilled records and information management staff or access to appropriate skills.	*Section 6 Policies and Responsibilities*, see 6.3 and 6.5
1.5 Responsibility for ensuring that records and information	*Section 6 Policies and Responsibilities*, see 6.3

management is integrated into work processes, systems, and services is allocated to business owners and business units.	
1.6 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.	*Section 6 Policies and Responsibilities*, see 6.3 and 6.5
1.7 Records and information management responsibilities are identified and addressed in outsourced, cloud and similar service arrangements.	*Section 6 Policies and Responsibilities*, see 6.3 *Section 9 Processes for creating, capturing and managing records*, see 9.6
1.8 Records and information management is monitored and reviewed to ensure that it is performed, accountable and meets business needs.	*Section 6 Policies and Responsibilities*, see 6.4

Standard on records management	AS ISO 15489.1: 2017
Principle 2: Records and information management support business	
2.1 Records and information required to meet short and long term needs are identified.	*Section 4 Principles for managing records* *Section 5 Records and records systems,* see 5.1 - 5.3 *Section 7 Appraisal*, see 7.1 - 7.5 *Section 8 Records controls*, see 8.2, 8.3, 8.5
2.2 High risk and high value areas of business and the systems, records and information needed to support these business areas are identified.	*Section 4 Principles for managing records* *Section 5 Records and records systems, see 5.1 - 5.3* *Section 6 Policies and Responsibilities*, see 6.1 - 6.2 *Section 7 Appraisal*, see 7.1 - 7.5 *Section 8 Records controls*, see 8.3 *Section 9 Processes for creating, capturing and managing records*
2.3 Records and information management is a designed component of all systems and service environments where	*Section 4 Principles for managing records*

high risk and/or high value business is undertaken.	*Section 5 Records and records systems*, see 5.1 - 5.3 *Section 7 Appraisal*, see 7.1 - 7.5 *Section 8 Records controls*, see 8.2 *Section 9 Processes for creating, capturing and managing records*
2.4 Records and information are managed across all operating environments.	*Section 4 Principles for managing records* *Section 5 Records and records systems*, see 5.1 - 5.3 *Section 9 Processes for creating, capturing and managing records*, see 9.6
2.5 Records and information management is designed to safeguard records and information with long term value.	*Section 5 Records and records systems*, see 5.1 - 5.3 *Section 7 Appraisal*, see 7.3 - 7.4 *Section 9 Processes for creating, capturing and managing records*, see 9.6 – 9.8
2.6 Records and information are sustained through system and service transitions by strategies and processes specifically designed to support business and accountability	*Section 5 Records and records systems*, see 5.1 - 5.3 *Section 7 Appraisal*, see 7.3 – 7.4 *Section 8 Records controls*, see 8.3 *Section 9 Processes for creating, capturing and managing records*, see 9.6 – 9.8
Standard on records management	**AS ISO 15489.1: 2017**
Principle 3: Records and information are well managed	
3.1 Records and information are routinely created and managed as part of normal business practice.	*Section 4 Principles for managing records* *Section 5 Records and records systems*, see 5.1 - 5.3 *Section 7 Appraisal* *Section 8 Records controls*, see 8.1 – 8.5 *Section 9 Processes for creating, capturing and managing records*

3.2 Records and information are reliable and trustworthy.	*Section 4 Principles for managing records* *Section 5 Records and records systems*, see 5.1 - 5.3 *Section 8 Records controls*, see 8.1 – 8.4 *Section 9 Processes for creating, capturing and managing records*, see 9.1
3.3 Records and information are identifiable, retrievable and accessible for as long as they are required.	*Section 5 Records and records systems*, see 5.1 - 5.3 *Section 8 Records controls*, see 8.1 – 8.4 *Section 9 Processes for creating, capturing and managing records*, see 9.4 - 9.7
3.4 Records and information are protected from unauthorised or unlawful access, destruction, loss, deletion or alteration.	*Section 5 Records and records systems*, see 5.3 *Section 8 Records controls*, see 8.4 – 8.5 *Section 9 Processes for creating, capturing and managing records*, see 9.5 – 9.9
3.5 Access to records and information is managed appropriately in accordance with legal and business requirements.	*Section 5 Records and records systems*, see 5.3 *Section 8 Records controls*, see 8.4 *Section 9 Processes for creating, capturing and managing records*, see 9.5, 9.6, 9.9
3.6 Records and information are kept for as long as they are needed for business, legal and accountability requirements.	*Section 5 Records and records systems*, see 5.3 *Section 8 Records controls*, see 8.5 *Section 9 Processes for creating, capturing and managing records*, see 9.9
3.7 Records and information are systematically and accountably destroyed when legally appropriate to do so.	*Section 5 Records and records systems*, see 5.3 *Section 8 Records controls*, see 8.5 *Section 9 Processes for creating, capturing and managing records*, see 9.9