Principles and functional requirements for records in electronic office environments
Principles and functional requirements for records in electronic office environments

Module 1

Overview and statement of principles
# CONTENTS

1 INTRODUCTION 4
   1.1 Scope and purpose 4
   1.2 Audience 5
   1.3 Related standards 5
   1.4 Structure and use 5

2 GOOD PRACTICE: ELECTRONIC RECORDS AND THE ROLE OF SOFTWARE 7

3 GUIDING PRINCIPLES 8
   3.1 Records-related principles 8
   3.2 Systems-related principles 9

4 IMPLEMENTATION ISSUES 10
   4.1 Components of successful electronic business information management 10
   4.2 Risks and mitigations 11
   4.3 Financial and organisational sustainability of electronic systems 13

5 OTHER FUNCTIONAL REQUIREMENTS REFERENCED AND EVALUATED 14

6 GLOSSARY 17
1 INTRODUCTION

A variety of functional specifications for records management software has been developed in the international community. In 2006, the International Council on Archives agreed to develop a harmonised, generic suite of recordkeeping functional requirements for software products based on existing jurisdiction-specific specifications, and to do so in a manner consistent with the International Standard on Records Management, ISO 15489. It is hoped that this suite of guidelines and functional requirements will assist jurisdictions that are developing, or looking to adopt, their own functional specifications, as well as inform the update and revision of previously existing standards. The application of this set of functional requirements is not only meant to inform the development of electronic records management software, but also to aid in the incorporation of recordkeeping functionality into generic business information systems software products, as well as specific line-of-business systems. These specifications can also be used by the private sector (for example, multinational corporations) as a stand-alone tool.

Principles and Functional Requirements for Records in Electronic Office Environments was sponsored by the International Council on Archives as a project in its Electronic Records and Automation Priority Area, lead by George Mackenzie, Director of the National Archives of Scotland. Adrian Cunningham (National Archives of Australia) was Project Coordinator. Archives New Zealand (Stephen Clarke) acted as the Secretariat for the project. Other participating countries included Cayman Islands (Sonya Sherman), United Kingdom – England and Wales (Richard Blake), Germany (Andrea Hänger and Frank Bischoff), Malaysia (Mahfuzah Yusuf and Azimah Mohd Ali), Netherlands (Hans Hofman), Scotland (Rob Mildren and Steve Bordwell), South Africa (Louisa Venter), Sweden (Göran Kristiansson), France (Olivier de Solan) and the United States (Mark Giguere). The project was also supported by the Australasian Digital Recordkeeping Initiative, a collaborative venture sponsored by the Council of Australasian Archives and Records Authorities. ADRI member Queensland State Archives (Rowena Loo and Anna Morris) contributed to the drafting of Module 3.

1.1 Scope and purpose

The aim of the Principles and Functional Requirements for Records in Electronic Office Environments project is to produce globally harmonised principles and functional requirements for software used to create and manage electronic records in office environments. There currently exist a number of jurisdiction-specific functional requirements and software specifications. The project’s objective is to synthesise this existing work into requirements and guidelines to meet the needs of the international archival community and to enable that community to liaise, in a consolidated manner, with the global software industry.

The objectives of the project are to:

- enable better recordkeeping in organisations at all levels of government regardless of juridical domain;
support the business needs of an organisation by enabling greater effectiveness and efficiency of the operations;

provide, through wider deployment of automated recordkeeping functionality, enhanced abilities to support auditing activities;

improve capabilities to comply with statutory mandates specified in various information-related legislation (for example, data protection and privacy);

ensure good governance (for example, accountability, transparency and enhanced service delivery) through good recordkeeping;

increase general awareness of automated recordkeeping capabilities via the dissemination of key principles; and

maximise cross-jurisdictional consistency regarding the articulation of recordkeeping functional requirements and to enable the global archival community to speak with one voice to the software vendor community.

The primary focus of this suite of guidelines and requirements is the creation and management of electronic records. While the modules support the long-term preservation of digital records, processes to achieve this are beyond the scope of the project. It is anticipated that the application of the requirements will be global in nature. Therefore, it is impossible, given the wide juridical range of potential applications, to include detailed implementation guidelines. In addition, as the ultimate testing environment for the basis of these modules is yet to be determined, inclusion of specific software test cases or scripts was deemed beyond the scope of the modules.

1.2 Audience

There are four key audiences for these modules:

- software developers and vendors – including non-records management software, so this document can serve as a universal benchmark for recordkeeping compliance;

- jurisdictional standard-setters – so these modules can serve as either the baseline for nascent standards development efforts, or as a basis for evaluating the already existing electronic records management standards;

- government agencies – so that all business functions can be evaluated against, and facilitated via, the incorporation of automated records management capabilities; and

- private-sector organisations – so that they can incorporate automated electronic records management into their business operations.

1.3 Related standards

The requirements are aligned with the records management principles in the International Standard on Information and Documentation – Records Management – Part 1 – General, ISO 15489, which sets out the records management requirements
that also apply when records are captured and managed within electronic records management systems.


The requirements are core, high-level and generic requirements for records. Readers seeking guidance in other areas of software functionality not addressed in this document should refer to other more detailed specifications such as US DoD 5015.2 and MoReq2. Readers should also take account of other relevant jurisdiction-specific standards, statements of requirements and specifications.

1.4 Structure and use

The suite of guidelines and functional requirements is organised into three modules:

- **Module 1: Overview and Statement of Principles**: background information, organisation, fundamental principles and additional context;
- **Module 2: Guidelines and Functional Requirements for Records in Electronic Offices**: a global high-level statement of core and optional requirements, including application guidelines and a compliance checklist; and

Module 2 is intended for use by organisations seeking to implement dedicated electronic records management systems. It is meant to be read in conjunction with Module 1.

Module 3 is intended for use by organisations wishing to incorporate records functionality into business systems. It is meant to be read in conjunction with Module 1.

Several non-mutually exclusive use scenarios are presented below to exemplify how these modules might be used:

- Reviewing recordkeeping functionality in existing software – an organisation could use these modules as a checklist to establish which required and desirable recordkeeping functions are present in deployed, non-recordkeeping software.
- Integrating electronic records management software into a business system – an organisation could use Module 3 to selectively incorporate specific records management functionality into existing business systems.
- Using a design specification for in-house software development – an organisation’s IT staff could use Module 3 during their software design and testing documentation of software development efforts.
• Evaluating software considered for purchase – an organisation could use Module 2 as a basis for evaluating and comparing capabilities of commercial, off-the-shelf electronic records management software.

• Procuring, deploying and configuring electronic records management software – an organisation could use Module 2 to form the basis of a functional requirements statement in formulating a request for proposal for electronic records management software procurement and implementation. The requirements presented in these modules may be tailored to suit the individual requirements of organisations, depending on their business needs.

• Designing/re-designing software products during software enhancement cycles – software developers could use Modules 2 and/or 3 as a checklist of potential functionalities that may warrant consideration and/or inclusion in upcoming planned releases of established software products (not necessarily limited to electronic records management software products).

• Developing jurisdiction-specific specifications and standards – an organisation could use these modules as either the basis of its own juridical electronic records management specification or as a comparative resource when considering the revision of existing local electronic records management standards. Jurisdiction-specific requirements may be added to the generic requirements presented in these modules.

2  GOOD PRACTICE: ELECTRONIC RECORDS AND THE ROLE OF SOFTWARE

As organisations introduce new technologies and new methods for undertaking work, older methods and procedures for controlling records may become less effective. In many organisations, valuable records are kept in centralised databases or shared directories. Alternatively, and not mutually exclusively, they may be widely distributed and stored on the decentralised hard drives of individuals’ personal computers. Further complicating the situation, in either of these scenarios not all of the stored information may constitute records.

In either case, measures needed for integrity and authenticity may be overlooked and the electronic records may not be available, understandable and usable to the organisation or the relevant archival institution.

Organisations that already rely on electronic records to conduct and document business, or that are interested in eliminating paper records from their systems, are seeking solutions to issues of authenticity, management and retention of electronic records. The decisions that organisations make today about the capability of their information systems, the organisation and structure of their information resources, and the policies and practices for recordkeeping in the digital environment will have a significant impact on the types of strategies and methods that archival institutions can employ to ensure long-term preservation of records with archival value.

Because the issues of archival management, especially in the electronic environment, are closely linked to the design of systems and the establishment of new information
policies, archivists have been driven to examine a broader set of records management issues in order to carry out the archival function in the digital environment. Software provides business process owners, records managers and archivists with substantial means of complying with the practice of good electronic recordkeeping.

3 GUIDING PRINCIPLES

Successful organisations need information systems for making, keeping and using authentic evidence (that is, records) of business activity to meet their business needs and legal obligations. In the electronic environment, the development and implementation of such systems should be both driven by the organisation’s business needs and informed by the following principles:

3.1 Records-related principles

1 Electronic business information has to be actively managed and reliably maintained as authentic evidence of business activity.

As business processes become more completely automated, the electronic information generated by such activities may serve as the only evidence of specific transactions or decisions. Maintenance of this evidence in the form of fixed records is necessary for operational viability and accountability of the organisation. This involves identifying a set of electronic information that will serve as the evidential record.

2 Business information has to be linked to its business context through the use of metadata.

In order for information to have the capability of functioning as a record, it is necessary to augment that information with additional data (that is, metadata) that places it in the context of the business operations and computing environment in which it was created. In the case of line-of-business systems accomplishing uniform transactions, this context is derived from the system and its documentation. In other systems, however, such contextual information must be appended to the record as it is necessary to provide the record with sufficient longevity for interpretation and to maximise its value and utility as evidence of business activity.

3 Business information has to be kept and must remain accessible to authorised users for as long as required.

Design and deployment of business information software must ensure that records can be searched for, retrieved and rendered in accessible formats and media for as long as is required for business and legal purposes. In this context, organisations should avoid the misuse of digital rights management technology and encryption.

4 Business information has to be able to be disposed of in a managed, systematic and auditable way.

A hallmark of appropriate recordkeeping is the retention and appropriate disposition of records generated by business processes according to specified
rules. Systems need to be able to dispose of records in a systematic, auditable and accountable way in line with operational and legal requirements.

3.2 Systems-related principles

5 Systems should support good business information management as an organic part of the business process.

Although it is not necessarily appreciated as such, good recordkeeping practices are an integral part of any business process. When automating any business process, one should always evaluate the advisability of simultaneous integration of recordkeeping software.

6 Systems for capturing and managing business information have to rely on standardised\(^1\) metadata as an active, dynamic and integral part of the recordkeeping process.

Automated recordkeeping solutions offer powerful capabilities to access and attach standardised contextual information, via standardised vocabularies and taxonomies, to record content at different times during the life of the record.

7 Systems have to ensure interoperability across platforms and domains and over time.

Electronic evidence, in the form of records, often has operational or juridical requirements for persistence over periods of time that may exceed the lifespan of the hardware or software that created it. As such, record information must be able to be presented in a manner that is understood and able to be modified, if necessary, for migration to other technology platforms.

8 Systems should rely as far as possible on open standards and technological neutrality.

Many software products that create or manage records are developed using proprietary implementations. Hardware or software dependencies can have adverse effects on access and preservation of record material in the long term. Use of open standards ameliorates these technological dependencies.

9 Systems should have the capacity for bulk import and export using open formats.

Electronic records resulting from a business process and managed by recordkeeping software may contain hardware or software dependencies. Recordkeeping software should ideally incorporate capabilities to remove these dependencies via support for bulk re-formatting as part of ingest or export capability or, at a minimum, via non-proprietary encoding of record metadata.

10 Systems must maintain business information in a secure environment.

For security purposes, systems automating a business process often incorporate safeguards that limit which actions particular individuals can take with electronic information (for example, viewing, printing, editing, copying or transmitting). Systems must not allow unauthorised modifications to any records (including

---

\(^1\) ‘Standardised’ may refer to an agreed organisational metadata schema or to the adoption/adaptation of a jurisdictional, national or international metadata standard.
metadata), and where authorised modifications are performed, they must be fully documented.

11 As much metadata as possible should be system generated.

Users are typically unwilling to interrupt their workflow more than three times in the accomplishment of tasks ancillary to executing the primary activity. It may be impractical and/or unnecessary to expect end-users to supply much of the metadata. Systems should be designed and implemented in a manner that allows automatic population of record metadata fields.

12 It should be as easy as possible for users to create/capture records of business activity.

It is necessary to design systems/software that automate recordkeeping in a way, ideally, that makes such recordkeeping largely ‘invisible’ to the end-users.

4 IMPLEMENTATION ISSUES

4.1 Components of successful electronic business information management

Good software is only one component of successful electronic business information management in organisations. Other components include:

- **Policy frameworks** – concomitant with the deployment of software with recordkeeping functionality, it is necessary to conduct an analysis of existing information management and security policies and laws to address areas where policy revision may need to occur due to gaps in software capabilities. This includes policies relating to recordkeeping responsibilities for different categories of employees, records retention and disposal. Associated with the policy frameworks that guide and support good business information management software may be tools such as classification schemes and metadata models.

- **Business process analysis** – it is a preferred practice that process analysis should ideally precede any IT deployment. This includes identifying, articulating and potentially reallocating roles and responsibilities.

- **Project management** – any IT deployment requires careful planning and monitoring across a series of discrete stages. Project management techniques are powerful tools that provide both temporal and fiscal accountability for such efforts.

- **Change management** – deployment of automation within an organisation changes not only the manner in which business processes are accomplished, but the roles and responsibilities of end-users of the system. Care must be taken to adequately prepare the human component of any IT deployment for these changes. Failures in the implementation of records software often result primarily from shortcomings in change management rather than from any shortcomings in the technology.
Risk management – as with any IT system deployment, the decision to automate recordkeeping should be informed by an analysis of risks associated with an analysis of alternatives that are formulated as part of the business case. Ongoing post-implementation risk assessment should be incorporated into the organisation’s overall risk management framework.

Sustainability – development and maintenance of automated systems generally straddle organisations’ budgeting cycles. When automating recordkeeping, care must be taken, as part of the development of a business case for the automation effort, to provide for the ongoing viability, operations and maintenance of the system.

Capability development – software automation requires organisations to develop or enhance the technical capabilities of affected line staff, as well as others in the organisation, who in some cases may have no familiarity with the technology. Care must be taken to develop these capabilities, as well as the technical capabilities of the organisation necessary to support and maintain automation efforts.

Quality management – deployment of automated solutions requires the development within an organisation of the capability to evaluate and accept software performance according to a variety of criteria. Additionally, criteria related to the impact of software deployment to a business process must be developed and evaluated.

Configuration management – it is necessary to ensure that the software not only has the necessary recordkeeping capabilities, but that the capabilities are configured correctly and in such a way that enables it to operate appropriately in an organisation’s IT infrastructure.

Corporate culture – it is vital that the culture of the organisation reinforces the value and importance of good recordkeeping and that it is something that is a standard expectation of all employees. Such expectations need to be regularly articulated by the chief executive through line management channels.

4.2 Risks and mitigations

Risks typically associated with records software deployments fall into many categories. Some of these include:

- software selection risks – making an appropriate determination, from a range of commercial off-the-shelf products, of which product is best suited for deployment in an organisation;

---

• **software development risks** – experiencing difficulties related to dependence on software vendors or developers, including delays in releases of the software or inability of the vendor to be able to diagnose and fix software problems;

• **technical compatibility risks** – inadequately accounting for difficulties in integrating the electronic records management software into the IT infrastructure of the organisation;

• **communication risks** – inability to effectively communicate progress and/or issues regarding the deployment to end-users or management;

• **documentation risks** – inability to implement adequate programmatic recordkeeping surrounding software deployment efforts;

• **project management risks** – inability to appropriately track schedules or concomitant resource expenditures can threaten the overall stability of a project;

• **training risks** – ineffective training on new software solutions that can engender difficulties in end-user acceptance of new technologies;

• **risks associated with initial declines in productivity** – until end-users become familiar with new automated business processes, overall productivity may initially suffer due to the introduction of software innovations;

• **staff turnover risks** – changes in either senior management championing, or in the responsibilities of key personnel implementing, a software deployment can have an adverse effect on the overall project;

• **scalability risks** – the extent to which software may need to ‘scale up’ to organisation-wide deployment needs to be considered and planned for at an early stage in the project; and

• **organisational change** – business environments often change significantly during the development or life of a records or business system. These changes may include the size, structure, work processes, functions and mandates of the organisation itself.

Any organisation deploying software should acknowledge that some prudent risk-taking is necessary when it comes to adopting new technology and changing business processes. One means of mitigating the risks associated with such deployments is to mount a pilot deployment in a section of the organisation before expanding use of the software enterprise-wide.

To minimise the risks associated with a pilot launch, the project team should:

• establish clear performance objectives and evaluation criteria;

• involve and continually encourage pilot project participants to use the system;

• perform prototype work sessions with the software before customising it;
finalise system design;
develop quality acceptance methodology;
expand the pilot through incremental roll-out to other areas of the organisation and inclusion of other record formats; and
assure that the pilot’s requirements are measurable and clearly understood by participants.

Enumerating problems that the project team is likely to encounter, and identifying possible ways in which to avoid or promptly address those situations, will minimise disruptions during the pilot. To better prepare for these eventualities:

- a review of similar projects will help to identify potential problems that may be encountered during an electronic records management pilot; and
- conducting pre-planning brainstorming exercises with the project team can help anticipate the challenges ahead.

For each potential problem, develop a contingency plan. This best-management practice will increase the governance body’s confidence in the team’s ability to successfully implement electronic records management organisation-wide. The following illustrate successful strategies for dealing with frequently encountered problems:

- Organisations often encounter resistance to changing work processes as electronic records management is introduced. Many organisations find that introducing newly hired employees, at the beginning of their employment, to the importance of good records management is the best strategy for conquering resistance to change regarding electronic records management.

- Ensure a version of the software will be up and running for use by the project pilot team before roll-out to the first group of pilot participants. Selecting individuals to train and work with the software during this pre-pilot phase will develop a cadre of relatively sophisticated users who can liaise with the pilot project participants. When the quality of this pre-pilot phase is deemed acceptable, you can formally launch your electronic records management pilot.

- Managing users’ expectations throughout the pilot will minimise the risk of pilot failure. This can be achieved, in part, through user training and constant communication with pilot project participants. Establishing communication vehicles for the rest of your organisation (for example, an organisation-wide view of your pilot project website or online newsletter), keeping staff apprised of the progress being made vis-a-vis electronic records management, reminds people that the project is ongoing. This will make deployment in their area easier if the solution is adopted organisation-wide.

4.3 Financial and organisational sustainability of electronic systems
Each juridical environment likely has established processes designed to ensure the financial and organisational stability of any capital investment. Although potentially
conceptually over-simplified, the totality of analyses comprising a business case can be thought of as the collective means by which an organisation ensures this stability in the case of an IT investment, such as recordkeeping software.

In its simplest form, a business case articulates a variety of analyses that substantiate an acquisition proposal for the expenditure of an organisation’s capital in accordance with its capital asset strategy and inventory control of such investments. In the case of recordkeeping software acquisition, such a business case might consist of:

- **acquisition strategy** – summary of the funding requirement for project stages (including into future fiscal years);
- **program management** – detailing program management team membership and responsibilities;
- **enterprise architecture** – delineation of how a particular software acquisition relates to other existing and planned IT components within an organisation;
- **analysis of alternatives** – describing alternatives that were considered, and lifecycle costs and returns on investments associated with each;
- **risk management** – description of the major risks for the selected alternative, indicating the probability of occurrence, impact and mitigation strategies;
- **performance goals** – articulating which of the organisation’s strategic goals are supported by the proposed deployment, inclusive of existing baseline measures and resulting performance improvements according to specific proposed performance metrics;
- **project management** – presentation of detailed work breakdown structures delineating accomplishments and the cost of attaining major project milestones; and
- **change management** – for line-of-business and records staff.

5 **OTHER FUNCTIONAL REQUIREMENTS REFERENCED AND EVALUATED**

The aim of this project is to harmonise multiple existing jurisdiction-specific electronic recordkeeping software specifications in a manner that complies with the general requirements set forth in the International Standard on Records Management, ISO 15489, Parts 1 and 2 (2001), and the International Standard on Records Management Processes – Metadata for Records, Part 1 – Principles and Part 2 – Conceptual and Implementation Issues, ISO 23081 (2006 and 2007). The jurisdiction-specific functional requirements considered in preparing these modules are as follows:

**Archives New Zealand**

*Electronic Recordkeeping Systems Standard*, June 2005

Bundesministerium des Innern, Germany  
DOMEA Concept Requirement Catalogue 2.0, June 2005  
http://www.kbst.bund.de/cln_011/nn_838524/SharedDocs/Anlagen-kbst/Domea/domea-requirements-catalogue-2-0,templateId=raw,property=publicationFile.pdf/domea-requirements-catalogue-2-0.pdf

Cornwell Management Consultants plc  
(for the European Commission Interchange of Documentation between Administrations Programme)  
Model Requirements for the Management of Electronic Records, March 2001  
http://www.cornwell.co.uk/edrm/moreq.asp#moreqdownload

Department of Defense, United States  
http://jitet.fhu.disa.mil/recmg/t/p50152s2.pdf

Department of Defense, United States  
http://jitet.fhu.disa.mil/recmg/t/dod50152v3_13jun06.pdf

DLM Forum Working Group for the Development of MoReq  

European Commission  
Model Requirements for the Management of Electronic Records Update and Extension, 2008, (MoReq2 Specification)  
http://www.moreq2.eu/

Indiana University  
Requirements for Electronic Records Management Systems, 2002  
http://www.indiana.edu/~libarch/ER/requirementsforrk.doc

International Council on Archives  
Authenticity of Electronic Records, ICA Study 13-1, November 2002

International Council on Archives  
Authenticity of Electronic Records, ICA Study 13-2, January 2004

National Archives and Records Administration, United States  
Functional Requirements and Attributes for Records Management Services, December 2005  

National Archives of Australia  
National Archives of Australia
Functional Specifications for business Information Systems Software, October 2006

Public Record Office Victoria
Standard for the Management of Electronic Records PROS 99/007 (Version 1), April 2000

Public Record Office Victoria

Riksarkivet, National Archives of Norway

State Records of South Australia

State Records of South Australia

State Records of South Australia
Across Government EDRMS Panel of Products Procurement and Pre-Implementation – Guideline, Version 1, October 2004

The National Archives, United Kingdom

The National Archives, United Kingdom

The National Archives, United Kingdom
The National Archives, United Kingdom
Requirements for Electronic Records Management Systems, 4: Implementation Guidance, 2004

The National Archives, United Kingdom
Rationale for the Functional Requirements for Electronic Records Management Systems, 2002
Link to various documents from:
http://www.nationalarchives.gov.uk/electronicrecords/rat2002/

The National Archives, United Kingdom
Requirements to Sustain Electronic Information Over Time, March 2006

The National Archives, United Kingdom
Functional Requirements for the Sustainability of Electronic Records Management Systems, March 2006

6 GLOSSARY

This Glossary is a subset of the more complete glossary of terms found in Modules 2 and 3.

