



Te Rua Mahara o te Kāwanatanga

ARCHIVES
NEW ZEALAND

Electronic Recordkeeping Metadata Standard

JUNE 2008

ISSUED UNDER THE PUBLIC RECORDS ACT 2005, SECTION 27

THIS STANDARD IS MANDATORY FOR ALL PUBLIC OFFICES
(EXCLUDING SCHOOLS), AND LOCAL AUTHORITIES.

IT IS DISCRETIONARY FOR STATE AND INTEGRATED SCHOOLS.



 tāhūhū te hanga me te tiaki
CONTINUUM

RECORDKEEPING STANDARD S8



Chief Archivist's Overview

The capability to manage corporate information well is fundamental to any successful organisation. The *Electronic Recordkeeping Metadata Standard* identifies some of the key requirements for successful management of information in the electronic recordkeeping environment.

This standard sets out a systematic approach to ensure the information managed in business systems and applications has meaning; also that it can be found when needed; it can be relied on to be what it sets out to be; and it can be moved safely from one system to another. Broad adoption of this standard across central and local government will assist knowledge sharing between organisations; by using shared approaches and processes common outcomes can be achieved.

The standard supports the Public Records Act 2005 requirement for the creation and maintenance of full and accurate business records. For records to be reliable evidence of business activity they must have context, which is documented in recordkeeping metadata.

Recordkeeping metadata documents the creation and use of records by identifying and describing records, including their content and relationships with other records and associated business activities. Recordkeeping metadata is essential to authenticate records and put them into context. Recordkeeping metadata allows you to manage your information assets with confidence and reuse your corporate knowledge to good purpose.

Metadata is often referred to as 'information about information'. Metadata gives a record its wider meaning. We are all familiar with metadata in one form or another. For example, the metadata associated with an email will include: the name of the sender and receiver, the date and time the email was sent and received, and the topic. Without this essential metadata, the purpose of the email will be unclear and its value as evidence will be non-existent.

The *Electronic Recordkeeping Metadata Standard* outlines the minimum requirements for creating and managing recordkeeping metadata. Much of the metadata identified in this standard already exists in common software applications or networks.

Minimum recordkeeping metadata does not necessarily need to be created, but rather located in existing systems and then managed. Where possible the attribution of metadata should be automatic and many business systems and applications have this capability. This standard expects that manual application of metadata is kept to a minimum. Ideally the only metadata users will need to apply manually will be a title that reflects an organisation's business requirements.

The creation and management of recordkeeping metadata requires technical expertise as well as an understanding of information management and recordkeeping. This standard is intended for a predominantly specialist audience. Staff in your organisation with responsibility for information and records management or technology management will need to refer to this document.

The standard is accompanied by *Technical Specifications* that contain a recordkeeping metadata schema that can be modified for use in your organisation's business systems and applications. Organisations are encouraged to use the recordkeeping metadata elements in this document when exceeding the minimums outlined in the standard.

If you have any questions or comments about this standard and the accompanying *Technical Specifications*, Archives New Zealand can advise further.

Signed:

A handwritten signature in cursive script, reading "D. M. Macaskill".

Chief Executive and Chief Archivist

Date: 25 June 2008

Review date: 2012

Acknowledgements

This standard was developed for the Government Recordkeeping Programme, Archives New Zealand by Barbara Reed, Director, Recordkeeping Innovation Pty Ltd, and Kate Jones, Senior Advisor, Government Recordkeeping Programme, Archives New Zealand, with advice and guidance from an advisory group comprising:

- › Claire Benson, Strategic Information Specialist, Ministry of Women's Affairs
- › Robert Eruera, Pou Arahi Taonga / Māori Heritage Librarian, Auckland City Libraries
- › Sarah Heal, Director, Information Leadership Consulting Limited
- › Gregory Jennings, Manager, Context Control Unit, Archives New Zealand
- › Catherine McKinney, Senior Information Management Officer, Department of Labour
- › Richard Murcott, Manager, Geospatial Regulatory Group, Land Information New Zealand
- › Noni Oldfield, Information Architect, Inland Revenue Department
- › Gillian Oliver, Senior Advisor, Digital Sustainability Programme, Archives New Zealand
- › Matt O'Mara, Information Services Manager, Wellington City Council
- › Derek Rayner, Senior Technical Analyst, State Services Commission.

The Chief Archivist acknowledges the advice and guidance of the advisory group members, who have been central to the development of this standard.

This standard operates within a framework of standards, as outlined in section 1.3 *Relationship with other Standards and Requirements*. The work of the National Archives of Australia in developing the *Australian Government Recordkeeping Metadata Standard (AGRkMS)* and the cooperation of Karen Skelton and Andrew Wilson of the National Archives of Australia are particularly noted. The Chief Archivist gratefully acknowledges their assistance in preparing this standard.

Contents

1	Introduction	1
1.1	Purpose	1
1.2	Scope	2
1.3	Relationship with other Standards and Requirements	2
1.4	Advice and Guidance	4
2	Mandate and Responsibilities	5
2.1	Application	5
2.2	Responsibilities	6
2.3	Exemptions	7
2.4	Legislative Basis	7
3	Overview of Standard	9
3.1	Relationship with Technical Specifications	9
3.2	Risk Management	11
4	Principles	14
5	Glossary of Key Terms	25
6	Appendix: Checklist of Minimum Requirements	30

1. Introduction

Under the Public Records Act 2005, public offices and local authorities must create full and accurate records of their activities in accordance with normal, prudent business practice, and ensure that those records are captured into systems which will maintain them in an accessible form for as long as they are required. These systems include recordkeeping metadata.

This standard establishes principles and minimum requirements for creating and managing recordkeeping metadata in electronic environments, in accordance with the Public Records Act 2005. It was developed by Archives New Zealand to ensure that full and accurate records of New Zealand state sector and local government business activity are adequately documented so that they can be managed effectively and continue to be useable over time.

Records consist of information in any format accompanied by metadata which:

- identifies and describes the record, including its contents, context, structural components, conditions of use and security, and relationships with other records, with people and with business being transacted
- identifies past and future events which document recordkeeping actions affecting the record's management and therefore authenticity and integrity.

Records in all formats require metadata to ensure they provide a full and accurate account of an organisation's business activities. While paper records also require metadata for their management, this standard specifically relates to recordkeeping metadata in electronic environments.

1.1 Purpose

The purpose of this standard is to support and improve government recordkeeping. Records cannot be considered authentic and reliable evidence of business without recordkeeping metadata. This standard is designed to:

- establish a framework for recordkeeping metadata applicable to any operational electronic environment in public offices and local authorities, including:
 - records systems/applications which manage records
 - business systems/applications which create and/or create and manage records
 - archival (long-term preservation) systems/applications which preserve and manage records over time
- establish principles for creating, maintaining and managing recordkeeping metadata
- establish a set of recordkeeping metadata elements suitable for use in any electronic system/application that creates or manages records.

1.2 Scope

While metadata applies to all records, regardless of format, this standard is specifically intended for electronic records or records in another format managed by an electronic system.