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Archives           | Materials created or received by a person, family or organisation, public or private, in the conduct of their affairs and preserved because of the enduring value contained in them or as evidence of the functions and responsibilities of their creator, especially those materials maintained using the principles of provenance, original order and collective control; permanent records.  
Note: This definition differs to the IT sphere where it refers to ‘a copy of one or more files or a copy of a database that is saved for future reference or for recovery purposes in case the original data is damaged or lost.’  
| Archival authority | The archival agency, archival institution, archival program agency or program responsible for selecting, acquiring and preserving archives, making them available and approving destruction of other records.                                                                 |
| business case      | A structured proposal for business improvement that functions as a decision package for organisational decision-makers. Includes an analysis of business process performance and associated needs or problems, proposed alternative solutions, assumptions, constraints and a risk-adjusted cost-benefit analysis. |
**business system**
For the purposes of this document, an automated system that creates or manages data about an organisation’s activities. Includes applications whose primary purpose is to facilitate transactions between an organisational unit and its customers – for example, an e-commerce system, client relationship management system, purpose-built or customised database, and finance or human resources systems.

**COTS**
Commercial off-the-shelf software

**disposition**
A range of processes associated with implementing retention, destruction or transfer decisions which are documented in disposition or other instruments.
Source: ISO 15489, Part 1, Clause 3.9

**Electronic record**
A record on electronic storage media, produced, communicated, maintained and/or accessed by means of electronic equipment.

**End-user**
In IT, the term end-user is used to distinguish the person for whom a hardware or software product is designed from the developers, installers and servicers of the product.

**Electronic records management software**
Specialised software used to automate the management of records.

**Human factors**
The study of how humans behave physically and psychologically in relation to particular environments, products or services. In a typical human factors or usability study, a group of hired or volunteer test subjects that represent future end-users is given tasks to do with a working prototype or early version of a product.

**Information**
Knowledge communicated or received. The result of processing, gathering, manipulating and organising data in a way that adds to the knowledge of the receiver.

**Information technology**
A term that encompasses all forms of technology used to create, store, exchange and use information in its various forms (business data, voice conversations, still images, motion pictures, multimedia presentations and other forms, including those not yet conceived).

**Term**
**Definition**

**Metadata**
Structured or semi-structured information, which enables the creation, management and use of records through time and within and across domains.
Structured information that describes and/or allows users to find, manage, control, understand or preserve other information over time.

**Migration**
The act of moving records from one system to another, while maintaining the records’ authenticity, integrity, reliability and useability. Migration involves a set of organised tasks designed to periodically transfer digital material from one hardware or software configuration to another, or from one generation of technology to another.
Source: Adapted from ISO 15489, Part 1, Clause 3.13 and Part 2, Clause 4.3.9.2.

**Pilot project**
An experimental initiative lasting for a limited time, the results of which are systematically evaluated.

**Proprietary software**
Software that is owned exclusively by a single company that carefully guards knowledge about the technology or the product’s inner workings.
<table>
<thead>
<tr>
<th><strong>Term</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Record (noun)</strong></td>
<td>Information in any format created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. Source: ISO 15489, Part 1, Clause 3.15.</td>
</tr>
<tr>
<td><strong>Recordkeeping</strong></td>
<td>The systematic creation, use, maintenance and disposition of records to meet administrative, legal, financial and societal needs and responsibilities.</td>
</tr>
<tr>
<td><strong>Reformat</strong></td>
<td>To create a copy with a format or structure different from the original, especially for preservation or access.</td>
</tr>
<tr>
<td><strong>Return on investment</strong></td>
<td>For a given use of money in an enterprise, the return on investment is how much profit or cost saving is realised. A return on investment calculation is sometimes used along with other approaches to develop a business case for a given proposal.</td>
</tr>
</tbody>
</table>
Principles and functional requirements for records in electronic office environments

Module 2

Guidelines and functional requirements for records in electronic office environments
## CONTENTS

1 INTRODUCTION
   1.1 Scope
   1.2 Purpose
   1.3 Audience
   1.4 Related standards
   1.5 Terminology
   1.6 Structure

2 GUIDELINES
   2.1 What are records and why are they important?
   2.2 Characteristics of electronic records and electronic records management systems
      2.2.1 Supporting import, export and interoperability
      2.2.2 Authentication, encryption and technological protection measures
   2.3 Overview of functional requirements
      2.3.1 Create
      2.3.2 Maintain
      2.3.3 Disseminate
      2.3.4 Administer
   2.4 Using the functional requirements set
      2.4.1 Key outcomes
      2.4.2 Obligation levels
      2.4.3 Risk and feasibility of not meeting the requirements

3 FUNCTIONAL REQUIREMENTS
   3.1 Capture
      3.1.1 Capture processes
      3.1.2 Point of capture metadata
      3.1.3 Aggregation of electronic records
      3.1.4 Bulk importing
      3.1.5 Electronic document formats
      3.1.6 Compound records
      3.1.7 Email
   3.2 Identification
   3.3 Classification
      3.3.1 Establishing a classification scheme
      3.3.2 Classification levels
      3.3.3 Classification processes
      3.3.4 Record volumes
   3.4 Managing authentic and reliable records
1  INTRODUCTION

Good management of records and information is fundamental to a well-functioning organisation since it supports business activity and provides a basis for efficient service delivery. It also provides the mechanism whereby both the private and public sectors can account for their decisions and actions. Records provide evidence for the public to confirm or claim their public rights and entitlements, as well as providing individuals with evidence to justify government decisions and a mechanism whereby they can have trust in private enterprise. Moreover, good records management is simply good business practice.

Records management systems facilitate:

- efficiency, by making information readily available when needed for decision-making and operational activities;
sound use of financial resources, by allowing timely disposal of non-current records;

- accountability, by enabling the creation of a complete and authoritative record of official activities;

- compliance, by demonstrating that legal requirements have been met; and

- risk mitigation, by managing the risks associated with illegal loss or destruction of records, and from inappropriate or unauthorised access to records.

1.1 Scope

A fundamental underlying principle is the distinction between business information systems (business systems) and electronic records management systems. Business systems contain data that is commonly subject to constant updates (dynamic), able to be transformed (manipulable) and only contain current data (non-redundant). By contrast, electronic records management systems contain data that is not dynamically linked to business activity (fixed), unable to be altered (inviolable), and may be non-current (redundant). Therefore business systems are beyond the scope of this Module (see Module 3: Guidelines and Functional Requirements for Records in business Systems). The records within an electronic records management system are, however, still dynamic in the sense that they can be (re)used in new business activity/contexts, so new metadata will be added through the ongoing use of the record content. It is more appropriate to speak about a framework for the systematic and structured management of records; records management systems link records to business activities, retain records of past actions, and fix the content and structure of records over time.

The scope of this Module is limited to products that are usually termed ‘electronic records management systems’. It does not seek to set requirements for records still in use within business systems. Digital objects created by email, word processing, spreadsheet and imaging applications (such as text documents, and still and moving images), where they are identified to be of business value, should be managed within electronic records management systems that meet the functional requirements in this Module. Records managed by an electronic records management system may be stored on a variety of different media formats, and may be managed in hybrid record aggregations that include both electronic and non-electronic elements.

This Module does not attempt to include requirements that are not specific to, or necessary for, records management, for example, general system management and design requirements. Nor does it include requirements common to all software applications, such as the performance, scalability and usability of the application. Given the target audience of this document, it also assumes a level of knowledge about developing design specifications, procurement and evaluation processes, and therefore these issues are not covered in this Module. Although not included in this Module’s requirements, the importance of non-records management functional requirements for records management systems is recognised through their inclusion in the high-level model outlined in Section 2.3: Overview of functional requirements.
Specifications for the long-term preservation of electronic records are also beyond the scope of this Module as this issue should be addressed separately by a dedicated strategy for digital preservation or ‘electronic archiving’. These electronic archiving considerations transcend the life of systems and are system independent; they need to be assessed in a specific longer-term strategic framework. However, recognition of the need to maintain records for as long as they are required must be addressed, and potential migration or format obsolescence issues should also be considered. Specific policies and procedures for these should be developed to support the longevity of records for permanent or long-term retention.

1.2 Purpose

This Module articulates a set of functional requirements for electronic records management systems. These requirements apply to records irrespective of the media in which they were created and stored. They are intended to:

- explain processes and requirements for identifying and managing records in electronic records management systems;
- develop requirements for records management functionality to be included in a design specification when building, upgrading or purchasing electronic records management systems software;
- inform records management functional requirements in the selection of commercially available electronic records management systems; and
- review the records management functionality or assess compliance of existing electronic records management systems.

This Module has been developed as part of an International Council on Archives project designed to:

- assist organisations to improve electronic records management practices;
- reduce the duplication of effort and associated costs in identifying a minimum level of records management functionality for electronic records management systems; and
- establish greater standardisation of records management requirements for software vendors across different jurisdictions.

1.3 Audience

The primary audience for this document is staff responsible for designing, reviewing and/or implementing electronic records management systems in organisations – whether those systems are commercial off-the-shelf electronic records management software applications, or custom-built applications. This Module primarily addresses the requirements of organisational records managers or system procurement project leaders, but will be relevant for jurisdictional standard-setters and the wider records management community. Another key audience is software vendors and developers who market and/or develop electronic records management system products. This Module is intended to inform their decision-making when designing records management functionality within electronic records management products.
Given the primary target audience for this document, the authors have tried to minimize the use of specific records management terminology. Where the use of such terminology is necessary, definitions can be found in the Glossary at Appendix A.

1.4 Related standards

Under its Electronic Records and Automation Priority Area, the International Council on Archives has developed a suite of guidelines and functional requirements as part of the Principles and Functional Requirements for Records in Electronic Office Environments project:

- Module 1: Overview and Statement of Principles;
- Module 2: Guidelines and Functional Requirements for Records in Electronic Office Environments; and

This document forms Module 2 of the project. It has been developed with the support of the Australasian Digital Recordkeeping Initiative.

While it is intended to serve as a stand-alone resource, for a broader understanding of the context and principles that have informed its development, readers should refer to Module 1: Overview and Statement of Principles. For details of appropriate functional requirements for (line of) business (information) systems, readers should refer to Module 3: Guidelines and Functional Requirements for Records in business Systems.

Readers of this document should also take note of any relevant jurisdiction-specific standards and specifications.

Note: this module is not intended to over-ride any local or jurisdiction-specific legislation standards or requirements.

The requirements in this Module are aligned with the records management principles in ISO 15489 Information and Documentation – Records Management – Part 1: General, which sets out the records management requirements that also apply when records are captured and managed within electronic records management systems.


The requirements presented in this Module are core, high-level and generic requirements for records. Readers seeking guidance in other areas of software functionality not addressed in this Module can refer to other more detailed specifications such as US DoD 5015.2 and MoReq2.
1.5 Terminology

Many of the terms used in this document have differing definitions across disciplines. For example, the term ‘archive’ may mean a storage of little-used data in a database to an IT audience, whereas it means the retention of fixed appraised information no longer retained for current business use within the records management discipline. It is therefore important that this document is read in conjunction with the Glossary at Appendix A. A number of the central concepts used in this document are also outlined below, to avoid misinterpretation:

- **Records** – information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.\(^3\) They provide evidence of business transactions and can exist in any format.

- **Records management** – the control of the creation, receipt, maintenance, use and disposal of records in accordance with professional and international standards of practice. Records management is distinct from document management, which is typically concerned with the provision of access, collaborative working and version control of documents, rather than the management of authenticity, reliability, integrity and useability over time.

- **Electronic records management systems** (commonly referred to as EDRMS or ERMS) – systems specifically designed to manage the maintenance and disposition of records. They maintain the content, context, structure and links between records to enable their accessibility and support their value as evidence. Electronic records management systems are distinguished from business systems, for the purpose of this document, because their primary function is the management of records.

- **business systems** – automated systems that create or manage data about an organisation’s activities (for the purpose of this document). They include applications whose primary purpose is to facilitate transactions between an organisational unit and its customers, for example, an e-commerce system, client-relationship management system, purpose-built or customised database, and finance or human resources systems. Business systems typically contain dynamic data that is commonly subject to constant updates (timely), able to be transformed (manipulable) and holds current data (non-redundant). For the purpose of this document, business systems exclude electronic records management systems.

- **System** – use of the term ‘system’ in this document refers to a computer or IT system. This is in contrast to the records management understanding of the term, which encompasses the broader aspects of people, policies, procedures and practices. While the focus of this Module is primarily electronic records management systems software, organisations will need to pay attention to wider aspects of records management frameworks, policies and tools to ensure records can be appropriately managed. For example, fundamental records management tools, such as disposition authorities and information

---

\(^3\) International Standard on Records Management, ISO 15489.
security classifications, must be in place and operate within an established records management culture within the organisation. A system may comprise more than one application and include plug-ins.

- **Records management metadata** – an inextricable part of records management, serving a variety of functions and purposes. In a records management context, metadata is defined as data describing the context, content and structure of records and their management through time (ISO 15489 – 1: 2001, 3.12). As such, metadata is structured or semi-structured information that enables the creation, registration, classification, access, preservation and disposition of records through time and within and across domains. Records management metadata can be used to identify, authenticate and contextualise records and the people, processes and systems that create, manage, maintain and use them, and the policies that govern them. Initially, metadata defines the record at its point of capture, fixing the record into its business context and establishing management control over it. During the existence of records or their aggregates, new layers of metadata will be added because of new roles in other business or usage contexts. This means that metadata continues to accrue information relating to the context of the records management and the business processes in which the records are used, and to structural changes to the record or its appearance.

Metadata can be sourced or re-used by multiple systems and for multiple purposes. Metadata applied to records during their active life may also continue to apply when the records cease to be required for current business purposes but are retained for ongoing research or other values. The purpose of records management metadata is to ensure authenticity, reliability, usability and integrity over time, and to enable the management and understanding of information objects, whether these are physical, analogue or electronic. However, metadata also needs to be managed as a record or as a component of a record.

Records management has always involved the management of metadata. However, the electronic environment requires a different expression of traditional requirements and different mechanisms for identifying, capturing, attributing and using metadata. In the electronic environment, authoritative records are those accompanied by metadata defining their critical characteristics. These characteristics must be explicitly documented rather than being implicit, as in some paper-based processes.

### 1.6 Structure

This document is divided into four main parts:

- **Part 1: Introduction** – explains the scope, purpose, audience and structure of the document.

- **Part 2: Guidelines** – provides an overview of the module’s conceptual basis and presents a high-level model of electronic records management system functionality. This section provides background information on the importance of records management, describes key terms and concepts, and outlines the framework of Part 3: Functional requirements. It also outlines
some of the issues and processes to be considered when reviewing, designing or purchasing electronic records management systems.

- **Part 3: Functional requirements** – provides a tabulation of the records management functional requirements that define the characteristics of an electronic records management system, and forms the records management functional requirements for systems assessment.

- **Part 4: Appendices** – provides a glossary of key terms, additional readings and a sample checklist of requirements for reviewing an existing electronic records management system.

## 2 GUIDELINES

### 2.1 What are records and why are they important?

Records are a valuable business asset. One of the key ways organisations are held accountable for their actions is through evidence of business transactions in the form of records. Records are ‘information created, received, and maintained as evidence and information, by an organisation or person, in pursuance of legal obligations or in the transaction of business.’ They must be retained for a period of time that is in line with an authorised retention schedule or disposition authority, sometimes referred to as a ‘disposition’.

A record is not just a collection of data, but is the consequence or product of an event and therefore linked to business activities. A distinguishing feature of records is that their content must exist in a fixed form, that is, be a fixed representation of the business transaction. Managing records in business systems, which contain data that is frequently updated and dynamic, is particularly challenging and may provide a rationale for implementing a separate electronic records management system.

Records comprise not only content but also information about the context and structure of the record. Records management metadata ‘identifies, authenticates and contextualises records and the people, processes and systems that create, manage, maintain and use them and the policies that govern them.’ It allows records to be located, rendered and understood in a meaningful way. ISO/TS 23081 – 2 provides a generic statement of records management metadata elements. Organisations may also have jurisdiction-specific elements sets to which they must adhere.

An appropriately managed record will provide a basis for:

- transparent, informed and quality decision-making and planning;
- an information resource that can be used to demonstrate and account for organisational activities; and
- consistency, continuity and efficiency in administration and management.

---


The International Standard on Records Management, ISO 15489, provides best-practice guidance on how records should be managed to ensure they are authentic, reliable, complete, unaltered and usable. Organisations that do not employ an electronic records management system may risk loss of key evidence of their business activities, thereby resulting in a lack of corporate memory, inefficiency and an inability to meet accountability and legislative requirements. The risks of not implementing an electronic records management system are:

- failure to meet legislative and regulatory requirements;
- embarrassment to your chief executive, the government and/or private individuals, especially if inability to manage information competently is highlighted in the media;
- poor strategic planning and poor decisions based on inaccurate information;
- business critical information not accessible for the conduct of business, dispute resolution, legal challenge or evidential purposes;
- loss of credibility, lowered public confidence, or financial or legislative penalties through inability to produce records or provide evidence of business activity when required in a timely manner;
- inability to provide evidence of the organisation’s activities or undertakings with external agencies, clients or contractors;
- inconsistent and inefficient conduct of business;
- inability to exploit organisational information and knowledge to full potential;
- unlawful disposal of records and inability to fully exploit corporate knowledge and data;
- duplication of effort, and poor resource and asset management;
- reduced capability of demonstrating good performance and any increased efficiencies or improved service delivery; and
- organisational embarrassment and damage to reputation.

The benefits of good recordkeeping include:

- protection and support in litigation, including the management of risks associated with the existence or lack of evidence of organisational activity;
- protection of the interests of the organisation and the rights of employees, clients, and present and future stakeholders;
- improved security of business records and robust management of commercial-in-confidence, personally sensitive or confidential information;
- the ability to deliver services in an efficient and consistent manner;
- ability to support current and future research and development activities;
- improved comprehensiveness and reliability of corporate memory;
- availability of relevant business activity records when required to support well-informed decision-making and policy development;
• reduced risk of data loss or accidental destruction of records;
• reliable performance measurement of business outputs;
• increased public and/or client confidence in the integrity of an organisation’s activities; and
• identification of vital records for disaster planning, so that organisations can continue to function in the event of severe disruption.

Authoritative and credible recordkeeping is an essential component of good governance and for underpinning reliable and consistent business practice and service delivery.

2.2 Characteristics of electronic records and electronic records management systems

Once records have been created, they must be managed and maintained for as long as required to ensure they have the following characteristics:\(^6\)

• **Authenticity** – the record can be proven to be what it purports to be, to have been created or sent by the person that created or sent it, and to have been created or sent at the time it is purported to have occurred.

• **Reliability** – the record can be trusted as a full and accurate representation of the transaction(s) to which they attest, and can be depended on in the course of subsequent transactions.

• **Integrity** – the record is complete and unaltered, and protected against unauthorised alteration. This characteristic is also referred to as ‘inviolability’.

• **Usability** – the record can be located, retrieved, preserved and interpreted.

Typically, electronic records management systems have the following attributes that seek to ensure these characteristics are maintained:

• **Creating records in context** – electronic records management systems enable organisations to capture evidence of their business activity. This involves identifying a set of electronic information to serve as the evidential record comprising both content and context. So, in order for information to have the capability of functioning as a record, it is necessary to augment that content information with additional data (that is, metadata) that places it in the context of the business operations and computing environment in which it was created.

• **Managing and maintaining records** – electronic records have to be actively managed as evidence of business activity, and to maintain their authenticity, reliability, integrity and usability. Maintenance of this evidence, as records, is necessary for operational viability and accountability of the organisation.

• **Maintaining records for as long as they are required** – records must be retained for a period of time that is in accordance with authorised legislative and jurisdictional requirements. Decisions about how long records must be

\(^6\) These are taken from ISO 15489.1 Records Management, Section 7.2 Characteristics of records.
retained are defined in disposition/disposal policies and rules. There will be some records that must be retained permanently while others will be required to be retained for varying periods or have a maximum retention period (for example, for privacy or data-protection legislative purposes).

Records have to be able to be disposed of in a managed, systematic and auditable way. A hallmark of appropriate records management is the retention and appropriate disposition of records according to specified rules. Systems need to be able to delete records in a systematic, auditable and accountable way in line with operational and juridical requirements. Organisations will need to meet the policies and procedures of their local jurisdictional authority for identifying, retaining and disposing of records.