It applies to all electronic software applications that create or manage records, including dedicated records systems, and business systems/applications that create records.

This standard does not apply to records created in legacy business systems/applications operational before the standard was issued in 2008. However, if such systems are fundamentally redeveloped or have significant functionality added after issue of this standard, then the application of the standard is mandatory.

For a definition of a legacy business system/application please see section 5 *Glossary of Key Terms*.

The standard is accompanied by *Technical Specifications*, which contain a high-level recordkeeping metadata schema and outline options for implementation. For further information see section 3.1 *Relationship with Technical Specifications*.

This standard is intended for use by:

- chief executives, other administrative heads and managers of organisations, as a benchmark for accountability within the organisation
- records, knowledge and information management professionals
- information technology professionals
- all other people in organisations who have responsibility for systems designed to create, receive, manage, store or transmit electronic records.

1.3 Relationship with other Standards and Requirements

While this standard applies specifically to the creation and management of recordkeeping metadata it overlaps with other recordkeeping processes and requirements.

1.3.1 Archives New Zealand Standards

Requirements for other related processes as defined by the Public Records Act 2005 are outlined in other publications issued by Archives New Zealand. Of particular relevance to this standard are:

- the *Create and Maintain Recordkeeping Standard*, which specifies minimum requirements for the making of full and accurate records by public offices and local authorities. The requirements are designed to ensure that records are available for access and maintenance over time, and provide a basis for an assessment of recordkeeping systems, policies and procedures for this purpose

- the *Electronic Recordkeeping Systems Standard*, which sets out functional specifications for electronic recordkeeping systems for use within the New Zealand public sector
- the *Digitisation Standard*, which establishes a framework for maintaining public records and local government protected records in electronic format only, where the original paper, or other non-electronic source record, has been copied.

Reference has been made to these standards in developing the *Electronic Recordkeeping Metadata Standard*, so that it is consistent with the requirements outlined in these standards.

Other relevant standards and guidance issued by Archives New Zealand can be found in the *Continuum Recordkeeping Kit*. All standards will be reviewed and revised over time. An up-to-date list and copies of all *Continuum* publications can be found on Archives New Zealand's *Continuum* website at: <http://continuum.archives.govt.nz/>.

1.3.2 Metadata Standards

This standard is issued in the context of other relevant standards, including international standards, which have been endorsed for use in the New Zealand public sector:

- *ISO 23081-1: 2006 Information and documentation — Records management processes — Metadata for records — Part 1: Principles*
- *AS/NZS ISO 23081-2: 2007 Information and documentation — Records management processes — Metadata for records — Part 2: Conceptual and implementation issues.*

Individual organisations will also need to adhere to metadata standards written for their specific communities or mandated for specific purposes. Examples include:

- *AS/NZS ISO 19115: 2005 Geographic information – Metadata*, of particular relevance to organisations managing records with spatial components such as land, mapping and natural resources organisations
- *CEN EN13606-1 Electronic Healthcare Record Communications, or HL7 Metadata Standards* for implementations of electronic medical records in the health care sector
- *NZGLS New Zealand Government Locator Service Standard*, for discovery metadata.

1.3.3 The Treaty of Waitangi / Te Tiriti o Waitangi

The rights of Māori to their recorded knowledge – which is taonga in the terms of the Treaty of Waitangi – should be respected when this knowledge is incorporated into government records and archives. This standard aims to support the Treaty of Waitangi in respect of Māori cultural practice regarding the identification of records containing traditional or sensitive knowledge and the appropriate management of these records.

1.4 Advice and Guidance

This standard sets out to clearly specify the minimum requirements for recordkeeping metadata. Further guidance documents to help implement the standard in specific environments will be available. The first of these is the *Guide to Recordkeeping Metadata in Electronic Document/Records Management Systems (EDRMS)*.

Advice and guidance on implementation is also available from Archives New Zealand:

Government Recordkeeping Programme
Archives New Zealand
PO Box 12050
Wellington 6144
Telephone: 04 499-5595
Email: rkadvice@archives.govt.nz

❖ 2. Mandate and Responsibilities

This standard is issued under s27 of the Public Records Act 2005. The standard is mandatory for all electronic records created and maintained by all public offices (excluding schools) and all local authorities, as defined and covered by the Act.

Public offices and local authorities are now expected to be working towards compliance with the standard. Full compliance with all requirements in the standard will be expected from 1 July 2010.

All electronic records created after 1 July 2010 must be persistently linked with appropriate metadata as outlined in this standard.

This standard does not apply to records created in legacy business systems/applications operational before the standard was issued in 2008. However, the application of the standard is mandatory when such systems are fundamentally redeveloped or have significant functionality added after issue of this standard.

For a definition of a legacy business system/application please see section 5 *Glossary of Key Terms*.

Compliance with the accompanying *Technical Specifications* is not mandatory.

2.1 Application

The standard is mandatory for:

- public service and non-public service departments
- offices of parliament
- crown entities, including district health boards and tertiary education institutions
- crown entity companies, including crown research institutes
- state enterprises
- regional councils
- territorial authorities
- council-controlled organisations
- council-controlled trading organisations
- local government organisations
- any other public office or local authority as defined in s4 of the Public Records Act 2005.

The standard is discretionary for:

- state and integrated schools.

2.2 Responsibilities

2.2.1 Administrative Head/Chief Executive Responsibilities

Ultimately the organisational administrative head, usually the chief executive, has the responsibility to ensure organisational compliance with the recordkeeping requirements of the Public Records Act 2005, including the requirements of this standard.

The Public Records Act 2005, defines an administrative head within a **public office** as:

- the person responsible for the performance of that office, for example, a chief executive within the meaning of s2(1) of the Public Finance Act 1989
- or for a public office that involves carrying out a statutory function, the holder of that office, for example, the Registrar-General of Land.

The Public Records Act 2005, defines an administrative head within a **local authority** as:

- the person responsible for the performance of the local authority, for example, the chief executive appointed under s42 of the Local Government Act 2002 or the chief executive of an organisation referred to in paragraph (b) of the definition of the term local authority in s4.

Where any doubt exists as to who is the administrative head of an organisation, please contact Archives New Zealand or seek legal advice to clarify the organisational responsibility.

2.2.2 Responsibilities for Records of Functions Carried out under Contract

The Public Records Act 2005 requires public offices and local authorities to create and maintain full and accurate records of their affairs, including records of matters contracted out to independent contractors. The legal obligation to ensure that records of government functions are created and maintained, therefore, rests always with the government entity, not the independent contractor. Depending on the nature of the work being contracted out, this will require either:

- the contractor creating and temporarily maintaining the records of the conduct of the function on behalf of the public office or local authority, or
- the contractor regularly providing the public office or local authority with sufficient information about the function to enable the creation and maintenance of full and accurate records, or
- a combination of the two.

Such records must be created and maintained according to the requirements of this standard. Contracts or agreements with contractors should contain provisions to ensure this can happen.

2.2.3 Compliance Framework

Under the Public Records Act 2005, there are a number of mechanisms to encourage compliance with these responsibilities. These include:

- s26 and s29, the Chief Archivist has the power to inspect public records or local authority records and their storage
- s31, the Chief Archivist may direct a public office or an approved repository to report on any aspect of its recordkeeping practice
- s33-s35, the Chief Archivist must commission independent recordkeeping audits of every public office, and reports on these audits will be presented to Parliament. These audits will start in 2010, and will measure compliance with requirements in this standard
- s61, willful or negligent damage of public records is an offence.

2.3 Exemptions

The Chief Archivist may grant exemptions from compliance with this standard, on certain terms and conditions. Appeals against these decisions may be made to the Minister responsible for Archives New Zealand, who may allow or disallow the appeal after consultation with the appropriate minister and the Archives Council.

Organisations who wish to seek an exemption should follow the process outlined on the Archives New Zealand *Continuum* website <http://continuum.archives.govt.nz/>.

2.4 Legislative Basis

The Public Records Act 2005 imposes the following responsibilities to ensure that public offices and local authorities document their business activities adequately and manage those records for as long as is necessary. (The full text of the Public Records Act 2005, and other New Zealand legislation are available online at www.legislation.govt.nz/).

s17, which requires public offices and local authorities to create and maintain records, states:

- 1) Every public office and local authority must create and maintain full and accurate records of its affairs, in accordance with normal, prudent business practice, including the records of any matter that is contracted out to an independent contractor.
- 2) Every public office must maintain in an accessible form, so as to be able to be used for subsequent reference, all public records that are in its control, until their disposal is authorised by or under this Act or required by or under another Act.
- 3) Every local authority must maintain in an accessible form, so as to be able to be used for subsequent reference, all protected records that are in its control, until their disposal is authorised by or under this Act.

s18 states that no person may dispose of public records or local authority-protected records without authority from the Chief Archivist, unless disposal is required by or under another Act.

s27 allows for the Chief Archivist to issue standards in relation to public records and local authority records.

s28 allows for the Chief Archivist to stipulate the application and content of any recordkeeping standards enacted.

s40 outlines requirements for protected records of local authorities.

Various other acts also support the need for a good standard of recordkeeping by public offices and local authorities in New Zealand. These include (but are not limited to) the following legislation:

- > Official Information Act 1982
- > Local Government Official Information and Meetings Act 1987
- > Public Finance Act 1989
- > Health and Safety Employment Act 1992
- > Financial Reporting Act 1993
- > Privacy Act 1993
- > Copyright Act 1994
- > Electronic Transactions Act 2002
- > Evidence Act 2006.

✘ 3. Overview of Standard

Metadata (or structured data about data) is a concept used by many groups concerned with structuring data for their specific purposes. This standard represents the recordkeeping view of metadata. It is specifically designed to meet the obligations of government organisations under the Public Records Act 2005 to create and maintain records over time.

A record is created to provide evidence of business activity. It may be created in any format. However, the content alone is not sufficient for a record to be considered authentic and reliable. Recordkeeping metadata gives context to the content and ensures that the essential characteristics are persistently linked together to form the record. Recordkeeping metadata enables the record to be managed according to recordkeeping principles.

There are broadly two forms of recordkeeping metadata: the metadata generated at the point the record is created or imported into a system; and the metadata generated as the record is used and maintained by the business.

- ✧ Point of Capture Metadata

The initial context of a record's creation is documented in the metadata and captured at the time a record is ingested/registered into a system which manages it. This metadata is 'fixed', and should not be altered once the record is captured.

- ✧ Recordkeeping Process Metadata

Metadata about the processes of managing the record, including the creation of the record, must be documented to ensure the integrity and authenticity of the record so that alterations, linkages, and uses of the record can be authoritatively tracked over time.

This standard contains principles relevant to creating and managing recordkeeping metadata. These are further refined into requirements against which public offices and local authorities can measure their compliance with this standard.

3.1 Relationship with Technical Specifications

This standard is accompanied by *Technical Specifications* that set out a schema for recordkeeping metadata, including a reference set of metadata elements and encoding schemes.

The *Technical Specifications* is a best practice document. The implementation of the recordkeeping metadata schema defined in the *Technical Specifications* is not mandatory under the Public Records Act 2005. However, this standard does require organisations to map their critical business systems to the recordkeeping metadata schema in the *Technical Specifications* (Requirement 5).

The schema in the *Technical Specifications* is a slightly modified version of the National Archives of Australia's *Australian Government Recordkeeping Metadata Standard (AGRkMS)*. The schema has been modified for use within the New Zealand recordkeeping and legislative environment. It is anticipated that this will form the basis

of an emerging joint Australian and New Zealand (ANZ) recordkeeping metadata schema. When that work is finalised, the *Technical Specifications* will be updated for compliance with the ANZ recordkeeping metadata schema.

The schema represents an emerging consensus on a set of elements applicable to recordkeeping in any environment. The *Technical Specifications* outline elements of recordkeeping metadata which apply to any environment in which records are created and managed. It is forward-looking, anticipating environments capable of managing complex electronic transactional records that exist in webs of relationships. The schema provides a broad reference set of metadata elements, from which individual agencies will be able to draw particular elements suited to their environment, in addition to the minimum required.

The guidance document *Guide to Implementing Recordkeeping Metadata in Electronic Document/Records Management Systems (EDRMS)* will provide modified views of the recordkeeping metadata schema in the *Technical Specifications* suited to specific implementation environments.

The structure of this standard and its relationship to other metadata standards is illustrated below.