- **Records management metadata can be configured** – to be meaningful as evidence of a business process, records must be linked to the context of their creation and use. To do this, the record must be associated with metadata about the business context in a classification structure. In addition to this ‘classification’ metadata, other metadata that should be captured at the point of creation includes:
  - identifier;
  - date of creation;
  - creator/author/person responsible; and
  - the business being conducted.

Much of this information can be automatically generated. In this Module, integration of metadata for managing records is addressed at a relatively high level. Rather than specifically detailing every metadata element required, the functional requirements set instead provides broad references to the need to have functionality that is capable of creating, capturing and maintaining adequate metadata elements. It is expected that each organisation will capture records management metadata in line with an identified records management metadata standard, in accordance with organisational and/or juridical requirements, and/or be consistent with ISO 23081 – 1: 2006, Information and Documentation – Records Management Processes – Metadata for Records, Part 1 – Principles; and ISO/TS 23081 – 2: 2007, Information and Documentation – Records Management Processes – Metadata for Records, Part 2 – Conceptual and Implementation Issues.

- **Records can be reassigned or reclassified, closed and if required, duplicated and extracted** – the identification of needs for records should establish at what point in the process a record should be created. Any further processes that happen to the record after this point must result in the creation of a new record or the recorded augmentation/versioning of the existing record, rather than alteration to it. This means that content and metadata that need to be kept to record previous decisions or processes cannot be overwritten, but that new content or metadata can be added.

It is important to ensure that the system is not ‘locked down’ to such an extent that simple mistakes (such as mistyping a name) cannot be corrected –
although permission for changes may be restricted to a system administrator or prevented by the system in exceptional circumstances, such as pending legal action.

- **Reports can be undertaken** – on records and the management thereof.
- **Security processes can be put in place** – normal systems controls over access and security support the maintenance of authenticity, reliability, integrity and usability, and therefore should be appropriately documented.

A risk assessment can inform business decisions as to how rigorous the controls need to be. For example, in a high-risk environment, it may be necessary to prove exactly what happened, when and by whom. This links to systems permissions and audit logging, to prove that approved actions are undertaken by authorised users. User requirements should be assigned at appropriate levels of access by an administrator.

### Table 1: System levels of access

<table>
<thead>
<tr>
<th>User</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User</td>
<td>Any person with permission to access the electronic records management system. That is, anyone who creates, receives, reviews and/or uses records stored in the system. This is the standard level of access that most employees of an organisation will possess.</td>
</tr>
<tr>
<td>Authorised user</td>
<td>A user with special access permissions that allow additional access to, and/or control over, records contained in the electronic records management system. Authorised users may in some instances be assigned permissions to undertake tasks similar to those of the system administrator, such as the ability to close and re-open records, create extracts of records and edit record metadata. The powers assigned to authorised users will vary depending on the business needs of the organisation and the level of responsibility allotted to the authorised user.</td>
</tr>
<tr>
<td>Records administrator (or records manager)</td>
<td>A system administrator, usually the records manager, with designated responsibility for configuring, monitoring and managing the electronic records management system content and its use.</td>
</tr>
<tr>
<td>System administrator (IT)</td>
<td>A person with responsibility for assigning and removing the permissions allocated to users and authorised users.</td>
</tr>
</tbody>
</table>

#### 2.2.1 Supporting import, export and interoperability

The ability to import and export records, and interoperability with other systems, is frequently required functionality. Records may need to be exported to other organisations in the event of mergers or government re-organisational changes.

Many records may need to be retained for longer than the lifespan of the software system itself, and therefore there is a need to be able to export records when transitioning to a new electronic records management system. There may also be a need to import records from business systems, particularly in collaborative business environments.

For ease of import and export, use of open formats and industry standards will increase levels of interoperability and reduce the cost and difficulty of any import/export process.
This functionality must be addressed at the planning stages as part of the business requirements.

2.2.2 Authentication, encryption and technological protection measures

These issues have an impact on the reliability of records issue. Electronic records management systems must allow records to be effectively managed when they have been subject to technological protection measures, electronic signatures and electronic watermarks (digital rights management). They should give particular consideration to the ongoing maintenance of records that have been subject to encryption and digital signatures. While encryption and digital signatures have a valuable role to play in ensuring the authenticity and integrity of records in transmission, they also present risks to the ongoing useability of the record as decryption keys and public keys for digital signatures may expire while the record is still required. For this reason, storing records in encrypted form is not recommended. Metadata can record the encryption and decryption processes and attest to the successful decryption of records.

If digital signatures are used as a means of protecting the authenticity and integrity of records, key management must be considered. Information about the digital signature and its validation should be recorded within the metadata.

2.3 Overview of functional requirements

This section identifies and briefly describes the functional requirements using a high-level model that clusters the requirements to highlight their inter-relationships (Figure 1). The model is primarily intended to provide an overview for readers who are not records management professionals.

Requirements for the long-term preservation of records, requirements common to all software applications and non-records management functionality are not detailed in this Module, but are indicated in the high-level model (solid grey shading). Potential integration points with IT architecture and other software applications are shown in the model as system inputs.

Individual requirements in Part 3: Functional requirements are grouped according to the clusters in the high-level model:

- create
- maintain
- disseminate
- administer.
Figure 1: Model of high-level functional requirements for electronic records management systems

Notes:

- Solid grey shading indicates functionality not detailed in Part 3: Functional requirements.
- This model depicts the functional requirements that are the components of electronic records management systems. It does not depict the sequence of work processes that electronic records management systems perform.
2.3.1 Create

Capture

Electronic records management systems uniquely capture, classify and identify records to ensure that their content, structure and context of creation are fixed in time and space. These records management processes facilitate the making of complete, authentic and usable records. There should be functionality to create a new record by reusing the content, structure and context of records once captured. While version/document control is beyond the scope of this Module it may also provide some of this functionality.

Records aggregations

Aggregations of electronic records are accumulations of related electronic record entities that, when combined, may exist at a level above that of a singular electronic record object, for example, a file. Aggregations represent relationships that exist between related electronic records and the system or environment in which they were created, and are recorded in their metadata links and/or other associations. These aggregations are typically controlled within a classification scheme in an electronic records management system.

Electronic records management systems may contain aggregations of records, records that are not aggregated, or both. Records aggregations structure related electronic records and support their management and usability. They may be at more than one level, and may have multiple relationships within separate aggregations.

Aggregations of electronic records may reflect relationships such as shared characteristics or attributes, or the existence of sequential relationships between related electronic records. The nature of the relationship between the electronic records of a particular aggregation will vary depending on factors such as their purpose and structure, and the content and format of the records themselves.

For example, an aggregation of electronic records may collectively constitute a narrative of events (that is, a series of connected business transactions), in which the records may have a sequential relationship. Any such sequential relationship between electronic records can be determined through the metadata elements associated with the records, such as titles, dates, author, container number (where applicable), and other such attributes. Where these relationships exist between records imported or extracted from external business systems, the electronic records management system should be capable of identifying, capturing, documenting and preserving them.

These aggregations may be formal, structured relationships (for example, digital files containing related digital documents), or may exist as less formalised, tightly bound metadata relationships recognised as establishing links between related records within an aggregation.

The aggregations must be fixed and maintained over time. Any change to an aggregation must be logged with an explanation. Aggregation for the management of records purposes should not be confused with, or replaced by, the generation of multiple, different aggregations in response to search requests or report queries.
Identification (registration)

To verify their existence within the system, every record and associated aggregation must have a unique identifier persistently linked to it. This allows the user to locate records and helps them to distinguish between versions.

Classification

Within electronic records management systems implementations, aggregations are often used to enable inheritance of characteristics to records created or related at a lower level of aggregation. Typically in electronic records management systems, information is managed as record objects, and aggregates these objects into a set of series or files. Agencies should take into account their own business needs when determining suitable records aggregations (for example, by function, activity or transaction) within their agency. Within a business classification scheme, a record’s contextual characteristics are attributed through structuring them according to identifiable business processes.
Subject-based classification schemes will allow records relating to broad subject areas to be grouped together, that is, the transactions and activities that occurred under a single subject, such as a particular property or client. However, under subject-based classification, the focus is on what the item or object is about, rather than on the purpose or activity that the record was created to document. Therefore, the context of the business activity can become disassociated, making disposal actions over subject-based files more difficult as they will contain records with differing retention periods.

Functional classification schemes are based on an analysis of the unique business functions and activities of an organisation, and are independent of the organisation’s administrative structure. This makes functional classification more flexible and stable as business units and structures are likely to change over time. This system breaks down traditional organisational information silos and enables easier retention and disposal.

**business classification scheme**

A business classification scheme is a conceptual hierarchical classification tool that can facilitate the capture, titling, retrieval, maintenance and disposition of records. It defines the way in which records are grouped together (aggregated) and linked to the business context in which they were created or transmitted. For example, individual records in an organisation-wide electronic records management system may be aggregated into series with their constituent record parts and contextual metadata, or may be subsequently aggregated into files. (Note that these terms are indicative only. Different electronic records management systems employ different terminology.) Records are often aggregated at three levels of granularity according to a three-tiered functional classification scheme as follows:

**Figure 3: Three-tiered functional classification scheme**

<table>
<thead>
<tr>
<th>Level 1</th>
<th>business function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Series, consisting of aggregations of files, may be referred to as ‘class’ or ‘category’</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 2</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Files, consisting of aggregations of individual records, may be referred to as ‘containers’. May be subdivided into volumes.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Level 3</th>
<th>Transaction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Items – in this document referred to as ‘records’. May be comprised of multiple components.</td>
<td></td>
</tr>
</tbody>
</table>

Note: This is a basic model. Aggregation to more than three levels may be necessary depending on the business processes described, or for clearer definition of complex topics.

The record (object) is located at the very bottom of the aggregation hierarchy. Some metadata values may be inherited from a higher layer of aggregation by all those
files or objects located below. Regardless of how many levels of aggregation below series or file level are implemented, each level should be consistent with the metadata requirements for the higher aggregation level.

2.3.2 Maintain

Managing authentic and reliable records

Records captured into electronic records management systems must be actively maintained to ensure their continued accessibility. Establishing appropriate security controls, building in disposal outcomes and enabling the management of hybrid records facilitate comprehensive, authentic, useable, tamper-proof and appropriately disposed records.

Controls and security

Records captured into an electronic records management system must be protected against intentional or accidental alteration of their content, structure and context throughout their life to retain their authenticity. Electronic records management systems must control access to, or alteration of, metadata. Location tracking, access controls and control over any alteration of records ensure the authenticity of records in an electronic records management system.

Hybrid records management

Agencies typically manage records that span a range of electronic and non-electronic media. Electronic records management systems must be able to ingest and maintain records management metadata relating to non-electronic records as well as electronic records and any associated records management metadata. Essentially, contextually related records regardless of whether they are in electronic or non-electronic format must be managed and subject to the same records management processes within their aggregations.

To facilitate hybrid records management functionality, the electronic records management system must be able to capture and maintain metadata relating to physical records. This requires the creation of markers that are metadata profiles of records physically held outside the business system. Markers contain metadata required by the business system to locate and manage physical records and allocate system management controls to them. A marker may denote a physical record, such as a plan or paper file, or an electronic record or aggregation of electronic records stored on removable media, such as a CD-ROM or magnetic tape.

Retention and disposal

Disposition authorities are policies that authorise the disposal of records, whether by destruction, transfer of control or applying a review period. Disposition/disposal authorities consist of disposal actions and retention periods for aggregations of records that may have a legislative or organisational use/requirement source. Organisations should review disposal actions when the relevant retention periods have expired.
Records are often transferred between electronic records management systems for a range of reasons other than disposal, for example, migration to a new electronic records management system as a result of a technology refresh or an organisational restructure. In all cases, where there is transfer of records (whether this involves movement to another electronic records management system or not) and/or subsequent destruction of records from the original electronic records management system, any existing records management metadata and point of capture metadata must be considered at the same time as the records to which they relate.

2.3.3 Disseminate

An electronic records management system must be able to search for, retrieve and render the records that it maintains. These functions facilitate useable records.

Searching is the process of identifying records or aggregations through user-defined parameters so that the records, aggregations and/or their associated records management metadata can be retrieved. Search and navigation tools are required to locate records, aggregations or records management metadata by employing a range of searching techniques to cater for novice and sophisticated users. Retrieving is the process of preparing the located records for rendering and viewing.

Rendering is the production of a human-readable representation of a record, usually to a visual display screen or in hardcopy format. Electronic records management systems typically contain records in a range of file formats. The user must be able to have human-readable access to records stored in all these formats through an appropriate rendering interface. Where it is meaningful to print a hardcopy of a record, the electronic records management system must provide functionality to allow all users to obtain printed copies of records and their records management metadata where appropriate.

2.3.4 Administer

As with most software applications, there is a need for a system administrator to undertake system maintenance and other support functions, such as maintenance of access groups and updating of the business classification system. Administration facilitates useable records, reliable systems, systematic practices and the routine application of records management procedures. This Module only refers to management of records administration that must be controlled and auditable to ensure the integrity, authenticity and reliability of the records.

2.4 Using the functional requirements set

Part 3 lists the set of functional requirements for the management of records in electronic systems. They are grouped according to the clusters from the high-level model in Figure 1.

2.4.1 Key outcomes

The functional requirements focus on the outcomes required to ensure records are managed appropriately, regardless of the type of electronic records management system employed. As the functional requirements provide a high-level description of
records management functionality rather than detailed specifications, it is recognised that the techniques and strategies to achieve the outcomes will depend on the type of system being used. It is intended that each organisation should tailor the functional requirements to meet its individual business needs.

2.4.2 Obligation levels

The keywords ‘must’, ‘should’ and ‘may’ that appear in the requirements in Part 3 indicate the relative importance of each requirement. These keywords are to be interpreted as follows:

- **Must** – requirements that use ‘must’ are necessary an absolute requirement for compliance with the requirement.
- **Should** – requirements that use ‘should’ may be ignored if a valid reason exists, but the full implications of this must be understood and carefully considered before choosing a different course.
- **May** – requirements that use ‘may’ are truly optional and may be incorporated or omitted as appropriate.

This document reflects international consensus; the requirements and obligation levels are not jurisdictionally specific or legally binding. Users should assess their own legislative environmental issues, business requirements and risk assessments where appropriate.

2.4.3 Risk and feasibility of not meeting the requirements

Risk is an important factor that should be considered in the management of records and applying these obligation levels and requirements. Possible risks may include adverse publicity, inefficient business activity, impaired ability to deliver services and a reduction in the organisation’s capacity to prosecute or defend allegations.

There is a wide range of requirements to show evidence of business processes. If there are any requirements that an organisation is considering not meeting, a risk and feasibility analysis can help determine an appropriate course of action, and ensure accountability in decision-making.

Organisations may have jurisdiction-specific risk management frameworks in place that define different levels of risk, which can be used to prioritise the identified requirements for evidence.

A feasibility analysis can help organisations to consider, in a structured way, the financial, technical, legal or operational capacity of the organisation.

3 FUNCTIONAL REQUIREMENTS

This part presents the set of functional requirements for electronic systems. They are divided into four sections according to key records management concepts and processes as outlined in Part 2: Guidelines:

- create
• maintain
• disseminate
• administer.

The functional requirements are focused on the outcomes required to ensure records are managed appropriately. They do not specify particular processes, as it is recognised that the techniques and strategies to achieve the outcomes will depend on the organisation and electronic records management system being used. The introductory text to each section provides summary information regarding the records management concept and the overarching aim of the subsequent requirements.

While they do not cover common system management and design requirements, such as interoperability, scalability and performance, it is acknowledged that such processes also support the recordkeeping functionality of the system. The functional requirements assume that a basic records management framework is in place, such as policies, procedures, and business retention and classification.

CREATE

3.1 Capture

Records are created in a diverse range of formats, may comprise multiple individual objects (compound records), and are transmitted by a wide range of communication channels (workflows, email, postal mail). Electronic records management systems must capture the content, structure and context of records to ensure they are reliable and authentic representations of the business activities or transactions in which they were created or transmitted. This is known as ‘point of capture’ metadata and should in itself be captured as a record; it should not be possible to alter any of these metadata features without changes being tracked and auditable.

3.1.1 Capture processes

The electronic records management system must:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enable integration with business applications so that transactional records created by those applications can be captured within the electronic records management system (including email, see Requirements 21–25).</td>
</tr>
<tr>
<td>2</td>
<td>Indicate when an individual record is captured within the electronic records management system.</td>
</tr>
<tr>
<td>3</td>
<td>Prevent the alteration of the content of any record by any user or administrator during the process of records capture. See also Requirements 88 and 89.</td>
</tr>
<tr>
<td>4</td>
<td>Prevent the destruction or deletion of any record by any user, including an administrator, with the exceptions of: • destruction in accordance with a disposition authority (see Section 3.6: Retention and disposal); and • authorised deletion by an administrator (see Section 3.8: Administration).</td>
</tr>
</tbody>
</table>
5. Support manual naming of electronic records, and allow this name to be different from the existing file name (including email subject lines used to construct record titles). If the existing filename is taken by default, the electronic records management system must allow this name to be amended at the time of capture.

6. Allow an administrator to alter the metadata of a record within the system if required, to allow finalisation/correction of the record profile. Any such action must be captured in a records management metadata.

7. Any revision or alteration of the records management/capture metadata must be captured as additional records management metadata.

8. Alert a user to any failure to successfully capture a record.

9. Be able, where possible and appropriate, to provide a warning if an attempt is made to capture a record that is incomplete or inconsistent in a way which will compromise its future apparent authenticity.

3.1.2 Point of capture metadata

To be meaningful as evidence of a business process, records must be linked to the context of their creation and use. In order to do this, the record must be associated with metadata about the business context in which it was created and its point of capture into the system.

Much of this information can be automatically generated by the system. It is expected that each organisation will capture records management metadata in line with an identified records management metadata standard (compliant with ISO 23081), and organisational and/or jurisdictional requirements.

The electronic records management system must:

10. Support the use of persistent metadata for records.

11. Acquire metadata elements for each record and persistently link them to the record over time.

12. Ensure that the values for metadata elements conform to specified encoding schemes.

13. Allow the administrator to pre-define (and re-define) the metadata elements associated with each record, including whether each element is mandatory or optional.

14. Allow all metadata for every record to be viewed by users, subject to access rights for individuals or groups of users.

15. Automatically capture the date and time of capture of each record as metadata elements linked to each record.

16. Support automatic extraction or migration of metadata from:
   • the software application that created the record;
   • an operating system or line of business system;
   • an electronic records management system; and
   • the file header, including file format metadata, of each record and its constituent components captured into the system.

17. Prevent the alteration of metadata captured in Requirement 16, unless authorised by the system administrator.
### 3.1.3 Aggregation of electronic records

Aggregations of electronic records are accumulations of related electronic record entities that when combined may exist at a level above that of a singular electronic record object, for example, a file or series. These relationships are reflected in the metadata links and associations that exist between the related electronic records, and between the electronic records and the system. For example, an aggregation of electronic records may collectively constitute a narrative of events (that is, a series of connected business transactions), in which the records may have a sequential relationship. Any such sequential relationship between electronic records can be determined through the metadata elements associated with the records, such as titles, dates, author, container number (where applicable), and other attributes. Where these relationships exist between records controlled by the electronic records management system, the system should be capable of identifying, capturing, documenting and maintaining or systematically disposing of them.

The electronic records management system **must:**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>21</strong></td>
<td>Ensure that all records captured within the electronic records management system are associated with at least one aggregation.</td>
</tr>
</tbody>
</table>
| **22** | Manage the integrity of all markers or other reference tags to records (where used), ensuring that:  
  • following a marker, whichever aggregation that the marker record is located in, will always result in correct retrieval of the record; and  
  • any change in location of a record also redirects any marker that references that record. |
| **23** | Not impose any practical limit on the number of records that can be captured in an aggregation, or on the number of records that can be stored in the electronic records management system. However, the system may permit the administrator to set limitations on the quantity of items within an aggregation if required for business purposes. |
| **24** | Allow users to choose at least one of the following where an electronic object has more than one manifestation:  
  • register all manifestations of the object as one record;  
  • register one manifestation of the object as a record; or  
  • register each manifestation of the object as a discrete record. |

The electronic records management system **should:**
Support the ability to assign records to multiple aggregations without their duplication.\(^7\)

### 3.1.4 Bulk importing

Records and their metadata may be captured into an electronic records management system in bulk in a number of ways, for example, from another electronic records management system or as a bulk transfer from an electronic document management system or workflow application. The electronic records management system must be able to accept these, and must include features to manage the bulk capture process.

The electronic records management system **must**:  

| 26 | Be able to capture in bulk records exported from other systems, including capture of:  
|    | • electronic records in their existing format, without degradation of content or structure, retaining any contextual relationships between the components of any individual record;  
|    | • electronic records and all associated records management metadata, retaining the correct contextual relationships between individual records and their metadata attributes; and  
|    | • the structure of aggregations to which the records are assigned, and all associated records management metadata, retaining the correct relationship between records and aggregations.\(^8\) |
| 27 | Be able to import any directly associated event history metadata with the record and/or aggregation, retaining this securely within the imported structure. |

### 3.1.5 Electronic document formats

Electronic records management systems will have to deal with a range of formats, both common applications and often business-specific formats. The electronic records management system must have the functionality to deal with the formats that you commonly use or are common to your business environment. This will vary across systems and organisations.

For ease of migration and export, use of open formats and industry standards will increase levels of interoperability and reduce the cost and difficulty of maintaining records effectively.

The electronic records management system **must**:  

| 28 | Support the capture of records created in native file formats from commonly used software applications such as:  
|    | • standard office applications (word processing, spread-sheeting, presentation, simple databases);  
|    | • email client applications;  
|    | • imaging applications; and  
|    | • web authoring tools. |

---

\(^7\) For example, an invoice might be added to a supplier file by one user and to a product file by another. This could be achieved by using a marker system.

\(^8\) For example, maintaining a persistent embedded metadata record of the original classification schema.
3.1.6 Compound records

Electronic records will comprise at least one component. An electronic record such as a text document will usually be a discrete record and comprise a single record object. Electronic records that comprise more than one component or multiple record objects, for example, a large technical report with dynamic links to diagrams and spreadsheets, may be referred to as ‘compound records’.

The nature of the components that comprise a given electronic record will vary. A component may be an electronic object, such as an electronic document, or a data element, such as an entry in a database. For example, a component of an electronic record in a system that encompasses the management of documents may consist of a single word-processed document, while components forming an electronic record in a human resource management system may comprise a number of closely linked data entries in a database (such as all data entered in connection with a single staff member’s personnel profile). These compound records should not be confused with internal record components or elements, such as a record object and its metadata or physical document and its marker.

The electronic records management system must:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 30 | Capture compound electronic records (records comprising more than one component) so that:  
• the relationship between the constituent components of each compound record is retained;  
• the structural integrity of each compound record is retained; and  
• each compound record is retrieved, displayed and managed as a single unit. |

31

Be able to capture compound records easily, preferably with one action, for example, a single click.

3.1.7 Email

Email is used for sending both simple messages and documents (as attachments), within and between organisations. The characteristics of email can make it difficult to track and register. Organisations must provide users with the capability of capturing selected email messages and attachments.

The electronic records management system must:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>32</td>
<td>Allow users to capture emails (text and attachments) as single records as well as individual records linked by metadata.</td>
</tr>
</tbody>
</table>

---

It is not always possible to capture specialised records (or those from specialised systems) with an electronic records management system; however, this risk should be mitigated against. Strategies for normalisation of formats for capture or a process of capturing the entire system should be considered. Where this is not possible, building records management capability into the business information system should be considered.
<table>
<thead>
<tr>
<th>33</th>
<th>Allow individual users to capture email messages (and attachments) from within their email application.</th>
</tr>
</thead>
</table>
| 34  | Allow users to choose whether to capture emails with attachments as:  
* email text only;  
* email text with attachments; or  
* attachments only.\(^{10}\) |
| 35  | Ensure the capture of email transmission data as metadata persistently linked to the email record. |
| 36  | Ensure that the text of an email and its transmission details cannot be amended in any way once the email has been captured. Nor should the subject line of the email itself be changeable, although the title of the record may be edited for easier access through, for example, keywords or by file-naming conventions. |
| 37  | Ensure that a human-readable version of an email message address is also captured, where one exists.\(^{11}\) |

### 3.2 Identification

To verify their existence within a system, every record and associated aggregation must have a unique identifier persistently linked to it. This allows to the user to locate records and helps them to distinguish between versions.

The electronic records management system **must:**

| 38  | Associate each of the following with a unique identifier:  
* record;  
* record extract; and  
* aggregation. |
| 39  | Require all identifiers to be unique and unduplicated within the entire electronic records management system. |
| 40  | Be able to store the unique identifiers as metadata elements of the entities to which they refer. |
| 41  | *Either:* Generate unique identifiers automatically, and prevent users from inputting the unique identifier manually and from subsequently modifying it (for example, a sequential number). |
| 42  | *Or:* Allow users to input a unique identifier, but validate that it is unique before it is accepted (for example, an account number). |
| 43  | Allow the format of the unique identifier to be specified at configuration time.\(^{12}\) |

Where unique identifiers are automatically generated, the electronic records management system **should:**

---

\(^{10}\) It is essential that these processes are recorded and embedded within the metadata of the records. The user must be alerted to the existence of the related items.

\(^{11}\) For example, for ‘Samuel Johnson’ <samjo@worldintnet.org> – ‘Samuel Johnson’ is the human-readable version of the email address samjo@worldintnet.org.

\(^{12}\) The identifier may be numeric or alphanumeric, or may include the concatenated identifiers of the volume and electronic aggregations above the record in the classification scheme.
Allow the administrator to specify at configuration time the starting number (for example, 1, 10, 100) and increment (for example, 1, 10) to be used in all cases.

### 3.3 Classification

#### 3.3.1 Establishing a classification scheme

A records classification scheme is a hierarchical classification tool that can facilitate the capture, titling, retrieval, maintenance and disposal of records. A classification scheme lies at the heart of any electronic records management system since it defines the way in which individual electronic records are grouped together (aggregated) and linked to the business context in which they were created or transmitted. By aggregating records, many of the records management processes described below can be carried out quickly and efficiently.

The electronic records management system **must**:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>45</strong></td>
<td>Support and be compatible with the organisational classification scheme.</td>
</tr>
<tr>
<td><strong>46</strong></td>
<td>Be able to support a classification scheme that can represent aggregations (at the function, activity, transaction level) as being organised in a hierarchy with a <strong>minimum</strong> of three levels.</td>
</tr>
<tr>
<td><strong>47</strong></td>
<td>Allow the inheritance of values from a classification scheme.</td>
</tr>
<tr>
<td><strong>48</strong></td>
<td>Allow naming conventions or thesauri to be defined at the time the electronic records management system is configured.</td>
</tr>
<tr>
<td><strong>49</strong></td>
<td>Support the initial and ongoing construction of a classification scheme.</td>
</tr>
<tr>
<td><strong>50</strong></td>
<td>Allow administrators to create new aggregations at any level within any existing aggregation.</td>
</tr>
<tr>
<td><strong>51</strong></td>
<td>Not limit the number of levels in the classification scheme hierarchy unless set by an administrator.</td>
</tr>
<tr>
<td><strong>52</strong></td>
<td>Support the definition of different record types that are associated with a specified set of metadata to be applied at capture.</td>
</tr>
<tr>
<td><strong>53</strong></td>
<td>Support the allocation of unique identifiers to records within the classification structure</td>
</tr>
</tbody>
</table>
Where the unique identifiers are based on sequential numbering, the electronic records management system **should:**

| 54  | Have the capacity to automatically generate the next sequential number within the classification scheme for each new electronic aggregation. |

The electronic records management system **may:**

| 55  | Support a distributed classification scheme that can be maintained across a network of electronic record repositories. |

Where the electronic records management system employs a graphical user interface, **it must:**

| 56  | Support browsing and graphical navigation of the aggregations and classification scheme structure, and the selection, retrieval and display of electronic aggregations and their contents through this mechanism. |

The electronic records management system **should:**

| 57  | Support the definition and simultaneous use of multiple classification schemes. This may be required, for example, following the merger of two organisations or migration of legacy systems. It is not intended for routine use. |

### 3.3.2 Classification levels

The electronic records management system **must:**

| 58  | Support metadata for levels within the classification scheme. |

| 59  | Provide at least two naming mechanisms for records in the classification scheme:
• a mechanism for allocating a structured alpha, numeric or alphanumeric reference code (that is, an identifier which is unique within the classification scheme) to each classification level; and
• a mechanism to allocate a textual title for each electronic aggregation.
It must be possible to apply both identifiers separately or together. |

| 60  | Allow only authorised users to create new classifications at the highest level in the classification scheme (for example, at the business function level). |

| 61  | Record the date of opening of a new aggregation within its associated records management metadata. |

| 62  | Automatically include in the records management metadata of each new aggregation those attributes that derive from its position in the classification scheme (for example, name, classification code). |

---

13 For example, if the following aggregations are within a classification scheme:
• 900 - 23 - 01 Manufacturing : Order Processing : Sales Order Validation;
• 900 - 23 - 02 Manufacturing : Order Processing : Invoicing;
• 900 - 23 - 03 Manufacturing : Order Processing : Credit Note Processing;

and the administrator adds a new aggregation to the ‘Order Processing’ aggregation, the electronic records management system should automatically assign it the reference 900 - 23 - 04. Likewise, if the administrator adds a new class to the ‘Manufacturing’ aggregation, the electronic records management system should automatically assign it the reference 900 - 24.
Allow the automatic creation and maintenance of a list of classification levels.

The electronic records management system should:

- Support a naming mechanism that is based on controlled vocabulary terms and relationships drawn (where appropriate) from an ISO 2788-compliant or ISO 5964-compliant thesaurus and support the linking of the thesaurus to the classification scheme.
- Support an optional aggregation naming mechanism that includes names (for example, people’s names) and/or dates (for example, dates of birth) as file names, including validation of the names against a list.
- Support the allocation of controlled vocabulary terms compliant with ISO 2788 or ISO 5964 as records management metadata, in addition to the other requirements in this section.

3.3.3 Classification processes

The electronic records management system must:

- Allow an electronic aggregation (including volumes) to be relocated to a different position in the classification scheme, and ensure that all electronic records already allocated remain allocated to the aggregations (including volumes) being relocated.
- Allow an electronic record to be reclassified to a different volume of an electronic aggregation.
- Restrict to authorised users the ability to move aggregations (including volumes) and individual records.
- Keep a clear history of the location of reclassified aggregations (including volumes) prior to their reclassification, so that their entire history can be determined easily.
- Prevent the deletion of an electronic aggregation or any part of its contents at all times, with the exceptions of:
  - destruction in accordance with a disposal authority; and
  - deletion by an administrator as part of an audited procedure.
- Allow an electronic aggregation to be closed by a specific administrator procedure, and restrict this function to an administrator.
- Record the date of closing of a volume in the volume’s records management metadata.
- Maintain internal integrity (relational integrity or otherwise) at all times, regardless of:
  - maintenance activities;
  - other user actions; and
  - failure of system components.

---

14 For example, if a file is in a hierarchical path: ‘Regional plan development : Public consultation : Public submissions’ and the administrator adds a new file named ‘Formal objections’ at the same level as the ‘Public submissions’ file, then it must automatically inherit the prefix ‘Regional plan development : Public consultation’.

15 This facility is intended for exceptional circumstances only, such as organisational mergers or other re-organisation, or to correct clerical errors. This requirement must be read together with Requirements 71, 72 and 80.

16 This facility is intended for exceptional circumstances only, such as to correct clerical errors. This requirement must be read together with Requirements 71, 72 and 80.

17 At a minimum, this must be stored in the metadata. It may also be desirable to record it elsewhere, for example, in the records management metadata of the object(s) being moved.
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>75</td>
<td>Not allow any volume that has been temporarily re-opened to remain open after the administrator who opened it has logged off.</td>
</tr>
<tr>
<td>76</td>
<td>Allow users to create cross-references between related aggregations or between aggregations and individual records.</td>
</tr>
<tr>
<td>77</td>
<td>Provide reporting tools for the provision of statistics to the administrator on aspects of activity using the classification scheme, including the numbers of electronic aggregations (including volumes) or records created, closed or deleted within a given period, by user group or functional role.</td>
</tr>
<tr>
<td>78</td>
<td>Allow the authorised users to enter the reason for the reclassification of aggregations (including volumes) and individual records.</td>
</tr>
<tr>
<td>79</td>
<td>Be able to close a volume of an electronic aggregation automatically on fulfilment of specified criteria to be defined at configuration, including at least: • volumes delineated by an annual cut-off date (for example, end of the calendar year, financial year or other defined annual cycle); • the passage of time since a specified event (for example, the most recent addition of an electronic record to that volume); and • the number of electronic records within a volume.¹⁹</td>
</tr>
<tr>
<td>80</td>
<td>Be able to open a new volume of an electronic aggregation automatically on fulfilment of specified criteria to be defined at configuration.</td>
</tr>
<tr>
<td>81</td>
<td>Allow an administrator to lock or freeze aggregations to prevent relocation, deletion, closure or modification when circumstances require, for example, pending legal action.</td>
</tr>
</tbody>
</table>

### 3.3.4 Record volumes

This section includes requirements relating to the use of volumes, which are typically used to subdivide aggregations that might otherwise be unmanageably large. The requirements for volumes only apply to the aggregations at the activity level. They are intended to be primarily useful for physical files in hybrid systems.

Where the electronic records management system uses volumes, it must:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>82</td>
<td>Allow administrators to add (open) electronic volumes to any electronic aggregation that is not closed.</td>
</tr>
<tr>
<td>83</td>
<td>Record the date of opening of a new volume in the volume’s records management metadata.</td>
</tr>
<tr>
<td>84</td>
<td>Automatically include in the metadata of new volumes those attributes of its parent aggregation’s records management metadata that assign context (for example, name, classification code).</td>
</tr>
<tr>
<td>85</td>
<td>Support the concept of open and closed volumes for electronic aggregations, as follows: • only the most recently created volume within an aggregation can be open; and • all other volumes within that aggregation must be closed (subject to temporary exceptions required by Requirement 68).²⁰</td>
</tr>
</tbody>
</table>

---

¹⁸ That is, it must be impossible for a situation to arise where any user action or any software failure results in an inconsistency within the electronic records management system or its database.

¹⁹ Other criteria may be desirable in particular circumstances, for example, where the size of the volume reaches the capacity of storage media.

²⁰ Note that the records in a volume can be accessed regardless of whether the volume is open or closed.
86 Prevent the user from adding electronic records to a closed volume (subject to the exceptions required by Requirement 68).

87 Allow an authorised user to add records to a closed file.\(^{21}\)

**MAINTAIN**

### 3.4 Managing authentic and reliable records

#### 3.4.1 Access and security

Organisations need to control access to their records. Typically, access to records and aggregations is limited to specific users and/or user groups. In addition to controlling access by user and user groups, some agencies will need to limit access further by using security classifications. This is achieved by allocating security classifications to aggregations and/or records. Users can then be allocated security clearances to permit selective access to aggregations or records at higher security categories.

Maintaining metadata of all records management actions undertaken by an electronic records management system and its users and administrators is essential to meeting requirements for legal admissibility. The volume of metadata information can become large if all actions are audited. Consequently, management may decide that some actions need not be audited. In most cases, the online metadata is periodically moved to offline storage and is disposed of at the same time as the records to which it relates, and a summary record retained. This process is also known as ‘tracking’.

Over time, records and aggregations may be transferred from one storage medium or location to another (for example, migration), as their activity decreases and/or their use changes. A tracking feature is needed to record the change of location for both ease of access and to meet regulatory requirements.

The electronic records management system **must**:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>88</td>
<td>Ensure that records are maintained complete and unaltered, except in circumstances such as court orders for amendments to record content and metadata, in which cases only system administrators may undertake such changes with appropriate authorisation.</td>
</tr>
<tr>
<td>89</td>
<td>Document any exceptional changes to records as described in Requirement 88 in relevant metadata.</td>
</tr>
<tr>
<td>90</td>
<td>Maintain the technical, structural and relational integrity of records and metadata in the system.</td>
</tr>
</tbody>
</table>

#### 3.4.2 Access controls

The electronic records management system **must**:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>91</td>
<td>Restrict access to system functions according to a user’s role and strict system administration controls.(^{22})</td>
</tr>
</tbody>
</table>

---

\(^{21}\) This facility is intended to be used to rectify user error, for example, if a volume has been closed unintentionally.
3.4.3 Establishing security control

Normal systems controls over access and security support the maintenance of authenticity, reliability, integrity and usability, and therefore should be appropriately implemented.

A risk assessment can inform business decisions as to how rigorous the controls need to be. For example, in a high-risk environment, it may be necessary to prove exactly what happened, when and by whom. This links to systems permissions and audit logging, to prove that approved actions are undertaken by authorised people.

The electronic records management system must:

<table>
<thead>
<tr>
<th></th>
<th>Allow only administrators to set up user profiles and allocate users to groups.</th>
</tr>
</thead>
<tbody>
<tr>
<td>92</td>
<td>Allow the administrator to limit access to records, aggregations and records management metadata to specified users or user groups.</td>
</tr>
<tr>
<td>93</td>
<td>Allow the administrator to alter the security category of individual records.</td>
</tr>
<tr>
<td>94</td>
<td>Allow changes to security attributes for groups or users (such as access rights, security level, privileges, initial password allocation and management) to be made only by the administrator.</td>
</tr>
</tbody>
</table>

3.4.4 Assigning security levels

The electronic records management system must:

<table>
<thead>
<tr>
<th></th>
<th>Allow only the administrator to attach to the user profile attributes that determine the features, records management metadata fields, records or aggregations to which the user has access. The attributes of the profile will:</th>
</tr>
</thead>
<tbody>
<tr>
<td>96</td>
<td>• prohibit access to the electronic records management system without an accepted authentication mechanism attributed to the user profile;</td>
</tr>
<tr>
<td></td>
<td>• restrict user access to specific records or aggregations;</td>
</tr>
<tr>
<td></td>
<td>• restrict user access according to the user’s security clearance;</td>
</tr>
<tr>
<td></td>
<td>• restrict user access to particular features (for example, read, update and/or delete specific records management metadata fields);</td>
</tr>
<tr>
<td></td>
<td>• deny access after a specified date; and</td>
</tr>
<tr>
<td></td>
<td>• allocate the user to a group or groups.</td>
</tr>
<tr>
<td>97</td>
<td>Be able to provide the same control functions for roles, as for users.</td>
</tr>
<tr>
<td>98</td>
<td>Be able to set up groups of users that are associated with an aggregation.</td>
</tr>
<tr>
<td>99</td>
<td>Allow a user to be a member of more than one group.</td>
</tr>
</tbody>
</table>

---

22 For example, an unauthorised user access attempt.

23 This is routinely required to reduce the level of protection given to records as their sensitivity decreases over time.

24 An example of an accepted authentication mechanism is a password.

25 This feature allows the administrator to manage and maintain a limited set of role access rights rather than a larger number of individual users. Examples of roles might include Manager, Claims Processing Officer, Security Analyst or Database Administrator.

26 Examples of groups might be Personnel or Sales Team.
If the electronic records management system maintains a list of aggregations, it must:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>100</td>
<td>Be able to limit users’ access to parts of the list (to be specified at the time of configuration).</td>
</tr>
<tr>
<td>101</td>
<td>Allow a user to stipulate which other users or groups can access records that the user is responsible for.27</td>
</tr>
</tbody>
</table>

### 3.4.5 Executing security controls

The electronic records management system must:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>102</td>
<td>Allow the administrator, subject to Section 3.4.6: Security categories, to alter the security category of all records within an aggregation in one operation. The electronic records management system must provide a warning if the security classifications of any records are lowered, and await confirmation before completing the operation.28</td>
</tr>
<tr>
<td>103</td>
<td>Allow the administrator to change the security category of aggregations, subject to the requirements of Section 3.4.6: Security categories.</td>
</tr>
<tr>
<td>104</td>
<td>Record full details of any change to security category in the records management metadata of the record, volume or aggregation affected.</td>
</tr>
</tbody>
</table>
| 105 | Provide one of the following responses (selectable at configuration time) whenever a user requests access to, or searches for, a record, volume or aggregation that they do not have the right to access:  
  • display title and records management metadata;  
  • display the existence of an aggregation or record (that is, display its file or record number) but not its title or other records management metadata; or  
  • not display any record information or indicate its existence in any way.29 |
| 106 | Never include, in a list of full text or other search results, any record that the user does not have the right to access.30 |

If the electronic records management system allows users to make unauthorised attempts to access aggregations (and their volumes) or records, it must:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>107</td>
<td>Log all unauthorised attempts to access aggregations (and their volumes) or records in their respective unique metadata.31</td>
</tr>
</tbody>
</table>

---

27 This function should be granted to the user by the administrator according to the agency’s policy.

28 This is routinely required to reduce the level of protection given to records as their sensitivity decreases over time.

29 These options are presented in order of increasing security. Note that the requirement in the third option (that is, the most stringent) implies that the electronic records management system must not include such records in any count of search results.

30 Note that if the first option of Requirement 103 is chosen, Requirement 104 may appear to be in conflict with it. This apparent conflict is intentional, for if this requirement is not present users may be able to use text searches to investigate the contents of documents to which they are not allowed access.

31 It will be acceptable for this feature to be controllable so that it only applies to administrator-specified security categories. Although the system should capture the location/interface and user or user log-in that attempted to gain access.
### 3.4.6 Security categories

The functional requirements in this section only apply to organisations that manage classified records within their electronic records management system. Please refer to your jurisdictional requirements and security requirements.

The electronic records management system **must:**

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>108</td>
<td>Allow security classifications to be assigned to records.(^{32})</td>
</tr>
</tbody>
</table>
| 109 | Allow security classifications to be selected and assigned at system level for:  
  - all levels of records aggregations (including volumes); and  
  - individual records or record objects. |
| 110 | Allow access-permission security categorisation to be assigned:  
  - at group level (be able to set up group access to specific aggregations, record classes security or clearance levels);  
  - by organisational role;  
  - at user level; and  
  - in combination(s) of the above.\(^{33}\) |
| 111 | Allow the assignment of a security category:  
  - at any level of records aggregation;  
  - after a specified time or event; and  
  - to a record type.\(^{34}\) |
| 112 | Support the automated application of a default value of ‘Unclassified’ to an aggregation or record not allocated any other security category. |
| 113 | Enable its security subsystem to work effectively together with general security products. |
| 114 | Be able to determine the highest security category of any record in any aggregation by means of one simple enquiry. |
| 115 | Support routine, scheduled reviews of security classifications. |
| 116 | Restrict access to electronic aggregations/records that have a security classification higher than a user’s security clearance. |

---

\(^{32}\) Security classification will be jurisdictionally or organisationally assigned but may include category levels such as:  
- Unclassified;  
- In Confidence (policy and privacy);  
- Sensitive (policy and privacy);  
- Restricted (national security information);  
- Confidential (national security information);  
- Secret (national security information); and  
- Top Secret (national security information).  
Further caveats may be assigned to any security clearance levels.

\(^{33}\) This will allow an administrator to manage and maintain a limited set of access-permissions/categories based on roles within the organisation rather than managing a large number of individual user-permission profiles for classified access.