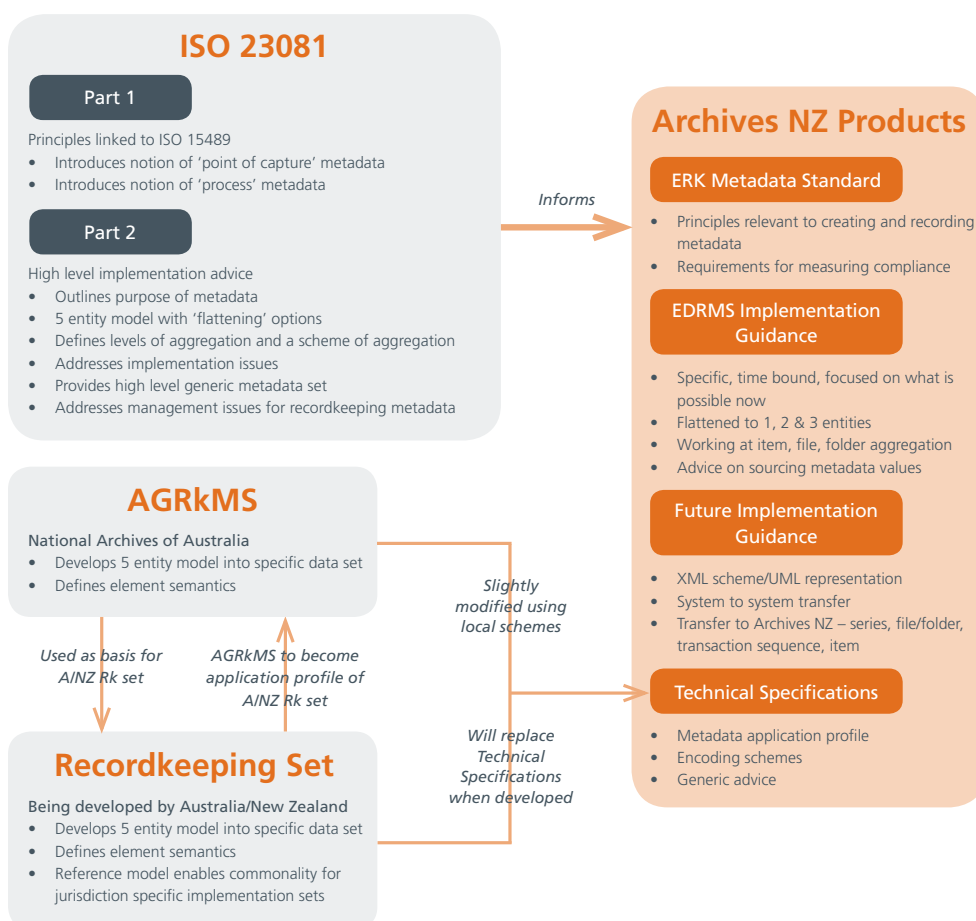


Figure 1: Relationship of this standard to other initiatives

3.2 Risk Management

Recordkeeping can only be successfully undertaken once risk management issues have been considered and addressed. Organisations should assess their systems and procedures against the potential risks associated with not creating and managing appropriate recordkeeping metadata. Organisations should then find ways to mitigate identified risks. The joint Australian and New Zealand standard *AS/NZS 4360:2004 Risk management* and the explanatory companion guidelines set out a framework for assessing risk which can be applied to recordkeeping issues.

Benefits of good recordkeeping can mitigate against the organisational risks of poor or unfocused information management. Recordkeeping metadata allows organisations to specify the information their systems need to capture about records, and provides a standardised way of capturing, managing and using this information. The ultimate benefit of creating and managing recordkeeping metadata is the creation of full and accurate records.

BENEFITS	HIGH LEVEL BUSINESS RISKS MITIGATED
Good management of electronic records.	<p>The inability of organisations to prove the integrity, authenticity and reliability of their electronic records.</p> <p>Insufficient contextual detail to ensure that records are identifiable, and able to be managed and interpreted.</p>
Improved discovery and retrieval of electronic records through sufficient description and the use of controlled vocabularies and other schemes.	<p>The conduct of business activities is inconsistent and inefficient.</p> <p>Inability to exploit organisational information and knowledge to its full potential.</p> <p>Poor strategic planning and poor decisions made on inaccurate information.</p>
Improved security for records and improved implementation of user permissions.	<p>The deliberate and untraceable alteration of records.</p> <p>Lack of trust from clients, customers and the public and damage to business relationships.</p> <p>Greater risk of embarrassment to the chief executive, minister, the government and private individuals.</p>

BENEFITS	HIGH LEVEL BUSINESS RISKS MITIGATED
Reduced risk of data loss, or accidental destruction of records, through the accurate identification and management of electronic records.	Unlawful disposal of records. Failure to meet regulatory and compliance requirements.
The increased ability to demonstrate accountability through the existence of records which document actions and decisions.	Inability to provide evidence of the organisation's activities or undertakings.
Increased public confidence in the integrity of an organisation's records.	Organisational embarrassment, loss of credibility, lowered public confidence and damage to reputation.
Increased opportunities to automate business and recordkeeping processes, such as triggering disposal actions and integrating with workflow processes.	Inability to automate business and recordkeeping processes. Business inefficiencies in key areas and disconnection of workflow management.
Enhanced capability for cross-organisational and cross-business process interoperability.	Inability to transfer data across organisational systems. Systems unable to communicate, resulting in a disconnection of business processes. Business critical information is not accessible for the conduct of business, dispute resolution, legal challenge or evidential purposes.
The protection of organisational records of historical and cultural value, through their transfer to archival repositories.	Responsibility for the loss of information that has enduring value to society and New Zealand's cultural and national identity.

BENEFITS	HIGH LEVEL BUSINESS RISKS MITIGATED
Enhanced credibility and avoidance of financial or legislative penalties by timely production of accurate records of business activity.	<p>Insufficient evidence to resolve disputes in a timely and authoritative manner.</p> <p>Inability to successfully defend legal challenges.</p> <p>Legislative and regulatory compliance cannot be assured.</p>
Identification of vital records for disaster planning, so that organisations can continue to function in the event of severe disruption.	Inability to function or deliver services due to temporary information loss or risk of permanently disabled capability.
An increased ability to plan for migration of records by identifying, in standardised and explicit ways, the software and hardware dependencies of records.	<p>Dependencies on proprietary systems.</p> <p>Inability to transfer data across organisational systems.</p> <p>Inability to retrieve and interpret records in obsolete formats or systems.</p>

Authoritative and credible recordkeeping is essential to good governance and reliable and consistent business practice and service delivery. Organisations may carry out recordkeeping audits and surveys to establish their capability and identify areas of weakness. These processes should form a sound basis for implementing business continuity, contingency and disaster planning programmes.

✂ 4. Principles

This standard has four principles which must be taken into account when defining and managing recordkeeping metadata. Each principle is followed by a statement of its objective and a list of minimum requirements, together with explanations as to why these requirements are considered essential. The principles are:

Principle 1: Recordkeeping Metadata Management Framework

The management of recordkeeping metadata must be defined, documented, assigned and integrated into policies and procedures for records and information management.

Principle 2: Recordkeeping Metadata Creation

Recordkeeping metadata must be created and managed.

Principle 3: Recordkeeping Metadata Maintenance

Recordkeeping metadata must be maintained to reflect business and recordkeeping actions, to sustain the record object throughout its existence, and to enable the transfer of records between systems and organisations.

Principle 4: Recordkeeping Metadata Disposal

Recordkeeping metadata must be subject to the same controls on disposal as applies to all records.

These high level principles are supported and achieved through meeting the requirements outlined in the 'Requirement' column. The requirements are the mandatory part of the standard. The requirements are focused on outcomes and the standard is not prescriptive about how these outcomes are achieved. This framework is concerned with identifying outcomes rather than prescribing specific recordkeeping practices.

To help clarify the intent of each requirement, there are corresponding explanations in the next column. The 'Explanation' column does not add any additional obligations. Terms such as 'should' and 'will' are used purely in an explanatory sense.

Principle 1: Recordkeeping Metadata Management Framework

The management of recordkeeping metadata must be defined, documented, assigned and integrated into policies and procedures for records and information management.

Please note this principle complements requirements in Archives New Zealand's *Create and Maintain Recordkeeping Standard*, particularly:

- Principle 1, Requirement 2: Organisations must have a defined, documented and implemented policy for recordkeeping, which is regularly reviewed
- Principle 4: Records must be managed systematically across both recordkeeping systems and business systems within an organisational recordkeeping framework.