\(^{34}\) Note that the correct level of security clearance may not be sufficient to obtain access. Searches will block access by not returning search results for records that are above a searcher’s access clearance, see Requirements 103 and 104.
If security classifications are assigned to aggregations as well as individual records (as per Requirement 107), then the electronic records management system **must:**

<table>
<thead>
<tr>
<th>No.</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>117</td>
<td>Be capable of preventing an electronic aggregation from having a lower security classification than any electronic record within that aggregation.</td>
</tr>
</tbody>
</table>

### 3.4.7 Records management process metadata

Metadata about the processes of managing the record, including the disposal of the record, needs to be documented to ensure the integrity and authenticity of the record, so that all alterations, linkages and uses of the record are able to be authoritatively tracked over time. Records exist at different layers of aggregation, for example, as documents, items, files or series. Records management metadata must be applied to records at all levels of aggregations. Although the record may be fixed and inviolable, the records management metadata will continue to accrue throughout the administrative life of the record. It must be persistently linked to the record to ensure that the record is authentic, unaltered and reliable.

The electronic records management system **must:**

<table>
<thead>
<tr>
<th>No.</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| 118 | Be capable of creating unalterable metadata of records management actions (actions to be specified by each agency) that are taken on records, aggregations or the classification scheme. The metadata should include the following records management metadata elements:  
  • type of records management action;  
  • user initiating and/or carrying out the action; and  
  • date and time of the action. |
| 119 | Track events, once the metadata functionality has been activated, without manual intervention, and store in the metadata information. |
| 120 | Maintain the metadata for as long as required. |
| 121 | Provide metadata of all changes made to:  
  • electronic aggregations (including volumes);  
  • individual electronic records; and  
  • records management metadata associated with any of the above. |
| 122 | Document all changes made to administrative parameters (for example, changes made by the administrator to a user’s access rights). |

---

35 The word ‘unalterable’ means that the metadata data cannot be modified in any way or deleted by any user. It may be subject to re-organisation and copying to removable media if required by, for example, database software, so long as its content remains unchanged and for a specific purpose. This process must not alter the original metadata data.
| 123 | Be capable of capturing and storing in the metadata information about the following actions:  
• date and time of capture of all electronic records;  
• reclassification of an electronic record in another electronic volume;  
• reclassification of an electronic aggregation in the classification scheme;  
• any change to the disposal authority of an electronic aggregation;  
• any change made to any records management metadata associated with aggregations or electronic records;  
• date and time of creation, amendment and deletion of records management metadata;  
• changes made to the access privileges affecting an electronic aggregation, electronic record or user;  
• export or transfer actions carried out on an electronic aggregation;  
• date and time at which a record is rendered; and  
• disposal actions on an electronic aggregation or record. |
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>124</td>
<td>Ensure that metadata is available for inspection on request, so that a specific event can be identified and all related data made accessible, and that this can be achieved by authorised external personnel who have little or no familiarity with the system.</td>
</tr>
<tr>
<td>125</td>
<td>Be able to export metadata for specified records and selected groups of records without affecting the metadata stored by the electronic records management system.</td>
</tr>
<tr>
<td>126</td>
<td>Be able to capture and store violations (that is, a user’s attempts to access a record or aggregation, including volumes, to which they are denied access), and (where violations can validly be attempted) attempted violations of access control mechanisms.</td>
</tr>
</tbody>
</table>
| 127 | Be able, at a minimum, to provide reports for actions on records and aggregations organised:  
• by record or aggregation;  
• by user; and  
• in chronological sequence. |
| 128 | Allow the metadata facility to be configurable by the administrator so that the functions for which information is automatically stored can be selected. The electronic records management system must ensure that this selection and all changes to it are stored in the metadata. |
| 129 | Be able to provide reports for actions on aggregations and records organised by workstation and (where technically appropriate) by network address. |
| 130 | Allow the administrator to change any user-entered records management metadata element. Information about any such change must be stored in the metadata. |

### 3.4.8 Tracking record movement

Location can refer to the physical location for hybrid records or the location within a classification structure or file structure for electronic records. Movement refers to changing the location of both electronic and physical records.

---

36 This functionality can be used by external auditors who wish to examine or analyse system activity.

37 It is acceptable for this feature to be controllable so that it only applies to administrator-specified security categories.

38 This functionality is intended to allow administrators to correct user errors, such as data input errors, and to maintain user and group access.
The electronic records management system must:

<table>
<thead>
<tr>
<th>131</th>
<th>Provide a tracking feature to monitor and record information about the location and movement of both electronic and non-electronic aggregations.</th>
</tr>
</thead>
</table>
| 132 | Record information about movements including:  
• unique identifier of the aggregation or record;  
• current location as well as a user-defined number of previous locations (locations should be user-defined);  
• date item sent/moved from location;  
• date item received at location (for transfers); and  
• user responsible for the move (where appropriate). |
| 133 | Maintain access to the electronic record content, including the ability to render it, and maintenance of its structure and formatting over time and through generations of office application software. |

3.5 Hybrid records management

3.5.1 Management of electronic and non-electronic records

Not all business systems are limited to the management of records in electronic format. Some business systems are specifically designed to provide for the management of physical records as well. Consequently, the functional requirements include requirements for hybrid system management to include functionality for managing records and files in physical format.

Hybrid file

The relationship between physical files and records in electronic formats differs significantly. As physical records (such as paper-based files) cannot be physically captured and registered directly into the business system, the business system must create and maintain markers – metadata profiles of physical records – to maintain linkages between the physical and electronic files.

Generally the marker will identify the title and unique identifier of the physical record, outline the record’s content and provide location information for retrieval.

A hybrid file exists where a related set of physical files and aggregations of electronic records (for example, electronic files) deals with the same function, activity or transaction, and must be managed as a single aggregation of records. Management of these hybrid files involves merging the aggregation of electronic records and physical file management processes.

Hybrid records

Electronic records can be linked to physical records or files through a tightly bound metadata relationship to form a hybrid record, in much the same way that physical files and aggregations of electronic records can be linked to create hybrid files. The metadata link between the electronic and physical records will be established through the marker, which will identify the physical record and its location. The

---

This may be achieved by use of a multi-format viewer application.
marker may be attached directly to the electronic record component of the hybrid record.

The electronic records management system **must**:

<table>
<thead>
<tr>
<th>No.</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>134</td>
<td>Be able to define in the classification scheme non-electronic aggregations and volumes, and must allow the presence of non-electronic records in these volumes to be reflected and managed in the same way as electronic records.</td>
</tr>
<tr>
<td>135</td>
<td>Allow both kinds of record to be managed in an integrated manner.</td>
</tr>
<tr>
<td>136</td>
<td>Allow a non-electronic aggregation that is associated as a hybrid with an electronic aggregation to use the same title and numerical reference code, but with an added indication that it is a hybrid non-electronic aggregation.</td>
</tr>
<tr>
<td>137</td>
<td>Allow a different records management metadata element set to be configured for non-electronic and electronic aggregations; non-electronic aggregation records management metadata must include information on the physical location of the non-electronic aggregation.</td>
</tr>
<tr>
<td>138</td>
<td>Ensure that retrieval of non-electronic aggregations displays the records management metadata for both electronic and non-electronic records associated with it.</td>
</tr>
<tr>
<td>139</td>
<td>Include features to control and record access to non-electronic aggregations, including controls based on security category, which are comparable with the features for electronic aggregations.</td>
</tr>
<tr>
<td>140</td>
<td>Support tracking of non-electronic aggregations by the provision of request, check-out and check-in facilities that reflect the current location of the item concerned.</td>
</tr>
</tbody>
</table>

The electronic records management system **should**:

<table>
<thead>
<tr>
<th>No.</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>141</td>
<td>Support the printing and recognition of bar codes for non-electronic objects (for example, documents, files and other containers), or should support other tracking systems to automate the data entry for tracking the movement of such non-electronic records.</td>
</tr>
<tr>
<td>142</td>
<td>Support the retention and disposal protocols and routinely apply to both electronic and non-electronic elements within hybrid aggregations.</td>
</tr>
</tbody>
</table>

Where aggregations have security categories, the electronic records management system **must**:

<table>
<thead>
<tr>
<th>No.</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>143</td>
<td>Ensure that a non-electronic record is allocated the same security category as an associated electronic record within a hybrid records aggregation.</td>
</tr>
</tbody>
</table>

**3.6 Retention and disposal**

**3.6.1 Disposition authorities**

‘disposition’ includes a number of actions, such as destruction, transfer, permanent archive and reassessment of a retention period, however the term for authorised records destruction is often ‘disposal’. In this Module the term ‘disposition’ is used to cover all these processes and the term ‘disposal’ is used as shorthand for assigning a period before authorised destruction can be considered.

Deletion is often considered to be (permanent) destruction, however material may still be accessible, discoverable or recoverable due to back-ups, personal hard drives and so on, and through digital forensics. These technical issues may be addressed at
a policy or technical level and may required serious consideration where legal or
security requirements are paramount.

Establishing disposition authorities

The electronic records management system must:

| 144 | Provide a function that: • specifies disposal authorities; • automates reporting and destruction actions; • disposes of compound records as a single action; and • provides integrated facilities for exporting records and records management metadata. |
| 145 | Be able to restrict the setting up and changing of disposal authorities to the administrator only. |
| 146 | Allow the administrator to define and store a set of customised standard disposal authorities. |
| 147 | Support retention periods from a minimum of one month to an indefinite period. |

Applying disposition authorities

The electronic records management system must:

| 148 | Be capable of assigning a disposal authority to any aggregation or record type. |
| 149 | By default, ensure that every record in an aggregation is governed by the disposal authority(s) associated with that aggregation. |
| 150 | Include a disposition action, agency retention period and trigger in the (metadata) record for the decision for each disposition authority. |
| 151 | For each aggregation: • automatically track retention periods that have been allocated to the aggregation; and • initiate the disposition process by prompting the administrator to consider and, where appropriate approve and execute, disposal action when disposition is due. |
| 152 | Allow at least the following decisions for each disposal authority: • retain indefinitely; • present for review at a future date; • destroy at a future date; and • transfer at a future date. |
| 153 | Allow retention periods for each disposal authority to be specified at a future date, with the date able to be set in at least the following ways: • passage of a given period of time after the aggregation is opened; • passage of a given period of time after the aggregation is closed; • passage of a given period of time since the most recent record has been assigned to the aggregation; • passage of a given period of time after a specific event (event to be identified in the schedule, and will be notified to the electronic records management system by the administrator, rather than being detected automatically by the electronic records management system); and • specified as ‘indefinite’ to indicate long-term preservation of the records. |

While these are generally inclusive, it is possible that some records will have types of retention requirements that are not listed.
Enable a disposal authority to be assigned to an aggregation that over-rides the disposal authority assigned to its ‘parent’ aggregation.\(^{41}\)

Allow the administrator to amend any disposal authority allocated to any aggregation at any point in the life of that aggregation.

Allow the administrator to change the authority(s) associated with an aggregation at any time.

Allow the definition of sets of processing rules that can be applied as an alerting facility to specified aggregations prior to initiation of a disposal process.\(^{42}\)

Provide the option of allowing electronic records or aggregations that are being moved between aggregations by the administrator to have the disposal authority of the new aggregation, replacing the existing disposal authority(s) applying to these records.

**Executing disposition authorities**

The electronic records management system **must:**

| 159 | Allow the administrator to delete aggregations, volumes and records (subject to Section 3.4.6: Security categories).\(^{43}\) |
| 160 | When executing disposition authorities, the electronic records management system must be able to:  
  • produce an exception report for the administrator;  
  • delete the entire contents of an aggregation or volume when it is deleted;  
  • prompt the administrator to enter a reason for the action;  
  • ensure that no items are deleted if their deletion would result in a change to another record (for example, if a document forms a part of two records – see Section 3.1.3: Aggregation of electronic records – one of which is being deleted);  
  • inform the administrator of any links from another aggregation or record to an aggregation or volume, that is about to be deleted, and request confirmation before completing the deletion;  
  • alert the administrators to any conflicts, for example, items that are linked to more than one disposition action involving pointers; and  
  • maintain complete integrity of the records management metadata at all times. |

If more than one disposal authority is associated with an aggregation, the electronic records management system **must:**

| 161 | Automatically track all retention periods specified in these disposal authorities, and initiate the disposal process once the last of all these retention dates is reached. |
| 162 | Allow the administrator to manually or automatically lock or freeze records disposition processes (freeze for litigation or legal discovery purposes, Freedom of Information purposes, etc.). |

---

\(^{41}\) For example, if an aggregation (‘parent’) contains another aggregation (‘child’), then it must be possible to assign a disposal authority to the ‘child’ that over-rides the disposal authority for the ‘parent’.

\(^{42}\) For example, during a review of the aggregation and contents by a manager or administrator, notify the administrator when an aggregation has a given security level.

\(^{43}\) This functionality is intended for exceptional circumstances only.
**Documenting disposition actions**

The electronic records management system **must**:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>163</td>
<td>Record any deletion or disposal action comprehensively in the process metadata.</td>
</tr>
<tr>
<td>164</td>
<td>Automatically record and report all disposal actions to the administrator.</td>
</tr>
</tbody>
</table>

**Reviewing disposition**

The electronic records management system **must**:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>165</td>
<td>Support the review process by presenting electronic aggregations to be reviewed, with their records management metadata and disposal authority information, in a manner that allows the reviewer to browse the contents of the aggregation and/or records management metadata efficiently.</td>
</tr>
</tbody>
</table>
| 166 | Allow the reviewer to take at least any one of the following actions for each aggregation during review:  
  - mark the aggregation for destruction;  
  - mark the aggregation for transfer;  
  - mark the aggregation for indefinite hold, for example, pending litigation; and  
  - change the disposal authority (or assign a different schedule) so that the aggregation is retained and re-reviewed at a later date, as defined in this section. |
| 167 | Allow the reviewer to enter comments into the aggregation’s records management metadata to record the reasons for the review decisions. |
| 168 | Alert the administrator to aggregations due for disposal before implementing disposal actions, and on confirmation from the administrator must be capable of initiating the disposal actions specified in this section. |
| 169 | Store in the metadata all decisions taken by the reviewer during reviews. |
| 170 | Produce a disposal authority report for the administrator that identifies all disposal authorities that are due to be applied in a specified time period, and provide quantitative reports on the quantity and types of records covered. |
| 171 | Be able to specify the frequency of a disposal authority report, the information reported and highlight exceptions such as overdue disposal. |
| 172 | Alert the administrator if an electronic aggregation that is due for destruction is referred to in a link from another aggregation and pause the destruction process to allow the following remedial action to be taken:  
  - confirmation by the administrator to proceed with or cancel the process; and  
  - generation of a report detailing the aggregation or record(s) concerned and all references or links for which it is a destination. |
| 173 | Support reporting and analysis tools for the management of retention and disposal authorities by the administrator, including the ability to:  
  - list all disposal authorities;  
  - list all electronic aggregations to which a specified disposal authority is assigned;  
  - list the disposal authority(s) applied to all aggregations below a specified point in the hierarchy of the classification scheme;  
  - identify, compare and review disposal authorities (including their contents) across the classification scheme; and  
  - identify formal contradictions in disposal authorities across the classification scheme. |
Provide, or support the ability to interface with, a workflow facility to support the scheduling, review and export/transfer process by tracking:
- progress/status of the review, such as awaiting or in-progress, details of reviewer and date;
- records awaiting disposal as a result of a review decision; and
- progress of the transfer process.

The electronic records management system should:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>175</td>
<td>Be able to accumulate statistics of review decisions in a given period and provide tabular and graphic reports on the activity.</td>
</tr>
</tbody>
</table>

### 3.6.2 Migration, export and destruction

The electronic records management system must:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>176</td>
<td>Provide a well-managed process to transfer records to another system or to a third party organisation and support migration processes.</td>
</tr>
<tr>
<td>177</td>
<td>Include all aggregations, volumes, records and associated metadata within aggregations whenever an electronic records management system transfers any aggregation or volume.</td>
</tr>
</tbody>
</table>
| 178 | Be able to transfer or export an aggregation (at any level) in one sequence of operations so that:
- the content and structure of its electronic records are not degraded;
- all components of an electronic record (when the record consists of more than one component) are exported as an integral unit including any technical protection measures;
- all links between the record and its records management metadata are retained; and
- all links between electronic records, volumes and aggregations are retained. |
| 179 | Be able to include a copy of the entire metadata set associated with the records and aggregations that are transferred or exported from an electronic records management system. |
| 180 | Produce a report detailing any failure during a transfer, export or destruction. The report must identify any records destined for transfer that have generated processing errors, and any aggregations or records that are not successfully transferred, exported or destroyed. |
| 181 | Retain copies of all electronic aggregations and their records that have been transferred, at least until such time as a successful transfer is confirmed.\(^{44}\) |
| 182 | Be able to continue to manage records and aggregations that have been exported from the electronic records management system to other forms of storage media. |
| 183 | Have the ability to retain records management metadata for records and aggregations that have been destroyed or transferred. |
| 184 | Allow the administrator to specify a subset of aggregation records management metadata that will be retained for aggregations which are destroyed, transferred out or moved offline.\(^{45}\) |

---

\(^{44}\) This is a procedural safeguard to ensure that records are not deleted before successful transfer is confirmed.
Enable the total destruction of records (whether identified by class or individually) stored on re-writable media by completely obliterating them so that they cannot be restored through specialist data recovery facilities.

The electronic records management system **should**:

1. Provide a utility or conversion tool to support the conversion of records marked for transfer or export into a specified file transfer or export format.
2. Provide the ability to add user-defined records management metadata elements required for archival management purposes to electronic aggregations selected for transfer.
3. Provide the ability to sort electronic aggregations selected for transfer into ordered lists according to user-selected records management metadata elements.

Where hybrid aggregations are to be transferred, exported or destroyed, the electronic records management system **should**:

4. Require the administrator to confirm that the non-electronic part of the same aggregations has been transferred, exported or destroyed before transferring, exporting or destroying the electronic part.

---

This is necessary for the organisation to know which records it has held and the dates they were destroyed or disposed of, without necessarily incurring the expense of keeping all the detailed records management metadata for the records.
3.6.3 Retention and disposal of electronic and non-electronic records

The electronic records management system must:

190 Support the allocation of disposal authorities to every non-electronic aggregation in the classification scheme. The authorities must function consistently for electronic and non-electronic aggregations, notifying the administrator when the disposal date is reached, but taking account of the different processes for disposing of electronic and non-electronic records.

191 Support the application of the same disposal authority to both the electronic and non-electronic aggregations that make up a hybrid aggregation.

192 Be able to apply any review decision made on a hybrid electronic aggregation to a non-electronic aggregation with which it is associated.

193 Alert the administrator to the existence and location of any hybrid non-electronic aggregation associated with a hybrid electronic aggregation that is to be exported or transferred.

194 Be able to record in the metadata all changes made to records management metadata references to non-electronic or hybrid aggregations and records.

195 Be capable of offering check-out and check-in facilities for non-electronic aggregations profiled in the system, in particular enabling the ability to record a specific user or location to which a non-electronic aggregation is checked out, and to display this information if the non-electronic aggregation is requested by another user.

196 Be capable of offering a request facility for non-electronic records profiled in the hybrid aggregation system, enabling a user to enter a date that the non-electronic element is required and generating a consequent message for transmission to the current holder of that non-electronic aggregation or the administrator, according to configuration.

197 Be able to export and transfer records management metadata of non-electronic records and aggregations.

The electronic records management system should:

198 Support the application of a review decision taken on a group of aggregations to any non-electronic aggregations within that group, by notifying the administrator of necessary actions to be taken on the non-electronic aggregations.

DISSEMINATE

3.7 Search, retrieve and render

Note that the electronic records management systems must never present information to any user who is not entitled to access it. All the features and functionality in this section must be subject to access controls as described in Section 3.4: Managing authentic and reliable records. To avoid complexity, this is assumed and is not repeated in each requirement below.

The electronic records management system must:

199 Provide a flexible range of functions that operate on the metadata related to every level of aggregation and on the contents of the records through user-defined parameters for the purpose of locating, accessing and retrieving individual records or groups of records and/or metadata.

200 Allow all record, volume and aggregation records management metadata to be searchable.
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>201</td>
<td>Allow the text contents of records (where they exist) to be searchable.</td>
</tr>
<tr>
<td>202</td>
<td>Allow the user to set up a single search request with combinations of records management metadata and/or record content.</td>
</tr>
</tbody>
</table>
| 203 | Allow administrators to configure and change the search fields to:  
- specify any element of record, volume and aggregation records management metadata, and optionally full record content, as search fields; and  
- change the search field configuration. |
| 204 | Provide searching tools for:  
- free-text searching of combinations of record and aggregation records management metadata elements and record content; and  
- Boolean searching of records management metadata elements (see also Requirement 219). |
| 205 | Provide for ‘wild card’ searching of records management metadata that allows for forward, backward and embedded expansion.46 |
| 206 | Allow searching within a single aggregation or across more than one aggregation. |
| 207 | Be able to search for, retrieve and display all the records and records management metadata relating to an electronic aggregation, or volume, as a single unit. |
| 208 | Be able to search for, retrieve and render an electronic aggregation by all implemented naming principles, including:  
- name; and  
- identifier (classification code). |
| 209 | Display the total number of search results on a user’s screen and must allow the user to then display the results list, or refine the search criteria and issue another request. |
| 210 | Allow records and aggregations featured in the search results list to be selected, then opened (subject to access controls) by a single click or keystroke. |
| 211 | Allow users to retrieve aggregations and records directly through the use of a unique identifier. |
| 212 | Never allow a search or retrieval function to reveal to a user any information (records management metadata or record content) that the access and security settings are intended to hide from that user. |
| 213 | Have integrated search facilities for all levels of the classification scheme.47 |
| 214 | Provide free-text and records management metadata searches in an integrated and consistent manner. |
| 215 | Present seamless functionality when searching across electronic, non-electronic and hybrid aggregations. |
| 216 | Allow users to save and re-use queries. |
| 217 | Allow users who are viewing or working with a record or aggregation, whether as the result of a search or otherwise, to see the record within the classification or aggregation hierarchy easily and without leaving or closing the record.48 |

---

46 For example, the search term ‘proj*’ might retrieve ‘project’ or ‘PROJA’; the term ‘C*n’ would retrieve ‘Commission’.

47 In other words, users should see the same interface, features and options whether searching for classes, aggregations or records.

48 For example, when reading a record, the user should be able to see what volume and aggregation the record is associated with. If viewing aggregation records management metadata, the user should be able to find out information about the aggregation in which it is located.
Allow users to refine (that is, narrow) searches.  

The electronic records management system should:

Provide word proximity searching that can specify that a word has to appear within a given distance of another word in the record to qualify as a search result (see also Requirements 202, 203 and 204).

Allow the records management metadata of any object (such as record, volume or aggregation) to be searched, whether the object itself is in electronic form or not, and regardless of whether the object is stored online, near-line or offline.

Provide display formats configurable by users or administrators for search results, including such features and functions as:
- select the order in which the search results are presented;
- specify the number of search results displayed on the screen;
- set the maximum number of search results;
- save the search results; and
- choose which records management metadata fields are displayed in search result lists.

Provide relevance ranking of the search results.

Be able to relate an ‘extract’ of an electronic record to the original record, so that retrieval of one allows retrieval of the other, while retaining separate records management metadata and access controls over the two items.

Provide concept searches through the use of a thesaurus incorporated as an online index.

Where a graphical user interface is employed, the electronic records management system must:

Provide a browsing mechanism that enables graphical or other display browsing techniques at any level of aggregation.

3.7.1 Rendering: displaying records

The electronic records management system must:

Render or download records that the search request has retrieved.

---

49 For example, a user should be able to start with the result list from a search and then initiate a further search within that list.

50 This will allow retrieval of documents with a broader, narrower or related term in their content or records management metadata. For example, a search for ‘ophthalmic services’ might retrieve ‘health services’, ‘eye test’ or ‘ophthalmology’.

51 This would be used with the searching techniques described above to provide a first-level view of records management metadata for a group of records or aggregations that have met the specified search criteria.

52 If the electronic records management system is storing records in a proprietary application format, it may be acceptable for the rendering to be performed by an application outside the electronic records management system.
The electronic records management system should:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>227</td>
<td>Render records that the search request has retrieved without loading the associated application software.(^{53})</td>
</tr>
<tr>
<td>228</td>
<td>Be able to render all the types of electronic records specified by the organisation in a manner that preserves the information in the records (for example, all the features of visual presentation and layout produced by the generating application package), and which renders all components of an electronic record in their original relationship.(^{54})</td>
</tr>
</tbody>
</table>

### 3.7.2 Rendering: printing

This section applies to records and their records management metadata and other data within the electronic records management system that can meaningfully be printed.

The electronic records management system must:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>229</td>
<td>Provide the user with flexible options for printing records and their relevant records management metadata, including the ability to print a record(s) with records management metadata specified by the user.</td>
</tr>
<tr>
<td>230</td>
<td>Allow the printing of records management metadata for an aggregation.</td>
</tr>
<tr>
<td>231</td>
<td>Allow the user to be able to print out a summary list of selected records (for example, the contents of an aggregation), consisting of a user-specified subset of records management metadata elements (for example, Title, Author, Creation date) for each record.</td>
</tr>
<tr>
<td>232</td>
<td>Allow the user to print the results list from all searches.</td>
</tr>
<tr>
<td>233</td>
<td>Be able to print all the types of electronic records specified by the organisation. Printing must preserve the layout produced by the generating application package(s) and include all (printable) components of the electronic record.(^{55})</td>
</tr>
<tr>
<td>234</td>
<td>Allow the administrator to specify that all printouts of records have selected records management metadata elements appended to them, for example, title, registration number, date and security category.</td>
</tr>
<tr>
<td>235</td>
<td>Allow the administrator to print the thesaurus, where a thesaurus exists within the system.</td>
</tr>
<tr>
<td>236</td>
<td>Allow the administrator to print any and all administrative parameters.</td>
</tr>
<tr>
<td>237</td>
<td>Allow the administrator to print disposal authorities.</td>
</tr>
<tr>
<td>238</td>
<td>Allow the administrator to print the classification scheme.</td>
</tr>
<tr>
<td>239</td>
<td>Allow the administrator to print metadata schema or element sets.</td>
</tr>
</tbody>
</table>

The electronic records management system should:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>240</td>
<td>Allow all records in an aggregation to be printed, in the sequence specified by the user, in one operation.</td>
</tr>
</tbody>
</table>

---

\(^{53}\) This is typically provided by integrating a viewer software package into the electronic records management system. This is frequently desirable to increase speed of rendering.

\(^{54}\) The organisation must specify the application packages and formats required.

\(^{55}\) The organisation must specify the application packages and formats required.
If the electronic records management system uses classification schemes and thesauri, it must:

241 Allow the administrator to print the file list.

### 3.7.3 Rendering: redacting records

A redacted record is a copy of an electronic record from which some material has been removed or permanently masked (redacted). An extract is made when the full record cannot be released for access, but part of the record can.

The electronic records management system must:

242 Allow the administrator to take a copy of a record for the purposes of redaction.\(^{56}\)

243 Record the creation of extracts in the records management metadata, including at least date, time, reason for creation and creator.

244 Store in the metadata any change made in response to the requirements in this section.

The electronic records management system should:

245 Provide functionality for redacting (see Glossary at Appendix A) sensitive information from the extract. If the electronic records management system does not directly provide these facilities, it must allow for other software packages to do so.\(^{57}\)

246 Prompt the creator of an extract to assign it to an aggregation.

247 Store a cross-reference to an extract in the same aggregation and volume as the original record, even if that volume is closed.

### 3.7.4 Rendering: other

This section applies only to records that cannot meaningfully be printed, such as audio, visual and database files.

The electronic records management system must:

248 Include features for rendering those records that cannot be meaningfully printed to an appropriate output device.\(^{58}\)

### 3.7.5 Rendering: re-purposing content

The electronic records management system must:

249 Allow the re-use or re-purposing of content.\(^{59}\)

---

\(^{56}\) This copy is referred to as an ‘extract’ of the record in this requirement (see Glossary at Appendix A).

\(^{57}\) It is essential that when these or any other redaction features are used, none of the removed or masked information can ever be seen in the extract, whether on screen, printed or played back, regardless of the use of any features such as rotation, zooming or any other manipulation.

\(^{58}\) Examples include audio, video and some websites.

\(^{59}\) An example may be allowing the user to cut text from a word-processed record or appending a dynamic link to an image-based record within another context.
ADMINISTER

3.8 Administration

In exceptional circumstances, records may be altered or deleted by system administrators. Where this is the case, copies of the records without the sensitive information (redacted copies) must be able to be created. System administrators also need to be able to manage system parameters, back up and restore data, and generate system reports. This section includes requirements for managing system parameters, back-up and restoration, system management and user administration. The administration of security classification, controls, classification and so on are addressed in the relevant security-related requirements in Section 3.4.4: Managing authentic and reliable records.

3.8.1 Administrator functions

The electronic records management system must:

| 250 | Allow the administrator to retrieve, display and re-configure system parameters and to re-allocate users and functions between user roles. |
| 251 | Provide back-up facilities so that records and their records management metadata can be recreated using a combination of restored back-ups and metadata. |
| 252 | Provide recovery and rollback facilities in the case of system failure or update error, and must notify the administrator of the results. |
| 253 | Monitor available storage space and notify the administrator when action is needed because available space is at a low level or because it needs other administrative attention. |
| 254 | Allow the administrator to make bulk changes to the classification scheme, ensuring all records management metadata and metadata data are handled correctly and completely at all times, in order to make the following kinds of organisational change: • division of an organisational unit into two; • combination of two organisational units into one; • movement or re-naming of an organisational unit; and • division of a whole organisation into two organisations. |
| 255 | Support the movement of users between organisational units. |
| 256 | Allow the definition of user roles, and must allow several users to be associated with each role. |

---

60 That is, the electronic records management system must allow administrators to ‘undo’ a series of transactions until a status of assured database integrity is reached. This is only required when error conditions arise.

61 When such a change is made, closed files must remain closed, retaining their references to the classification scheme before the change, and open files must either be closed, retaining their references to the classification scheme before the change and cross-referenced to a new file in the changed scheme, or be referenced to the changed scheme, but clearly retaining all prior references to the classification scheme before the change. Changes to organisational units described above may imply corresponding changes to the classification schemes of the units and their user populations. The term ‘bulk changes’ implies that all aggregations and records affected can be processed with a small number of transactions, rather than needing to be processed individually. Note that this element will apply especially where classification schemes are based on an organisation plan and be less necessary where classification is functionally assessed.
3.8.2 Metadata administration

Metadata schemas have to be administered, including the creation, addition, deletion or alteration of metadata elements, and the semantic and syntactical rules and obligation status applied to those elements.

The electronic records management system must:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>257</td>
<td>Communicate any errors encountered in saving data to storage media.</td>
</tr>
</tbody>
</table>

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>258</td>
<td>Allow the administrator to create, define and delete metadata elements, including custom fields.</td>
</tr>
<tr>
<td>259</td>
<td>Allow the administrator to apply and modify metadata schema rules, including semantic and syntactical rules, encoding schemes and obligation status.</td>
</tr>
<tr>
<td>260</td>
<td>Allow the administrator to configure the system to restrict the viewing or modifying of metadata elements by group, functional role or user.</td>
</tr>
<tr>
<td>261</td>
<td>Document all metadata administration activities.</td>
</tr>
</tbody>
</table>

3.8.3 Reporting

This section articulates basic reporting requirements. It does not articulate the requirements for a comprehensive reporting subsystem.

The electronic records management system must:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 262 | Provide flexible reporting facilities for the administrator. They must include, at a minimum, the ability to report the following:  
• numbers of aggregations, volumes and records;  
• transaction statistics for aggregations, volumes and records; and  
• activity reports for individual users. |
| 263 | Allow the administrator to report on metadata based on selected:  
• aggregations;  
• volumes;  
• record objects;  
• users;  
• time periods; and  
• file formats and instances of each format. |
| 264 | Be able to produce a report listing aggregations, structured to reflect the classification scheme, for all or part of the classification scheme. |
| 265 | Allow the administrator to request regular periodic reports and one-off reports. |
| 266 | Allow the administrator to report on metadata based on selected:  
• security categories;  
• user groups; and  
• other records management metadata. |
| 267 | Include features for sorting and selecting report information. |
| 268 | Include features for totalling and summarising report information. |
| 269 | Allow the administrator to restrict users’ access to selected reports. |
3.8.4 Back-up and recovery

Electronic records management systems must have comprehensive controls to create regular back-ups of the records and records management metadata that they maintain. These back-ups should enable the electronic records management system to rapidly recover records if any are lost because of system failure, accident or security breach. In practice, back-up and recovery functions may be divided between electronic records management system administrators and IT staff.

The electronic records management system must:

<table>
<thead>
<tr>
<th>Number</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>270</td>
<td>Provide automated back-up and recovery procedures.</td>
</tr>
</tbody>
</table>
| 271    | Allow the administrator to schedule back-up routines by:  

• specifying the frequency of back-up; and  

• allocating storage media, system or location for the back-up (for example, offline storage, separate system, remote site). |
| 272    | Allow only the administrator to restore from electronic records management system back-ups. Full integrity of the data must be maintained after restoration. |
| 273    | Allow only the administrator to roll-forward the electronic records management system from a back-up to a more recent state, maintaining full integrity of the data. |
| 274    | Allow users to indicate that selected records are considered to be ‘vital records’. |
| 275    | Be able to notify users whose updates may have been incompletely recovered, when they next use the system, that a potentially incomplete recovery has been executed. |

4 APPENDICES

A Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access controls</td>
<td>A scheme of non-hierarchical mechanisms, which may be applied to digital records to prevent access by unauthorised users. May include the definition of user access groups and ad hoc lists of individual named users. See also Security controls, System access control and User access group. Source: Adapted from The National Archives (UK), Requirements for Electronic Records Management Systems, 3: Reference Document, 2002, p. 28.</td>
</tr>
<tr>
<td>Accountability</td>
<td>The principle that individuals, organisations and the community are required to account to others for their actions. Organisations and their employees must be able to account to appropriate regulatory authorities, to shareholders or members, and to the public to meet statutory obligations, audit requirements, relevant standards and codes of practice, and community expectations.</td>
</tr>
<tr>
<td>Action tracking</td>
<td>The process in which time limits for actions are monitored and imposed on those conducting the business</td>
</tr>
</tbody>
</table>

Vital records are those records that are absolutely necessary for the organisation’s ability to continue its business either in terms of its ability to cope with emergency/disaster conditions or to protect its financial and legal interests. The identification and protection of such records, therefore, is of great importance to any organisation.
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Activity</td>
<td>The second level of a business classification scheme. Activities are the major tasks performed by an organisation to accomplish each of its functions. An activity is identified by the name it is given and its scope note. The scope of the activity encompasses all the transactions that take place in relation to it. Depending on the nature of the transactions involved, an activity may be performed in relation to one function, or it may be performed in relation to many functions. See also business classification scheme, Function and Transaction.</td>
</tr>
<tr>
<td>Adequate</td>
<td>Records should be adequate for the purposes for which they are kept. Thus, a major initiative will be extensively documented, while a routine administrative action can be documented with an identifiable minimum of information. There should be adequate evidence of the conduct of business activity to be able to account for that conduct.</td>
</tr>
<tr>
<td>Administrator</td>
<td>A role responsible for the day-to-day operation of the corporate records management policy within an organisation. May also indicate responsibility for operation of the corporate records management system.</td>
</tr>
<tr>
<td>Aggregation</td>
<td>Any accumulation of record entities at a level above record object (document, digital object), for example, digital file, series. Individual records may be aggregated into files and individual files, with their constituent records subsequently aggregated into files (depending on terminology used by the electronic records management system). See also File, and Record category.</td>
</tr>
<tr>
<td>Application program interface (API)</td>
<td>An application program(ming) interface is the specific method prescribed by a computer operating system or application program so that the application program can make requests of the operating system or another application.</td>
</tr>
<tr>
<td>Appraisal</td>
<td>The process of evaluating business activities to determine which records need to be captured and how long the records need to be kept, to meet business needs, the requirements of organisational accountability and community expectations.</td>
</tr>
<tr>
<td>Archival authority</td>
<td>The archival agency, archival institution, archival program agency or program responsible for selecting, acquiring and preserving archives, making them available and approving destruction of other records.</td>
</tr>
<tr>
<td>Archive</td>
<td>The whole body of records of continuing value of an organisation or individual. Sometimes called ‘corporate memory’.</td>
</tr>
<tr>
<td>Archives</td>
<td>Materials created or received by a person, family or organisation, public or private, in the conduct of their affairs and preserved because of the enduring value contained in them or as evidence of the functions and responsibilities of their creator, especially those materials maintained using the principles of provenance, original order and collective control; permanent records. Note: This definition differs to the IT sphere where it refers to ‘a copy of one or more files or a copy of a database that is saved for future reference or for recovery purposes in case the original data is damaged or lost.’ Source: IBM Dictionary of Computing, McGraw Hill, New York, 1994, p. 30.</td>
</tr>
<tr>
<td>Authentication</td>
<td>The process of establishing that the sender of a message is who they claim to be. Source: National Archives of Australia, Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption, 2004.</td>
</tr>
<tr>
<td>BCS</td>
<td>See business classification scheme.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| business classification scheme (BCS)      | 1. A conceptual representation of the functions and activities performed by an organisation. The scheme is a taxonomy derived from the analysis of business activity.  
2. The basis from which classification tools, such as a functions thesaurus and records classification scheme, are developed.  
See also disposition authority, Records classification tool and Taxonomy.  

business activity  
An umbrella term covering all the functions, processes, activities and transactions of an organisation and its employees. Includes public administration as well as commercial business.  

business system  
For the purposes of this document, an automated system that creates or manages data about an organisation’s activities. Includes applications whose primary purpose is to facilitate transactions between an organisational unit and its customers – for example, an e-commerce system, client relationship management system, purpose-built or customised database, and finance or human resources systems.  
See also Electronic document and records management system and Electronic records management system (both are commonly referred to as EDRMS).  

Capture  
1. The process of lodging a document or digital object into a recordkeeping system and assigning metadata to describe the record and place it in context, thus allowing the appropriate management of the record over time. For certain business activities this functionality may be built into business systems so that the capture of records and associated metadata is concurrent with the creation of records. See also Registration.  
2. 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. Once captured within an electronic records management system, users should not be able to alter the content, structure and context of a record.  

Certification authority  
A body that generates, signs and issues public key certificates that bind subscribers to their public key.  