REQUIREMENT	EXPLANATION
<p>Requirement 1: Records and information management policies and procedures must specify the role of recordkeeping metadata in ensuring authenticity, reliability, and integrity.</p>	<p>Recordkeeping metadata is a core component of managing records, particularly electronic records. As such, it should be explicitly referenced in the records and information policies of a public office or local authority.</p> <p>In particular, the distinction between recordkeeping point of capture metadata and process metadata should be included, as this is a key factor in making recordkeeping different to other information communities' understanding and use of metadata.</p> <p>See <i>Guide to Developing a Recordkeeping Policy</i> at: http://continuum.archives.govt.nz/.</p>
<p>Requirement 2: Responsibility for:</p> <ul style="list-style-type: none"> ➤ creating, maintaining and altering an organisation's recordkeeping metadata schemas and encoding schemes ➤ attribution and verification of point of capture recordkeeping metadata <p>must be assigned, documented, communicated and regularly reviewed.</p>	<p>Recordkeeping metadata elements are often modified for specific implementation purposes. Responsibility must be assigned for identifying additions or variations to the organisation's recordkeeping metadata schema.</p> <p>Local encoding schemes are used to manage classification, security, disposal actions, titling protocols, and other areas of recordkeeping. Responsibility for their use and documentation must be assigned.</p> <p>Employees have responsibilities for records creation which may include manually adding metadata. Procedures should be defined to apply quality checking across manually attributed metadata, whether this is by the creator, by sampling or by automatic analysis. These responsibilities must be assigned and documented.</p> <p><i>(See also Requirement 10.)</i></p>

REQUIREMENT	EXPLANATION
<p>Requirement 3: Rules relating to changing recordkeeping metadata must be defined.</p>	<p>Records must be tamper-proof and authentic. Changing recordkeeping metadata can significantly alter the meaning, accessibility, and authenticity of the record object. Tight procedural controls are needed to define who, and in what situations, may change (as opposed to 'add to') already existing recordkeeping metadata.</p> <p>In some limited circumstances, change to metadata may be permitted – for example, in maintaining correct personal details under the Privacy Act 1993.</p> <p><i>(See also Requirement 11.)</i></p>
<p>Requirement 4: Metadata schema and encoding schemes must be maintained, documented and communicated.</p>	<p>Metadata schema and encoding schemes are key control tools for electronic recordkeeping and explain the parameters and meanings of metadata values allocated to electronic records.</p> <p>The metadata schema and encoding schemes must be maintained and kept up-to-date to reflect business requirements and particularly language usage.</p> <p>Some organisations will do this through a formal metadata registry structure that manages changes and versions, others will not use such formal structures. Regardless, versions and a record of changes to these control tools must be maintained and their validity periods clearly identified.</p> <p>Metadata schema and associated encoding schemes are also records and should be managed as such.</p>
<p>Requirement 5: Metadata in all business-critical systems/applications which create records must be mapped to the recordkeeping metadata schema in the accompanying <i>Technical Specifications</i>.</p>	<p>It is expected systems/applications that manage electronic records, such as Electronic Document/Records Management Systems (EDRMS), comply with this standard. However, many other systems/applications exist within organisations, some of which are critical to undertaking the business of the organisation. Each organisation will determine what constitutes a business critical system/application. These systems are to be mapped to the recordkeeping metadata schema established in the <i>Technical Specifications</i>.</p> <p>Creating mappings between the business system/application and the recordkeeping metadata schema in the accompanying <i>Technical Specifications</i> will:</p> <ul style="list-style-type: none"> > increase knowledge and understanding of the recordkeeping metadata schema > enable extraction of records from business systems/applications for migration to new systems, transfer to another agency or for longer-term retention > enable organisations to determine strategies for maintaining compliant records within the business system/application.

Principle 2: Recordkeeping Metadata Creation

Recordkeeping metadata must be created and managed.

REQUIREMENT	EXPLANATION
<p>Requirement 6: Recordkeeping metadata must be assigned to or associated with all record objects and aggregations.</p>	<p>Records are often managed as aggregations.</p> <p>Files/folders or transaction sequences, such as the sequence of processes involved in executing an online transaction, are aggregations of individual records. Every level of record aggregation requires metadata to accompany its creation and management.</p> <p>Managing records in aggregations enables inheritance of controls from higher to lower aggregations, thus enhancing opportunity for automation and reducing the creation and management of unnecessarily duplicated metadata and minimising unnecessary variation.</p>
<p>Requirement 7: Organisations must document their decisions about the attribution of recordkeeping metadata.</p>	<p>The amount of recordkeeping metadata applied to records must be determined according to risk assessment strategies associated with the business being done.</p> <p>International standards and the accompanying <i>Technical Specifications</i> outline five metadata entities: record; agent; business; mandate; and relationship. Organisations may implement these as separate entities, or may choose to 'flatten' them and bring all mandatory elements into fewer entities. The most minimalist implementation must have at least one entity – records – into which the other mandatory elements are subsumed. See the <i>Guide to Recordkeeping Metadata in Electronic Document/Records Management Systems (EDRMS)</i> for more information.</p> <p>Minimum recordkeeping metadata elements are specified in Requirements 8 and 9 of this standard. Beyond these minimum requirements, each organisation should determine what is required for its business purposes. Where exposure to business risk is acceptable, organisations may comply with the minimum requirements only. Such decisions must be documented and justified.</p> <p><i>(See also Requirements 8, 9 & 13.)</i></p>

REQUIREMENT	EXPLANATION
<p>Requirement 8: At point of capture of a record object, the following minimum recordkeeping metadata must be attributed:</p> <ul style="list-style-type: none"> > a unique identifier > a name > date of creation > who created the record > what business is being conducted > creating application and version. 	<p>These metadata elements are the absolute minimum which must be addressed when a record object is captured as a record. They represent a minimalist approach, lower than that outlined in the accompanying <i>Technical Specifications</i>. The intent is to specify elements which should be possible to identify from most record-creating software. They are inadequate to ensure a full and accurate record but will enable an organisation to reconstruct some context, enabling it to defend the record's authenticity. Without these minimal metadata elements, reconstruction of a complete record is impossible.</p> <p>If only the minimum metadata is captured, reconstructing the context of the records after the event may be costly.</p> <p>These minimum metadata elements are defined below. The intention is to enable organisations to capture existing metadata associated with a record object in its creating software application.</p> <ul style="list-style-type: none"> > <i>Unique identifier:</i> a unique identifier for the entity, enabling retrieval of this record object and no other within its recordkeeping context. This may be achieved using a combination of data fields. This is represented by element 2 'Identifier' in the <i>Technical Specifications</i>. See section 5 <i>Glossary of Key Terms</i> for further explanation. > <i>Name:</i> the title or name given to the record object. This is represented by element 3 'Name' in the <i>Technical Specifications</i>. > <i>Date of creation:</i> the date the record object is first saved or entered into the system. In some circumstances it is possible to automatically capture the date/time associated with this action and organisations are encouraged to capture this information if it is available. This is represented by element 4.1 'Date Range: Start Date' in the <i>Technical Specifications</i>. > <i>Who created the record:</i> ideally this would identify the author (person or system) of the record, the signatory, and (if different) the person responsible for the capture. This may not always be possible, so organisations are required to capture what details they are able to from the metadata assigned automatically by the creating application. This is represented by element 3, 'Name' when referencing the Agent entity in the <i>Technical Specifications</i> in a multi-entity implementation, or by the 'Agent.Name' element in a flattened single entity implementation. > <i>What business is being conducted:</i> ideally this will capture the breakdown of business activity and function, from a business classification scheme. However, where such a formal recordkeeping tool does not exist, the names of network folders might be appropriate, or a description taken from the name of the business system – e.g. SAP Financial Asset Management or Complete Human Resources Information System (CHRIS). This is represented by a number of elements in the <i>Technical Specifications</i>, depending on the source of the values. Options include element 3 'Business.Name', element 17 'Record.Keyword', (if a structured business classification scheme is used), or in the case of a network directory path it could be element 3 'Record.Name'.