Classification  
1. The systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in a classification system.  
2. Classification includes determining document or file naming conventions, user permissions and security restrictions on records.  
See also business classification scheme, Records classification scheme and Taxonomy.  
Source: Adapted from ISO 15489, Part 1, Clause 3.5; AS 4390, Part 1, Clause 4.8. |
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Component</strong></td>
<td>A set of constituent parts that comprises a digital record (such as the multimedia components of a web page). It is necessary to capture metadata about components to enable a record to be managed over time – for example, for migration purposes. Source: Adapted from The National Archives (UK), <em>Requirements for Electronic Records Management Systems, 3: Reference Document</em>, 2002, p. 1.</td>
</tr>
<tr>
<td><strong>Compound record</strong></td>
<td>A record that comprises multiple individual electronic objects, for example, web pages with embedded graphics and style sheets.</td>
</tr>
</tbody>
</table>
| **Control**            | 1 The physical and/or intellectual management established over records by documenting information about their physical and logical state, content, provenance and relationships with other records. The systems and processes associated with establishing control include registration, classification, indexing and tracking. See also *Classification* and *Registration*.  
2 An IT term for the process of eliminating a record from a system in such a way that the record may still be retrieved if necessary. Also known as ‘soft delete’. See also *Destruction*. |
<p>| <strong>Controlled vocabulary</strong> | An alphabetical list containing terms or headings that are authorised or controlled so that only one heading or form of heading is allowed to represent a particular concept or name. See also <em>Thesaurus</em>. Source: Adapted from J Kennedy and C Schauder, <em>Records Management: A Guide to Corporate Recordkeeping</em>, 2nd edition, Longmans, Melbourne, 1988, p. 291. |
| <strong>Conversion</strong>         | The process of changing records from one medium to another or from one format to another. Conversion involves a change of the format of the record but ensures that the record retains the identical primary information (content). See also <em>Migration</em>. Source: Adapted from the ISO 15489, Part 1, Clause 3.7 and Part 2, Clause 4.3.9.2. |
| <strong>Cryptographic key</strong>  | The data elements used for the encryption or decryption of electronic messages. They consist of a sequence of symbols that control the operation of a cryptographic transformation, such as encipherment. Source: National Archives of Australia, <em>Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption</em>, 2004. |
| <strong>Database</strong>           | An organised collection of related data. Databases are usually structured and indexed to improve user access and retrieval of information. Databases may exist in physical or digital format.                                                                                                                                                     |
| <strong>Deletion</strong>           | The process of removing, erasing or obliterating recorded information from a medium outside the disposition process. Deletion within electronic systems generally refers to the removal of the marker (that is, location information) that allows the system to identify where a particular piece of data is stored on the medium. See also <em>Destruction</em> and <em>disposition</em>. |
| <strong>Descriptor</strong>         | A non-hierarchical qualifier (for example, ‘Personnel’) attached to a security category to limit access to particular records. Descriptors may be informative or advisory but cannot actively control access. Source: Adapted from The National Archives (UK), <em>Requirements for Electronic Records Management Systems, 3: Reference Document</em>, 2002, pp. 27–8. |
| Term                     | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | Source: Adapted from ISO 15489, Part 1, Clause 3.8.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>disposition authority (also Disposal</td>
<td>A formal instrument that defines the retention periods and consequent disposition actions authorised for classes of records described in the authority. See also disposition action, disposition class and Retention period. Source: Adapted from AS 4390, Part 1, Clause 4.10.</td>
</tr>
<tr>
<td>class (also Disposal class)</td>
<td></td>
</tr>
<tr>
<td>disposition trigger (also Disposal</td>
<td>The point from which the disposition action is calculated. This can be a date on which action is completed or a date on which an event occurs. See also Retention period.</td>
</tr>
<tr>
<td>trigger)</td>
<td></td>
</tr>
<tr>
<td>Document (noun)</td>
<td>Recorded information or an object that can be treated as a unit. See also Record. Source: ISO 15489, Part 1, Clause 3.10.</td>
</tr>
<tr>
<td>Electronic document and records</td>
<td>An electronic records management system capable of providing document management functionality.</td>
</tr>
<tr>
<td>management system (EDRMS)</td>
<td></td>
</tr>
<tr>
<td>Electronic messaging systems</td>
<td>Applications used by organisations or individuals for sending and receiving, as well as storing and retrieving, electronic messages. These systems generally do not possess recordkeeping functionality. Source: National Archives of Australia, Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records, exposure draft, 2004.</td>
</tr>
<tr>
<td>Electronic records management system</td>
<td>An automated system used to manage the creation, use, maintenance and disposition of electronically created records for the purposes of providing evidence of business activities. These systems maintain appropriate contextual information (metadata) and links between records to support their value as evidence. The primary purpose of an electronic records management system is the capture and management of digital records. These systems are commonly referred to as EDRMS. See also Electronic document and records management system (EDRMS). Source: National Archives of Australia, Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records, exposure draft, 2004.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Encryption</td>
<td>The process of converting data into a secure code, through the use of an encryption algorithm, for transmission over a public network. The mathematical key to the encryption algorithm is encoded and transmitted with the data, thus providing the means by which the data can be decrypted at the receiving end and the original data restored. Sources: National Archives of Australia, <em>Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records</em>, exposure draft, 2004. Adapted from the Australian Government Information Management Office, <em>Trusting the Internet: A Small business Guide to E-security</em>, 2002, p. 43.</td>
</tr>
<tr>
<td>Evidence</td>
<td>Proof of a business transaction. Not limited to the legal sense of the term.</td>
</tr>
<tr>
<td>Export</td>
<td>A disposition process, whereby copies of a digital record (or group of records) are passed with their metadata from one system to another system – either within the organisation or elsewhere. Export does not involve removing records from the first system. See also Transfer. Source: Adapted from The National Archives (UK), <em>Requirements for Electronic Records Management Systems</em>, 3: Reference Document, 2002, p. 3.</td>
</tr>
<tr>
<td>Extract</td>
<td>A copy of a digital record, from which some material has been removed or permanently masked. An extract is made when the full record cannot be released for access, but part of the record can. Source: Adapted from The National Archives (UK), <em>Requirements for Electronic Records Management Systems</em>, 3: Reference Document, 2002, p. 3.</td>
</tr>
<tr>
<td>Field</td>
<td>A set of one or more related data elements that represent a category of information within a database. See also Database.</td>
</tr>
</tbody>
</table>
| File                 | 1  (Noun) An organised unit of documents accumulated during current use and kept together because they deal with the same subject, activity or transaction.  
2  (Verb) The action of placing documents in a predetermined location according to a scheme of control.  
*Note:* For the purposes of this document the records management definition of this term will apply. This differs from the IT definition, which identifies a file as a named collection of information stored on a computer and treated as a single unit. Source: Adapted from J -Ellis (ed.), *Keeping Archives*, 2nd edition, Australian Society of Archivists and Thorpe, Melbourne 1993, p. 470. |
| Format               | The physical form (such as paper or microfilm) or computer file format in which a record is maintained. See also Native format. Source: Adapted from Department of Defense (US), *Design Criteria Standard for Electronic Records Management Software Applications*, DoD 5015.2-STD, 2002, p. 14. |
| Function             | 1  The first level of a business classification scheme. Functions represent the major responsibilities that are managed by the organisation to fulfil its goals.  
2  The largest unit of business activity in an organisation or jurisdiction. Source: Adapted from AS 4390, Part 4, Clause 7.2. |
<p>| Graphical user interface (GUI) | A graphical, rather than purely textual, user interface to a computer (for example, windows-style interface). |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hybrid file</td>
<td>A set of related digital files and physical files. Both files are held in a tightly bound relationship within the business system and managed as a single object. Records managed within a hybrid file deal with the same subject, activity or transaction.</td>
</tr>
<tr>
<td>Hybrid record</td>
<td>1. A set of related digital and physical components that are linked by metadata in a tightly bound relationship and managed as a single record. See also <em>Physical record</em> and <em>Record</em>.</td>
</tr>
<tr>
<td></td>
<td>2. A record consisting of electronic and non-electronic components. <em>The electronic record and its associated records management metadata is maintained within the electronic records management system together with the records management metadata relating to the non-electronic record.</em></td>
</tr>
<tr>
<td>Hybrid recordkeeping system</td>
<td>A recordkeeping system containing a combination of paper, electronic or other formats.</td>
</tr>
<tr>
<td>Identify (Identification)</td>
<td>The process of persistently linking a record or aggregation with a unique identifier. See also <em>Registration</em>.</td>
</tr>
<tr>
<td>Indexing</td>
<td>The process of establishing access points to facilitate retrieval of records and/or information.</td>
</tr>
<tr>
<td>Import</td>
<td>To receive digital records and associated metadata into one system from another, either within the organisation or elsewhere.</td>
</tr>
<tr>
<td>Inherit</td>
<td>To take on a metadata attribute from a parent entity.</td>
</tr>
<tr>
<td>Instance</td>
<td>An occurrence of a digital record in a particular format or at a particular point in time. For example, one instance of a record may be in its native format while another instance is a rendition. Instances may be created as a product of migration or conversion processes.</td>
</tr>
<tr>
<td>Marker</td>
<td>A metadata profile of a record physically held outside the business system. A marker may denote a physical record (such as a large bound volume or building plan) or an electronic record stored on removable media (such as a CD-ROM or video). A representational link to a relevant record within the electronic records management system to alert users to the existence of a relevant record that is required to be accessible in more than one location.</td>
</tr>
<tr>
<td></td>
<td><em>Note:</em> A paper file will usually be represented and managed in the business system as a physical file. It is not envisaged that a physical file would contain markers for each document or record placed on a paper file, unless specifically required to do so in order to meet a particular business requirement of the organisation. This may also be referred to as an electronic records management system specific term.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Metadata        | Structured or semi-structured information, which enables the creation, management and use of records through time and within and across domains.  
Structured information that describes and/or allows users to find, manage, control, understand or preserve other information over time.  
| Migration       | The act of moving records from one system to another, while maintaining the records’ authenticity, integrity, reliability and useability. Migration involves a set of organised tasks designed to periodically transfer digital material from one hardware or software configuration to another, or from one generation of technology to another.  
Source: Adapted from ISO 15489, Part 1, Clause 3.13 and Part 2, Clause 4.3.9.2.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Native format   | The format in which the record was created, or in which the originating application stores records. See also Conversion.  
| Physical file   | An entry in the record plan for a hardcopy (usually paper) file. The file itself is stored outside the business system but metadata about its location and management is maintained in the system. A physical file may stand on its own within the records classification scheme, or it may form part of a hybrid file of closely related digital and physical objects. See also File and Marker.  
| Physical record | A record in hardcopy form, such as a folio, paper file, bound volume, photograph, microfilm, audio recording or moving image recording. See also Marker, Physical file and Record.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Quality records | Records used to demonstrate conformance to specified requirements and effective operation of quality systems under the AS/NZS ISO 9000 series.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Record (noun)   | Information in any format created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. See also Hybrid record and Physical record.  
Source: ISO 15489, Part 1, Clause 3.15.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Record category | A subdivision of the records classification scheme, which may be further subdivided into one or more lower-level record categories. A record category is constituted of metadata which may be inherited from the parent (for example, records category) and passed on to a child (for example, file or aggregation of digital records). The full set of record categories, at all levels, together constitutes the records classification scheme. See also Records classification scheme.  
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Record type</strong></td>
<td>Definition of a record object which specifies particular management requirements, metadata attributes and forms of behaviour. A default record type is the norm. Specific record types are deviations from the norm, which allow an organisation to meet regulatory requirements (such as privacy or data matching) for particular groups of records. Source: Adapted from The National Archives (UK), Requirements for Electronic Records Management Systems, 3: Reference Document, 2002, p. 5.</td>
</tr>
<tr>
<td><strong>Records classification scheme</strong></td>
<td>A hierarchical classification tool which, when applied to a business system, can facilitate the capture, titling, retrieval, maintenance and disposition of records. A records classification scheme stems from an organisation’s business classification scheme.</td>
</tr>
<tr>
<td><strong>Records classification tool</strong></td>
<td>A device or method used to assist in classifying, titling, accessing, controlling and retrieving records. May include a records classification scheme, thesaurus, indexing scheme or controlled vocabulary.</td>
</tr>
<tr>
<td><strong>Records continuum</strong></td>
<td>The whole extent of a record’s existence. Refers to a consistent and coherent regime of management processes from the time of the creation of records (and before creation, in the design of recordkeeping systems), through to the preservation and use of records as archives.</td>
</tr>
<tr>
<td><strong>Records management</strong></td>
<td>The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of, and information about, business activities and transactions in the form of records. Source: ISO 15489, Part 1, Clause 3.16.</td>
</tr>
<tr>
<td><strong>Records management (Recordkeeping)</strong></td>
<td>The making and maintaining of complete, accurate and reliable evidence of business transactions in the form of recorded information. Recordkeeping includes the creation of records in the course of business activity and the means to ensure the creation of adequate records; the design, establishment and operation of recordkeeping systems; and the management of records used in business (traditionally regarded as the domain of records management) and as archives (traditionally regarded as the domain of archives administration). Source: Adapted from AS 4390, Part 1, Clause 4.19 and Part 3, Foreword.</td>
</tr>
<tr>
<td><strong>Records management metadata</strong></td>
<td>Identifies, authenticates and contextualises records and the people, processes and systems that create, manage, maintain and use them, and the policies that govern them. See also Metadata. Source: ISO 23081, Part 1, Clause 4.</td>
</tr>
<tr>
<td><strong>Records management system</strong></td>
<td>A framework to capture, maintain and provide access to evidence over time, as required by the jurisdiction in which it is implemented and in accordance with common business practices. Recordkeeping systems include both records practitioners and records users; a set of authorised policies, assigned responsibilities, delegations of authority, procedures and practices; policy statements, procedures manuals, user guidelines and other documents which are used to authorise and promulgate the policies, procedures and practices; the records themselves; specialised information and records systems used to control the records; and software, hardware and other equipment, and stationery. Source: Adapted from AS 4390, Part 3, Clause 6.2.1.</td>
</tr>
<tr>
<td><strong>Redaction</strong></td>
<td>The process of masking or deleting information in a record.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Registration</td>
<td>The act of giving a record or file a unique identity in a recordkeeping system to provide evidence that it was created or captured. Registration involves recording brief descriptive information about the context of the record and its relation to other records. In the archival context, both aggregations (such as series) and individual record items can be registered. See also Capture and Identify. Sources: Adapted from ISO 15489, Part 1, Clause 3.18; AS 4390, Part 1, Clause 4.24.</td>
</tr>
<tr>
<td>Render</td>
<td>The production of a human-readable representation of a record, usually to a visual display screen or in hardcopy.</td>
</tr>
<tr>
<td>Rendition</td>
<td>Instance of a digital record made available in another format or on different medium by a process entirely within the business system control, without loss of content. A rendition should display the same metadata and be managed in a tightly bound relationship with the native format record. Renditions may be required for preservation, access and viewing purposes. See also Conversion.</td>
</tr>
<tr>
<td>Retention period</td>
<td>The length of time after the disposition trigger that a record must be maintained and accessible. At the expiration of the retention period, a record may be subject to a disposition action. See also disposition action and disposition trigger.</td>
</tr>
<tr>
<td>Security category</td>
<td>Hierarchical designation (such as ‘Top Secret’ or ‘Protected’) allocated to a user, user role, digital record or other record plan entity to indicate the level of access allowed. The security category reflects the level of protection that must be applied during use, storage, transmission, transfer and disposal of the record. See also Security controls. Source: Adapted from Cornwell Management Consultants (for the European Commission Interchange of Documentation between Administrations Programme), Model Requirements for the Management of Electronic Records (MoReq Specification), 2001, p. 107.</td>
</tr>
<tr>
<td>Security classification system</td>
<td>A set of procedures for identifying and protecting official information, the disclosure of which could have adverse consequences. The security classification system is implemented by assigning markings that show the value of the information and indicate the minimum level of protection it must be afforded. See also Classification and Security category. Source: Adapted from Attorney-General’s Department, Commonwealth Protective Security Manual, 2000.</td>
</tr>
<tr>
<td>Security controls</td>
<td>A scheme of protective markings which may be allocated to users, digital records and record plan entities to restrict access. May include a hierarchical security category, possibly in conjunction with a non-hierarchical qualifier. See also Access controls and Descriptor.</td>
</tr>
<tr>
<td>System access control</td>
<td>Any mechanism used to prevent access to the business system by unauthorised users. May include the definition of user profiles, or the use of ID and password login. See also Access controls and Security controls.</td>
</tr>
<tr>
<td>System administrator</td>
<td>A user role with designated responsibility for configuring, monitoring and managing the business system and its use. May exist at various degrees of seniority with a variety of permissions to undertake system administration functions and some records management processes.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>----------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>System rules</strong></td>
<td>Policies internal to system software that may be established and/or configured by a system administrator in order to govern the functionality of a given system and determine the nature of operational processes applied by that system.</td>
</tr>
</tbody>
</table>
| **Thesaurus**        | 1. In a thesaurus, the meaning of a term is specified and relationships to other terms are shown. A thesaurus should provide sufficient entry points to allow users to navigate from non-preferred terms to preferred terms adopted by the organisation.  
2. A records classification tool comprising an alphabetical presentation of a controlled list of terms linked together by semantic, hierarchical, associative or equivalence relationships. |
| **Taxonomy**         | 1. The classification of entities in an ordered system that indicates natural relationships.  
2. The science, laws and principles of classification.  
See also Classification. |
| **Tracking**         | Creating, capturing and maintaining information about the movement and uses of records.  
| **Transaction**      | The smallest unit of business activity. Uses of records are themselves transactions.  
The third level in a business classification scheme.  
See also Activity, business classification scheme and Function.  
Sources: Adapted from AS 4390, Part 1, Clause 4.27; AS ISO 15489, Part 2, Clause 4.2.2.2. |
| **Transfer**         | A disposition process, consisting of a confirmed export of digital records and associated metadata, and where applicable aggregations of digital records, followed by their destruction within the exporting business system. Records may be transferred from one organisation to another following administrative change, from an organisation to archival custody, from an organisation to a service provider, from the government to the private sector or from one government to another.  
| **Transfer (custody)** | Change of custody, ownership and/or responsibility for records. |
| **Transfer (movement)** | Moving records from one location to another. |
| **User access group** | Discrete set of named individuals (users known to the business system) that makes up a stable and nameable group. Access to particular records or other file plan entities may be restricted to members of certain user access groups.  
See also Access controls.  
<p>| <strong>User permissions</strong> | Privileges allocated to employees determining the extent of access to records and authority to author/originate, add, alter and dispose of records in recordkeeping system. |</p>
<table>
<thead>
<tr>
<th><strong>Term</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>User profile</td>
<td>A summary of all attributes allocated to a user of the business system. Includes all data known to the system, such as username, ID and password, security and access rights, functional access rights. See also Access controls.</td>
</tr>
<tr>
<td>User role</td>
<td>An aggregation or standard set of business system functional permissions that may be granted to a predefined subset of system users. Source: Adapted from The National Archives (UK), Requirements for Electronic Records Management Systems, 3: Reference Document, 2002, p. 6.</td>
</tr>
<tr>
<td>Volume</td>
<td>A sub-division of an electronic or non-electronic aggregation. Also referred to as a ‘part’. Usually a file part closed off due to size or time period constraints, for example, ‘Expense claim forms 2007-2008’. See also Aggregation.</td>
</tr>
</tbody>
</table>

**B  Further reading**


### Sample checklist of requirements for reviewing an existing electronic records management system

This tool assumes that the electronic recordkeeping system in question contains records and the records of the business transactions have been identified. It is also assumed that the fundamental records management tools such as the disposition authority, business classification scheme, and security and access classification scheme are in place within the organisation.

<table>
<thead>
<tr>
<th>No.</th>
<th>Checkpoint</th>
<th>Evidence of achievement / comments</th>
<th>Level of achievement (1–5):</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>5 = Satisfied</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3 = Partially satisfied</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1 = Not satisfied</td>
</tr>
</tbody>
</table>

**GENERAL**

- Are personnel appropriately trained to be able to implement their recordkeeping responsibilities?

**CREATE RECORDS THAT ARE LINKED TO THEIR CONTEXT**

- Can ‘fixed’/static records be created by the system?
- Can the system create records that are linked to their business context?
- Does the system capture the required recordkeeping metadata elements in line with jurisdictional standards and business needs?
- Is the recordkeeping metadata linked to the records, and are these linkages maintained over time?

**MANAGE AND MAINTAIN RECORDS**

- Are documented policies and procedures in place for the management of the records?
- Can the records be proven to be what they purport to be; have been created or sent by the person that created or sent it; and have been created or sent at the time purported?
- Are there sufficient controls to protect the records from unauthorised access, alteration, deletion and use?
- Can the records be searched for, displayed and accessed in a meaningful way?
- Are there policies and procedures in place for conducting recordkeeping audits on the system on a regular basis?
| **Are back-up and disaster recovery plans in place for the system?** |
| **Is a complete and current set of system documentation maintained (for example, specifications, manuals, design, integration, etc.)?** |
| **If digital signatures are in use, can the records be read as and when required?** |

**IMPORT AND EXPORT OF RECORDS AND INTEROPERABILITY**

| **Where records are stored with one organisation, but the responsibility for management and control resides with another, are the responsibilities clearly understood, traceable and documented?** |
| **Are there processes and mechanisms in place which support ongoing access to records, in line with retention requirements, beyond the life of the system?** |
| **Are records capable of being transferred from the system to an archival institution for archiving?** |

**RETENTION AND DISPOSAL**

| **Can you execute disposition actions in line with the disposition authority?** |
| **Are records being retained in line with disposition authorities, and not being deleted or overwritten?** |

**HYBRID SYSTEMS**

| **Where the system manages both physical and electronic records, does it support hybrid recordkeeping functionality?** |
Principles and functional requirements for records in electronic office environments

Module 3

Guidelines and functional requirements for records in business systems
## CONTENTS

1 INTRODUCTION
   1.1 Scope and purpose
   1.2 Audience
   1.3 Related standards
   1.4 Terminology
   1.5 Structure

2 GUIDELINES
   2.1 Why is it important to have evidence of business processes and activities?
   2.2 The business systems landscape and recordkeeping
   2.3 Determining needs for evidence of events, transactions and decisions in business systems
      2.3.1 Analyse the work process
      2.3.2 Identify requirements for evidence of the business
      2.3.3 Identify the content and its associated management information that record this evidence
      2.3.4 Identify linkages and dependencies
      2.3.5 Devise strategies to address core recordkeeping processes based on an options assessment
      2.3.6 Risk and options assessment
      2.3.7 Implementation
   2.4 Using the functional requirements
      2.4.1 Key outcomes
      2.4.2 Developing a software design specification for a business system with records management functionality
      2.4.3 Reviewing, assessing and auditing existing business systems
      2.4.4 Undertaking the review process
   2.5 Entity relationship models
      2.5.1 Record categories and the records classification scheme
      2.5.2 Aggregations of electronic records
      2.5.3 Electronic records
      2.5.4 Extracts
      2.5.5 Components

3 FUNCTIONAL REQUIREMENTS
   3.1 Creating records in context
      3.1.1 Creating a fixed record
      3.1.2 Record metadata
      3.1.3 Managing of aggregations of electronic records
      3.1.4 Records classification
   3.2 Managing and maintaining records
3.2.1 Metadata configuration 129
3.2.2 Record reassignment, reclassification, duplication and extraction 131
3.2.3 Reporting on records 132
3.2.4 Online security processes 132
3.3 Supporting import, export and interoperability 135
3.3.1 Import 135
3.3.2 Export 136
3.4 Retaining and disposing of records as required 137
3.4.1 Compliance with disposition authorisation regimes 137
3.4.2 Disposition application 139
3.4.3 Review 141
3.4.4 Destruction 142
3.4.5 Disposition metadata 143
3.4.6 Reporting on disposition activity 144

4 APPENDICES 145
A Glossary 145
B Integrating recordkeeping considerations into the systems development life cycle 153
1 Project initiation 153
3 Requirements analysis 154
4 Design 154
5 Implementation 155
6 Maintenance 155
7 Review and evaluation 156
C Further reading 157
1 INTRODUCTION

Organisations implement business systems to automate business activities and transactions. As a result, the electronic information generated by a business system increasingly serves as the only evidence or record of the process, despite the system not being designed for this purpose. Without evidence of these activities, organisations are exposed to risk and may be unable to meet legislative, accountability, business and community expectations.

Because of the dynamic and manipulable nature of business systems, the capture of fixed records and the ongoing management of their authenticity, reliability, usability and integrity can be challenging. Organisations are therefore faced with a significant risk of mismanagement, inefficiency and unnecessary expenditure.

While these same organisations may have an electronic records management system (ERMS), it may not capture all records of the organisation. This document is designed to address the records management gap caused by the increasing use of business systems.

It provides guidelines on identifying and addressing the needs for records, and a set of generic requirements for records management functionality within business systems software. It aims to:

- assist organisations to improve electronic records management practices;
- reduce the duplication of effort and associated costs in identifying a minimum level of functionality for records in business systems; and
- establish greater standardisation of records management requirements for software vendors.

The document does not prescribe a specific implementation approach. The intent of these specifications can be realised through interfacing or integrating the business system with an electronic records management system or by building the functionality into the business system.

1.1 Scope and purpose

This document will help organisations to ensure that evidence (records) of business activities transacted through business systems are appropriately identified and managed. Specifically, it will assist organisations to:

- understand processes and requirements for identifying and managing records in business systems;
- develop requirements for functionality for records to be included in a design specification when building, upgrading or purchasing business system software;

---

An electronic records management system is a type of business system specifically designed to manage records. However, in the interests of clarify and brevity, for the purpose of this document, ‘business system’ should be taken as excluding an electronic records management system.
- evaluate the records management capability of proposed customised or commercial off-the-shelf business system software; and
- review the functionality for records or assess compliance of existing business systems.

It does not provide a complete specification but rather outlines a number of key records management requirements, with recommended levels of obligation, that can be used as a starting point for further development. As outlined in the document, organisations will still need to assess, amend and select their requirements based on their business, technical and jurisdictional environments and constraints.

This Module only addresses records management requirements and does not include general system management. Design requirements such as usability, reporting, searching, system administration and performance are beyond the scope of this document. It also assumes a level of knowledge about developing design specifications, procurement and evaluation processes, therefore these related issues are not covered in any detail.

Requirements for the long-term preservation of electronic records are not explicitly covered within this document. However, the inclusion of requirements for export supports preservation by allowing the export of records to a system that is capable of long-term preservation activities, or for the ongoing migration of records into new systems.