REQUIREMENT	EXPLANATION
	<ul style="list-style-type: none"> ➤ <i>Creating application and version:</i> the name and version of the software application that created the record. This is represented by element 19.3 'Format: Creating Application Name' and element 19.4 'Format: Creating Application Version' in the <i>Technical Specifications</i>. <p>For example, most of these elements can be taken from the 'properties' elements or network directory structures associated with a document in common office software. Using the metadata associated with an electronic 'word' document, the values would be:</p> <ul style="list-style-type: none"> ➤ A unique identifier (path name, document name, date): <i>S:\current clients\Archives NZ metadata standard\Consultation\Post exposure comments\Recordkeeping Metadata Standard Exposure Draft – Editorial Comments from Submissions Process – Track Changes Document 19.02.08.doc</i> ➤ A name: <i>BR Recordkeeping Metadata Standard Exposure Draft – Editorial Comments from Submissions Process – Track Changes Document</i> ➤ Date of creation: <i>Tuesday, 19 February 2008</i> ➤ Who created the record: <i>Barbara Reed, Recordkeeping Innovation Pty Ltd</i> ➤ What business is being conducted (from folder structure): <i>Current Clients\Archives NZ Metadata Standard\Consultation\Post exposure resolution</i> ➤ Creating application and version: <i>Microsoft Word 97-2003 Document</i>. <p><i>(See also Requirements 7 & 9.)</i></p>
<p>Requirement 9: For each action undertaken on a record object the following minimum recordkeeping process metadata must be maintained:</p> <ul style="list-style-type: none"> ➤ the date of the action ➤ the identification of the person or system undertaking the action ➤ what action was undertaken. 	<p>Many electronic systems/applications maintain this type of information in audit trails. However, to meet this standard, actions need to be linked to the record object, and able to be accessed at the same time as the record object.</p> <p>The ability to authoritatively assert who has created, accessed, modified or destroyed a record is critical to ensure authenticity, reliability, and integrity.</p> <p>Most commonly used office software suites create such data at a minimum level within the properties associated with documents. This data may be sufficient to enable reconstruction of the actions connected to a record object.</p> <p>Audit trails and properties relied upon for any necessary reconstruction of records will need to be retained for as long as the record object itself.</p> <p>The application of this minimum metadata only, may result in the need for reconstruction of the record. This is a prohibitive process involving significant manual resources and interpretation.</p> <p>In the <i>Technical Specifications</i>, event histories are recorded as relationships between records and agents, with the preceding or superseded value documented in element 7 'Change History'.</p> <p><i>(See also Requirements 7 & 8.)</i></p>

REQUIREMENT	EXPLANATION
<p>Requirement 10: Organisations must identify where requirements to extend the recordkeeping metadata exist.</p>	<p>The recordkeeping metadata defined in this standard and in the accompanying <i>Technical Specifications</i> represents a recordkeeping perspective. Organisations also exist within many specialty domains and industry areas. They may have requirements specific to those domains that can be expressed in metadata and assigned to records. The metadata defined for recordkeeping may be extended to suit business requirements of individual organisations, industries, or professions.</p> <p>Extensions often involve adding terminology commonly used in a specific discipline or industry. This may be accommodated by incorporating subject taxonomies as approved encoding schemes at item or file levels. However, where necessary, additional metadata elements or sub-elements can be added to the metadata schema.</p> <p>Care should be taken to ensure that the precise meaning of metadata elements taken from another domain are appropriately interpreted into the records metadata schema.</p> <p>Further guidance on extending recordkeeping metadata schemas is included in the appendices of the <i>Guide to Implementing Recordkeeping Metadata in Electronic Document/Records Management Systems (EDRMS)</i>.</p> <p><i>(See also Requirement 2.)</i></p>

Principle 3: Recordkeeping Metadata Maintenance

Recordkeeping metadata must be maintained to reflect business and recordkeeping actions, to sustain the record object throughout its existence, and to enable the transfer of records between systems and organisations.

REQUIREMENT	EXPLANATION
<p>Requirement 11: Recordkeeping metadata must be persistently linked with a record object for its entire period of retention.</p>	<p>Records consist of both the content (record object) and the recordkeeping metadata associated with the context and management of the content.</p> <p>Recordkeeping process metadata provides the accumulating history of events, changes, and actions undertaken on the record object and its metadata. This metadata provides the evidence of management processes and is essential to proving authenticity and reliability.</p> <p>The recordkeeping metadata does not need to be stored with the record object, but may be stored, for example, in an associated database, or in separate indexes or registers. However, persistent links between the metadata and the record object must be maintained for the whole of the record's existence.</p> <p>Care is needed when referencing metadata stored externally to the record and which may be dynamically updated – that is overwritten to maintain the most recent information. For recordkeeping metadata to maintain the meaning, metadata must be static, or maintained at the specific point in time the reference is made. For example, details about individuals may be stored in an online organisational directory which maintains the most recent position filled by a specific individual. However, for recordkeeping it is important to know what position that person held at the time the record was created/captured or action undertaken. The newer (dynamic) data should not overwrite the static (point of time) metadata linked to the record.</p> <p><i>(See also Requirements 3, 12 & 14.)</i></p>

REQUIREMENT	EXPLANATION
<p>Requirement 12: Recordkeeping metadata must accompany record objects being transferred from their original creating environment or system.</p>	<p>As explained in Requirement 11, recordkeeping metadata can be stored separately to the record object. However, once transferred outside its creating environment, the recordkeeping metadata must be copied or persistently linked with the record object to enable the content to be appropriately interpreted. This is a particular threat in migration processes.</p> <p>When moving records from a creating environment, additional metadata may need to be added to provide context to the record. For example, within a single creating environment such as the State Services Commission (SSC), there is no need to explicitly nominate that the record belongs to the SSC, but when it is moved, shared or used to transact business outside the SSC, the record needs to clearly identify it originated from the SSC. Or, as a further example, when transmitting records outside the organisation, to comply with the Government Communications Security Bureau's¹ (GCSB) requirements, it may be necessary to add a security classification to alert the receiver. This was unnecessary when the record was contained within the organisation's own environment or systems. Similarly, it may be necessary to augment the identifier of a record with an agency name or identifier to ensure that the record identifier remains unique in a cross organisational environment.</p> <p>Recordkeeping metadata should be able to be expressed in standard formats (such as XML) so other applications can receive and process the metadata.</p> <p>Where a business decision is taken at migration to move only selected elements of the metadata to a new environment within the original organisation, this constitutes a business appraisal decision and is subject to Requirements 13-15, but will not require Archives New Zealand's approval.</p> <p><i>(See also Requirement 11.)</i></p>

¹ GCSB: Government Communications Security Bureau: *NZ ICT Security Manual* <http://www.gcsb.govt.nz/publications/nzsit/index.html>

Principle 4: Recordkeeping Metadata Disposal

Recordkeeping metadata must be subject to the same controls on disposal as apply to all records.

REQUIREMENT	EXPLANATION
<p>Requirement 13: Recordkeeping metadata must be subject to appraisal decisions prior to its disposal.</p>	<p>The general expectation is that recordkeeping metadata will be retained for at least as long as the record object to which it relates.</p> <p>However, at system set up, decisions about which recordkeeping process metadata to document are made at the discretion of an organisation and should be documented and justified in the system documentation. For example, an organisation may choose not to maintain a record of who has accessed a record for longer than one year after the record was created, or only details of a certain number of the last locations may be maintained.</p> <p>Such decisions may affect the capacity of the organisation to prove the complete story of interactions with a record and may therefore compromise the integrity and authenticity of a record. These are decisions based on risks associated with the business and legislative requirements.</p> <p>Because recordkeeping metadata may exist physically separately from the record object, it is capable of supporting disposal actions independent of the record object. Where an organisation seeks to vary the general expectation that the recordkeeping metadata will be retained for at least as long as the record object to which it relates, this is an appraisal decision. Such appraisal decisions should be documented and appropriately authorised by Archives New Zealand in accordance with normal appraisal processes.</p> <p><i>(See also Requirements 7, 12 & 14.)</i></p>
<p>Requirement 14: Recordkeeping metadata must be protected from unauthorised disposal.</p>	<p>Authority to dispose of a record object does not necessarily imply authority to dispose of its associated metadata.</p> <p>Following Requirements 3 and 11, recordkeeping metadata disposal must be authorised and documented.</p> <p>Where disposal is authorised as part of the organisation's disposal authority issued under the Public Record Act 2005, full details of the person undertaking or authorising the disposal action, the reasons for the action, the results of the action, and a date/time of action should be documented.</p> <p>This requirement can be met by creating a record of the disposal event in the recordkeeping metadata.</p> <p><i>(See also Requirements 11, 13 & 15.)</i></p>

REQUIREMENT	EXPLANATION
<p>Requirement 15: After authorised disposal actions on a record are implemented (including transfer and destruction), the following minimum recordkeeping metadata must be retained for as long as is required by the business:</p> <ul style="list-style-type: none"> > point of capture metadata including a unique identifier, a name, date of creation, who created the record, what business is being conducted, and the creating application and version > the date the disposal action took place > the authority governing the record's destruction > the person/role undertaking the disposal action. 	<p>Where the record object or contents of a record is transferred or destroyed, evidence of its existence and the authorised actions undertaken to dispose of the record must be kept for a longer period which is subject to negotiation in the appraisal process. This allows the organisation to unambiguously assert the fate of a record.</p> <p>Organisations will be compliant with this requirement if they create, in a new record, a summary report aggregating individual instances of these metadata elements for identifiable records.</p> <p><i>(See also Requirement 14.)</i></p>

✘ 5. Glossary of Key Terms

Included are definitions of terms specific to this standard. For definitions of more general terms please see the *Glossary of Archives and Recordkeeping Terms* at <http://continuum.archives.govt.nz/> .

Aggregation:

An ordered sequence of related records. For example, within the entity 'agent', an individual, a work unit, a department, a division, a branch or the organisation as a whole can be described. Within the entity class 'record', an item, a folder, a file, a series, etc, can be described. Each of these layers is referred to as an aggregation.

Application profile:

An application profile delineates the use of metadata elements declared in an element set. While an element set establishes concepts, as expressed via metadata elements, and focuses on the semantics or meanings of those elements, an application profile goes further and adds business rules and guidelines on the use of the elements. It identifies element obligations and constraints, and provides comments and examples to assist in the understanding of the elements. Application profiles may include elements integrated from one or more element sets thus allowing a given application to meet its functional requirements.

Authenticity:

An authentic record is one that can be proven:

- 1) to be what it purports to be
- 2) to have been created or sent by the person or system purported to have created or sent it
- 3) to have been created or sent at the time purported.

Business activity:

An umbrella term covering all functions, processes, activities and transactions of an organisation and its employees to produce a product and/or service in the conduct or normal business practice. This includes public administration as well as commercial business.

Business system/application:

Software designed to manage interrelated business processes and information, to achieve business outcomes.

Capture:

The process of fixing the content, structure and context of a record to ensure that it is a reliable and authentic representation of the business activities or transactions in which it was created or transmitted.

Control tools:

Specific recordkeeping tools that govern the processes and descriptions of:

- > registration – provides evidence of the existence of records in a recordkeeping system
- > classification – allows for appropriate grouping, naming, security protection, user permissions and retrieval
- > indexing – allocates attributes or codes to particular records to assist in their retrieval
- > tracking – provides evidence of where a record is located, what action is outstanding on a record, who has seen a record, when such access took place and the recordkeeping transactions that have been undertaken on the record
- > disposal – refers to the many options in relation to the fate of public records and local authority records including: transfer of control to Archives New Zealand or any other public office/local authority, destruction, sale, alteration, or discharge.

Context:

The knowledge necessary to sustain a record's meaning or evidential value. Context describes the 'who, what, where and why' of record creation and management.

Destruction:

The process of eliminating a record from a system beyond any possible reconstruction.

Disposal:

The final decision concerning the fate of records, i.e. destruction or transfer to archives. On rare occasions the disposal may be by sale or donation.

Within the legal framework of New Zealand, disposal, in relation to a public record or local authority record, means:

- 1) the transfer of control of a record
- 2) the sale, alteration, destruction, or discharge of a record.

Electronic record:

Record consisting of information stored in a form based not on human readable symbols but on a binary encoding, which can be manipulated by computers and therefore be made readable by humans. An electronic record consists of both a record object and recordkeeping metadata.

Encoding schemes:

Schemes that aid in the interpretation of an element value. These schemes include controlled vocabularies and formal notations or parsing rules. A value expressed using an encoding scheme will thus be a token selected from a controlled vocabulary (e.g. a term from a classification system or set of subject headings) or a string formatted in accordance with a formal notation.

Entity:

See *Metadata entity*.

Export:

The process of formatting data in such a way that it can be used by another application and can be passed from one system to another system, either within the organisation or elsewhere. An application that can export data can create a file in a format that another application understands, enabling the two programmes to share the same data. Export (rather than transfer) does not necessarily mean removing data from the first system.

Extensible:

Having the potential to be expanded in scope, area or size. The ability to extend a core set of metadata with additional elements.

Integrity:

The integrity of a record refers to it being complete and unaltered. Integrity is protected via control measures such as access monitoring, user verification, authorised destruction and security.

Legacy:

For the purposes of this standard only, legacy shall mean systems/applications existing before the issue of the standard in June 2008.

Mapping:

A chart or table that identifies the semantic equivalent (meaning or function) of data elements in a metadata standard to fields or data elements that have similar function or meaning occurring in a business system/application.

Metadata:

Structured information that describes and/or enables finding, managing, controlling, understanding or preserving other information over time.

See also, *Recordkeeping metadata*.

Metadata element:

A discrete unit of data. An element may contain sub-elements. Note: equivalent to 'attribute' in UML (Unified Modelling Language) terminology.

Metadata element set:

See *Metadata schema*.

Metadata entity:

Set of metadata elements describing the same aspect of data e.g. record, agent, mandate, business or relationship.

Note: equivalent to 'class' in UML terminology.

Metadata schema:

Framework that specifies and describes a standard set of metadata elements and their interrelationships. Note: Schemas provide a formal syntax (or structure) and semantics (or definitions) for the metadata elements.

Metadata values:

The content of a metadata element, which provides information about a characteristic or attribute of a resource.

Point of capture metadata:

Metadata that documents the business context in which records are created, as well as the content, structure and appearance of those records.

Process metadata:

Metadata that documents records management and business processes in which records are subsequently used, including any changes to the content, structure and appearance.

Reconstruction:

The process of retrospectively identifying the data needed to recreate a defensible set of events relating to the creation, alteration, management and destruction of a record. This includes who has undertaken the events, the sequence of action and when they took place.

Record:

Information, whether in its original form or otherwise, including (without limitation) a document, a signature, a seal, text, images, sound, speech, or data compiled, recorded, or stored:

- 1) in written form on any material
- 2) on film, negative, tape, or other medium so as to be capable of being reproduced
- 3) by means of any recording device or process, computer, or other electronic device or process.

An electronic record consists of both a record object and recordkeeping metadata.

Record object:

The physical or logical group of data, existing at the lowest level of aggregation of a record, containing the electronic content of a transaction.

Recordkeeping metadata:

Data that enables the creation, management and use of records through time. Recordkeeping metadata can be used to identify, authenticate and contextualise records and the people, processes and systems that create, manage and use them.

Schema:

See *Metadata schema*.

Tamper-proof:

Made resistant to interference. Protection against tampering, or the deliberate altering or adulteration of a record.

Transaction:

The smallest unit of business activity. The use of a record is itself a transaction.

Unique Identifier:

A string of characters assigned to a record object enabling retrieval of this record object and no other within its recordkeeping context.

Note: a unique identifier may be derived from multiple existing data elements or may be system assigned when a record is created. If the identifier contains data that may change over time e.g. a path name, then a change process will be needed to ensure external links that use the identifier can still be resolved after an update. It may also be necessary to update identifiers when records are moved to a different system or location so uniqueness can be guaranteed. If organisational systems allow, it could be advantageous to investigate use of a standard universal identifier and namespace.

✘ 6. Appendix: Checklist of Minimum Requirements

This checklist is a tool for managing risks associated with recordkeeping metadata. It can be used to assess compliance with the standard. Where a requirement is not met, an organisation must assess the risks involved and plan to address them.

PRINCIPLE/REQUIREMENT	YES	NO	IF NO, WHAT RISKS EXIST?	ACTIONS REQUIRED TO TREAT RISKS
<p>Principle 1: Recordkeeping Metadata Management Framework</p> <p><i>The management of recordkeeping metadata must be defined, documented, assigned, and integrated into policies and procedures for records and information management.</i></p>				
<p>Requirement 1: Records and information management policies and procedures must specify the role of recordkeeping metadata in ensuring authenticity, reliability, and integrity.</p>				
<p>Requirement 2: Responsibility for:</p> <ul style="list-style-type: none"> > creating, maintaining and altering an organisation's recordkeeping metadata schemas and encoding schemes > attribution and verification of point of capture recordkeeping metadata <p>must be assigned, documented, communicated and regularly reviewed.</p>				
<p>Requirement 3: Rules relating to changing metadata must be defined.</p>				

PRINCIPLE/REQUIREMENT	YES	NO	IF NO, WHAT RISKS EXIST?	ACTIONS REQUIRED TO TREAT RISKS
Requirement 4: Metadata schema and encoding schemes must be maintained, documented and communicated.				
Requirement 5: Metadata in all business critical systems/ applications which create records must be mapped to the recordkeeping metadata schema in the accompanying <i>Technical Specifications</i> .				
Principle 2: Recordkeeping Metadata Creation <i>Recordkeeping metadata must be created and managed.</i>				
Requirement 6: Recordkeeping metadata must be assigned to all record objects and aggregations.				
Requirement 7: Organisations must document their decisions about the attribution of recordkeeping metadata.				

PRINCIPLE/REQUIREMENT	YES	NO	IF NO, WHAT RISKS EXIST?	ACTIONS REQUIRED TO TREAT RISKS
<p>Requirement 8: At point of capture of a record object, the following minimum recordkeeping metadata must be attributed:</p> <ul style="list-style-type: none"> > a unique identifier > a name > date of creation > who created the record > what business is being conducted > creating application and version. 				
<p>Requirement 9: For each action undertaken on a record, the following minimum recordkeeping process metadata must be maintained:</p> <ul style="list-style-type: none"> > the date of the action > identification of the person or system undertaking the action > what action was undertaken. 				
<p>Requirement 10: Organisations must identify where requirements to extend the recordkeeping metadata exist.</p>				
<p>Principle 3: Recordkeeping Metadata Maintenance</p> <p><i>Recordkeeping metadata must be maintained to reflect business and recordkeeping actions, to sustain the record object throughout its existence and to enable the transfer of records between systems and organisations.</i></p>				

PRINCIPLE/REQUIREMENT	YES	NO	IF NO, WHAT RISKS EXIST?	ACTIONS REQUIRED TO TREAT RISKS
Requirement 11: Recordkeeping metadata must be persistently linked with a record object for its entire period of retention.				
Requirement 12: Recordkeeping metadata must accompany record objects being transferred from their original creating environment or system.				
Principle 4: Recordkeeping Metadata Disposal <i>Recordkeeping metadata must be subject to the same controls on disposal as apply to all records.</i>				
Requirement 13: Recordkeeping metadata must be subject to appraisal decisions prior to its disposal.				
Requirement 14: Recordkeeping metadata must be protected from unauthorised disposal.				

PRINCIPLE/REQUIREMENT	YES	NO	IF NO, WHAT RISKS EXIST?	ACTIONS REQUIRED TO TREAT RISKS
<p>Requirement 15: After authorised disposal actions on a record are implemented (including transfer or destruction), the following minimum recordkeeping metadata must be retained for as long as is required by the business:</p> <ul style="list-style-type: none"> > point of capture metadata including a unique identifier, a name, date of creation, who created the record, what business is being conducted, and the creating application and version > the date the disposal action took place > the authority governing the record's destruction > the person undertaking the disposal action. 				



Electronic Recordkeeping
Metadata Standard

ISSN 1176-2713

ISBN 978-0-478-18224-8