While the guidance presented in this Module should be applicable to recordkeeping in highly integrated software environments based on service-oriented architectures, such scenarios are not explicitly addressed. Similar principles and processes will apply in such environments, but additional analysis will be required to determine what processes and data constitute, across multiple systems, the required evidence or record of any particular transaction.

Use of the term ‘system’ in this document refers to a computer or IT system. This is in contrast to the records management understanding of the term that encompasses the broader aspects of people, policies, procedures and practices. Organisations will need to consider these wider aspects, and to ensure that fundamental records management supporting tools such as disposition authorities,64 information security classifications and a records culture are in place, in order to ensure records from business systems can be appropriately managed.

1.2 Audience

The primary audience for this document is staff responsible for designing, reviewing and/or implementing business systems in organisations, such as business analysts and groups overseeing information and communications technologies procurement or investment decisions.

The audience also includes records professionals who are involved in advising or assisting in such processes, and software vendors and developers who wish to incorporate records functionality within their products.

---

64 A formal instrument that defines the retention periods and consequent actions authorised for classes of records described in the authority.
Given the target audience for this document, the use of specific records management terminology has been kept to a minimum. Where the use of such terminology is necessary, definitions can be found in the Glossary at Appendix A. Some key definitions are also provided in Section 1.4: Key definitions.

1.3 Related standards

Under its Electronic Records and Automation Priority Area, the International Council on Archives has developed a suite of guidelines and functional requirements as part of the Principles and Functional Requirements for Records in Electronic Office Environments project:

- Module 1: Overview and Statement of Principles;
- Module 2: Guidelines and Functional Requirements for Records in Electronic Office Environments; and

This document is Module 3 of the broader project. It has been developed with the support of the Australasian Digital Recordkeeping Initiative.

While this Module may be used as a stand-alone resource, for a broader understanding of the context and principles that have informed its development, readers should also refer to Module 1.

The functional requirements identified in Part 2 are based on the minimum requirements for records functionality as defined in the International Standard for Records Management, ISO 15489.


1.4 Terminology

It is recognised that many of the terms used in this document have different meanings for different disciplines. It is therefore important that this document is read in conjunction with the Glossary at Appendix A. A number of the key concepts used in this document are also detailed below:

- **Records** are information created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. They provide evidence of business transactions and can exist in any format.

- **business systems**, for the purposes of this document, are automated systems that create or manage data about an organisation’s activities. They include applications whose primary purpose is to facilitate transactions between an

organisational unit and its customers – for example, an e-commerce system, client-relationship management system, purpose-built or customised database, or finance or human resources systems. Business systems are typified by containing dynamic data that is commonly subject to constant updates (timely), able to be transformed (manipulable) and holds current data (non-redundant). For the purposes of this document, business systems exclude electronic records management systems.

- **Electronic records management systems** (ERMS) are specifically designed to manage the maintenance and disposition of records. They maintain the content, context, structure and links among records to enable their accessibility and support their value as evidence. Electronic records management systems are distinguished from business systems, for the purpose of this document, because their primary function is the management of records.

1.5 **Structure**

This document is divided into four main parts:

- **Part 1: Introduction** – describes the scope, purpose, audience and structure of the overall document.

- **Part 2: Guidelines** – provides background information on the importance of records management, describes key terms and concepts, and outlines a process for determining an organisation’s need for records and identifying records within business systems. It also outlines some of the issues and processes to be considered when reviewing, designing, purchasing or building business systems to incorporate functionality for records.

- **Part 3: Functional requirements** – provides an overview of the high-level functional requirements for records that may be incorporated into a business system, and outlines a recommended set of mandatory and optional records management functional requirements for business systems (referred to as the ‘functional requirements’).

- **Part 4: Appendices** – provides a glossary of key terms and a list of additional reading.

2 **GUIDELINES**

2.1 *Why is it important to have evidence of business processes and activities?*

A key way organisations account for their activities is through evidence of business transactions in the form of records. Records are valuable business assets that enable organisations to defend their actions, improve decision-making, prove ownership of physical and intellectual assets, and support all business processes.

Records are ‘information created, received, and maintained as evidence and information, by an organisation or person, in pursuance of legal obligations or in the
transaction of business.

They must be retained for a period of time that is in line with an authorised retention schedule or ‘disposition authority’.

Organisations with business systems that have insufficient functionality for records risk loss of this evidence, resulting in inefficiency, an inability to meet accountability and legislative requirements, and a lack of corporate memory.

A record is not just a collection of data, but is the consequence or product of an event. A distinguishing feature of records is that their content must exist in a fixed form, that is, be a fixed representation of the business transaction. This can be particularly challenging in a business system that, by nature, contains data that is frequently updated and dynamic.

Records comprise not only content but also information about the context and structure of the record. This information can be captured through metadata. Metadata fixes the record in its business context and documents the record’s management and use over time. Records metadata therefore serves to identify, authenticate and contextualise the record, not only at the point of creation, but continues to document its management and use over time. It allows records to be located, rendered and understood in a meaningful way. The International Standard on Information and Documentation—Record Management Processes—Metadata for Records, Part 2, ISO 23081, provides a generic statement of metadata elements. Organisations may also have jurisdictional-specific elements sets to which they must adhere.

An appropriately managed record will:

- aid transparent, informed and quality decision-making and planning;
- provide an information resource that can be used to demonstrate and account for organisational activities; and
- enable consistency, continuity and efficiency in administration and management, among other benefits.

The International Standard on Records Management, ISO 15489, provides best-practice guidance on how records should be managed to ensure they are authentic, reliable, complete, unaltered and usable.

2.2 The business systems landscape and recordkeeping

Business systems are normally mapped against some form of business process. Given that records are the product of transactions and transactions, collectively, form business processes (for example, the transactions involved in processing an application for a licence), it follows that the integration of recordkeeping functionality in business systems should be undertaken from the perspective of the business process.

---

business processes having the greatest potential for reflecting good recordkeeping are those that are highly structured with well-defined transactions where the identification of where in the business process records should be generated and even what they should look like (for example, forms) is relatively clear. Similarly it follows that recordkeeping has great potential for being integrated successfully in the business systems supporting such business processes because, by necessity, their design has to be mapped to the transactions supporting the business processes. Furthermore, the development of business systems supporting defined business processes normally proceeds through a series of structured steps based on the use of generally accepted systems development tools and techniques that address each phase of the systems development life cycle, from planning and design to implementation and review. In addition, in well-managed business systems development projects, accountability for the integrity of the design, development, and maintenance of the systems (including the integrity of the data generated by the systems) is clearly assigned across all of those communities in the organisation that have a responsibility for the systems (that is, from business users of the systems to the specialists responsible for developing the systems). All of these factors heighten the potential for recordkeeping considerations to be integrated in the design of business systems supporting structured and well-defined business processes.

Recordkeeping integration is challenged significantly in an environment where business processes are poorly defined, where tools and techniques for systematically designing and developing systems are weak, and where accountability for the technologies supporting the environment (and especially the information generated in the environment) has not been assigned clearly. In such an environment individuals (often ‘office workers’ at all levels of the organisation) have a high level of autonomy in deciding what information they create and share, how they share it, where they put it, how they organise, describe and retain it, and how they dispose of it. Such an environment is often dominated by email messages and their attachments where there are few business rules to guide their creation, transmission and management. The integration of recordkeeping in such an environment is extremely difficult because the foundation of defined business processes (or workflow in the parlance of the modern office), structured approaches to systems development and assigned accountability are not in place (for more information, see Appendix B).

2.3 Determining needs for evidence of events, transactions and decisions in business systems

Not all information contained in a business system will necessarily be required to be recorded as evidence. Prior to reviewing, designing, building or purchasing business systems software, it is necessary to determine an organisation’s needs for records in order to develop and implement appropriate strategies. This process is outlined in Figure 1 and discussed in the following sections.

Figure 1: Steps to determine requirements for records
2.3.1 Analyse the work process

Business systems typically store large volumes of data that are frequently updated. Because of this, it can be difficult to know what information in the system needs to be managed as a record to provide evidence of the business process or transaction. Business systems may consist of:

- a collection of data elements (or structured data) that are linked and controlled by the system, for example, entries in a database;  
- distinct digital objects controlled by the system that have a clearly defined data format (or unstructured/semi-structured information), for example, documents, emails or spreadsheets; or
- a combination of the above.

The process of identifying records must commence by stepping back from the IT system itself, and undertaking an analysis of the work processes, including related

---

This document primarily focuses on the management of records arising from structured rather than unstructured data.
regulatory and business requirements, to determine what evidence is required to be kept.70

As records are directly linked to business processes, identifying the records is assisted by standard business process analysis techniques and tools, such as activity diagrams, process decompositions and flowcharts.71

It is important to work closely with the organisation’s records professionals during this process, as much of this work may have been undertaken when developing the organisation’s disposition authority.72

The process of identifying the records entails two main tasks. These are:

1. identification of requirements for evidence of the business being conducted in the business system; and
2. identification of the information that records this evidence, that is, the ‘record’.

2.3.2 Identify requirements for evidence of the business73

Step 1 – determine the broad business functions and specific activities and transactions carried out, in full or in part, by the business system

This analysis may include consideration of business process documentation and system inputs, outputs, and related policies and procedures.74 In highly integrated environments, multiple systems may need to be covered in the analysis in order to obtain a complete picture of the business process or activity. Particularly in the government environment, systems may also be shared by multiple organisations.

Step 2 – for each function, activity and transaction or business process managed by the system, consider what evidence is required to be retained by the organisation

Requirements may be derived from a number of sources. Consider such issues as:

- Are there legislative obligations to record certain evidence? Some legislation may implicitly or explicitly state the need to create certain records in certain forms.

---


71 For further information on modelling business process, see the business Process Modelling Notation website at http://www.bpmn.org/.


73 The term ‘evidence’ is used in this document in the sense of demonstrating or documenting the proof of a business transaction, rather than its narrower legal context.

74 This analysis may have already been done, either for records management purposes such as disposition or classification, or in the development of the system itself through business process review.
- Are there regulatory instruments that must be adhered to and require evidence to demonstrate compliance, for example, mandatory standards, codes of practice and so on?
- Are there organisational rules that require evidence be recorded, for example, policies, codes of conduct, reporting and so on?
- What evidence is required of decisions made to support the business process itself or to inform future decision-making?
- Are any of the business functions or activities of the organisation considered high risk or subject to a high level of litigation that demands a greater level of documented evidence?
- Who are the various stakeholders and what are the different expectations they may have about what evidence is required to be retained?
- What are the community’s expectations for evidence of the work process?

This process may involve a wide range of consultation and validation with senior management. The International Standard on Work Process Analysis for Records, ISO/TR 26122-2008, and the Australian DIRKS Manual are useful resources for these purposes.75

### 2.3.3 Identify the content and its associated management information that record this evidence

Not all information contained in a business system will necessarily be required to be recorded as evidence.

*Step 3 – for each requirement for evidence, identify the content or data that make up the evidence*

In systems that manage distinct digital objects, such as word-processed documents, data is already drawn together into a logical construct. This means that it can be relatively easy to identify specific documents or reports that contain the content that could act as evidence of a particular business activity or transaction.

For others, it will require analysis of the data structures, data models and class models that underlie the system to identify the specific data elements that together constitute the content and provide the necessary evidence (see Figures 2 and 3 below for an illustration of this).

It is important to note that the content or data that make up the evidence may not just be within the system. It may also be in other systems, documentation about the system, procedures, paper inputs and so on. Particularly in highly integrated systems.

---

environments, parts of the required evidence may be held across multiple systems and some systems or components may be shared with other organisations.

There may be a number of different content elements that could serve to make up the evidence. Deciding which content is best suited to form the required evidence will be based on an assessment of the business need and risk. Records need to be adequate, that is, there should be sufficient evidence of the conduct of business activity or transaction to be able to account for that conduct. Therefore a major initiative will be extensively documented, while a routine low-risk action may be documented with an identifiable minimum amount of information.

Figure 2 provides a representation of the contents of a database controlled by a business system. In this example the record is made up of a grouping of related data elements from a number of different fields. Each record will consist of the identified data elements in the database and the associated metadata required to link the elements and provide the necessary structure and context to support the record.

**Figure 2: Identification of information components/data elements comprising an electronic record in a database**

Note that it is possible for a single record to include multiple elements from a single database field or table, and that it is also possible for a single data element to form part of more than one record.

---

76 Figure 2 provides a view of a normalised database. Relational database concepts, standard data modelling and normalisation techniques should be enforced to provide the necessary structure and context to support the traceability of the record.

77 ‘Record’ is used here in the records management sense rather than its database meaning.
Figure 3 provides a simplistic example of the tables that comprise a portion of a relational database for a human resource management system. Each table represents a portion of the database that contains closely linked information. Tables A, B and C provide data relating to personnel, salaries and cost centres, respectively. Tables D and E provide linkages between the data elements in the other tables. Table D links staff with their relevant pay levels, while Table E links staff with their cost centres.

Each table consists of a number of columns that represent fields containing data elements. The rows within each table establish linkages between data elements within the different fields. In database literature, these rows within tables are sometimes referred to as ‘records’, although these linked data elements are not always records in the records management sense of the term.

In line with the business process analysis, there are a number of potential records in Figure 3. These records are represented as a number of inter-related data elements that may be connected across one or more tables and comprise data elements from one or more fields.
Figure 3: Further example of the identification of information components/data elements comprising an electronic record in a database

<table>
<thead>
<tr>
<th>Table A: Personnel</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Staff no.</strong></td>
<td><strong>Surname</strong></td>
</tr>
<tr>
<td>0078652</td>
<td>Larsen</td>
</tr>
<tr>
<td>0078653</td>
<td>Lee</td>
</tr>
<tr>
<td>0078654</td>
<td>Smith</td>
</tr>
<tr>
<td>0078655</td>
<td>Schmidt</td>
</tr>
<tr>
<td>0078656</td>
<td>Darcy</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table B: Salaries</th>
<th></th>
<th>Table C: Cost centres</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pay code</strong></td>
<td><strong>Level</strong></td>
<td><strong>Year</strong></td>
</tr>
<tr>
<td>A41</td>
<td>APS4</td>
<td>Year 1</td>
</tr>
<tr>
<td>A42</td>
<td>APS4</td>
<td>Year 2</td>
</tr>
<tr>
<td>A43</td>
<td>APS4</td>
<td>Year 3</td>
</tr>
<tr>
<td>A44</td>
<td>APS4</td>
<td>Year 4</td>
</tr>
<tr>
<td>A51</td>
<td>APS5</td>
<td>Year 1</td>
</tr>
<tr>
<td>A52</td>
<td>APS5</td>
<td>Year 2</td>
</tr>
<tr>
<td>A53</td>
<td>APS5</td>
<td>Year 3</td>
</tr>
<tr>
<td><strong>Staff no.</strong></td>
<td><strong>Pay code</strong></td>
<td></td>
</tr>
<tr>
<td>0078652</td>
<td>A53</td>
<td></td>
</tr>
<tr>
<td>0078653</td>
<td>A42</td>
<td></td>
</tr>
<tr>
<td>0078654</td>
<td>A42</td>
<td></td>
</tr>
<tr>
<td>0078655</td>
<td>A41</td>
<td></td>
</tr>
<tr>
<td>0078656</td>
<td>A51</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table D: Staff to pay levels</th>
<th></th>
<th>Table E: Staff to cost centres</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Centre code</strong></td>
<td><strong>Cost centre</strong></td>
<td><strong>Director</strong></td>
</tr>
<tr>
<td>M001</td>
<td>Melbourne Office</td>
<td>Shay Jones</td>
</tr>
<tr>
<td>S001</td>
<td>Sydney Office</td>
<td>Fred Nguyen</td>
</tr>
<tr>
<td>P001</td>
<td>Perth Office</td>
<td>Alberta Johnson</td>
</tr>
<tr>
<td>C001</td>
<td>Canberra Office</td>
<td>John Wasp</td>
</tr>
<tr>
<td><strong>Staff no.</strong></td>
<td><strong>Centre code</strong></td>
<td></td>
</tr>
<tr>
<td>0078652</td>
<td>M001</td>
<td></td>
</tr>
<tr>
<td>0078653</td>
<td>M001</td>
<td></td>
</tr>
<tr>
<td>0078654</td>
<td>C001</td>
<td></td>
</tr>
<tr>
<td>0078655</td>
<td>S001</td>
<td></td>
</tr>
<tr>
<td>0078656</td>
<td>P001</td>
<td></td>
</tr>
</tbody>
</table>

Key

- Yellow: Data elements comprising the personnel record of Kyra Darcy
- Blue: Data elements comprising the record of Bob Smith's address details
- Red: Data elements comprising the record of Melbourne Office staff
Three distinct types of records have been identified in the system:

- The yellow rows identify data elements that form a single personnel record. This record spans data elements in all five tables and contains information on the staff member, name, address, salary level and cost centre.

- The blue row identifies data elements that provide a record of an individual’s name, address and staff number. This single row of information could be construed as a record, but in this case the record indicated by the yellow rows is more comprehensive and would be preferable.

- The red rows identify data elements that form a record of all staff members belonging to a particular cost centre. These rows may represent an alternative method of interrogating the data contained in the tables.

Note that the information contained in Table B does not constitute a record in this scenario, only part of the staff salary record. This is because the data contained in Table B is supplemental and only gains value as a component of a record when it is placed in context of a staff member in Table A. The Table B information itself is likely to have come from an external record such as a workplace agreement.

It should be noted that there may, in some instances, be overlap between records identified in a database. The data elements that form part of one record in a relational database may also form part of other records generated by the same database. For example, the staff record of ‘Jamie Lee’ and the record of Melbourne office staff will both draw on the same data elements from Table A.

Where overlap occurs between the data elements that form electronic records, the business system must be capable of ensuring that it will not destroy the shared data elements until both identified electronic records have reached their minimum retention period.

**Step 4 – identify the additional information required to manage the content over time as evidence**

This will be the records metadata that is an integral part of the record. Records metadata can be used to control the length of time a record is maintained, establish its access rights and restrictions, and facilitate searching for and retrieval of the record.

The creation, capture and management of metadata for records are essential to allow records to be identified, understood and retrieved, and to protect the evidence of their authenticity, reliability and integrity. Metadata should be captured in line with an identified metadata standard for records, as stipulated by jurisdictional and/or organisational requirements.

Metadata does not need to be retained together with the content, as long as they are linked or associated in some way. Metadata may be contained in systems external to the business system in question, or may encompass documentation or tools such as XML schemas and data, and class models that allow records to be understood and remain meaningful over time.

Particularly in database environments, it can be difficult to distinguish between the record’s content and its metadata. For example, metadata that provides evidence that
a particular person accessed a record on a particular date and/or time is itself a record. Often metadata in a business system pertains to the system as a whole. That is, it applies in an overarching way to all records in the system, not to individual records. It can reside in system rules or system documentation and not be applied to individual records.

### 2.3.4 Identify linkages and dependencies

A key characteristic of records is that they cannot be understood in isolation. In order to provide context for the record, additional information about the work process or the business system may be required to ensure the records are understandable, to prove the reliability of the evidence, or if records need to be moved from one system to another in the future. Required system information may include:

- location;
- system issues/faults;
- size;
- business rules implemented;
- file formats;
- security;
- privacy management;
- data structures;
- data and class models;
- workflow routing rules; and
- audit trails.

Required information about the work process may include relevant policies and procedural documents to show that decisions are made and processes undertaken in accordance with authorised standards.

In addition, as noted in Section 2.3.1: Analyse the work process, many processes will extend beyond a single business system. Necessary linkages to other systems, or related information in paper form, must also be considered before strategies are developed to manage the records in the business system.

A key dependency is how long the records need to be kept. Records must be retained for a period of time that is in accordance with authorised legislative and jurisdictional requirements and business needs. Decisions about how long records must be retained are defined in a disposition authority. Organisations will need to meet the requirements of relevant jurisdictional authorities for retaining and disposing of records.78

---

78 For more information on disposition requirements, consult with your jurisdictional authority if relevant, or see ISO 15489, Section 4.2.4.
Records that are required to be retained for longer periods will generally require more stringent controls to ensure they can be managed and remain accessible for as long as required, as specified in an authorised disposition authority. Depending on demand for access to older records, the organisation may decide not to keep all records in the live system. However, it is essential that they can be identified and retrieved in accordance with agreed service levels.

### ‘Archiving’ and retention and disposition of records

The term ‘archiving’ has different meanings in the records management and IT communities (see Glossary at Appendix A).

‘Archiving’ of data to second-tier or offline storage does not change the recordkeeping requirements and should not be considered as meeting requirements relating to retention and disposition of records. In addition, backing up of business systems for business-continuity or disaster-recovery purposes does not meet disposition requirements.

For more information, see Section 3.4: Retaining and disposing of records as required.

### 2.3.5 Devise strategies to address core recordkeeping processes based on an options assessment

Following the identification of requirements for evidence in the form of records, and of the related dependencies and linkages, appropriate strategies to manage the records can be devised. Strategies must be based on an assessment of records-related risks.

To be considered authentic and reliable evidence, content must be fixed to a point in time and unalterable. Because business systems generally contain dynamic, current data that is subject to regular updates, strategies for maintaining a ‘fixed’ record must be implemented. These strategies will be influenced by the decision regarding which system will manage the records and informed by an options assessment.

Prior to use of the functional requirements, organisations will need to consider the extent to which functionality for records will be provided through internal mechanisms within a business system application itself, or whether the requirements will be met by interacting with software applications external to the system that are capable of providing the necessary records management functionality.

The mandatory functional requirements in this document outline the core recordkeeping processes that must be addressed. Options to implement these requirements, shown in Figure 4, may include:

- designing the business system to internally perform the records management functions;
- integrating with an identified records management system, such as an electronic records management system; or
- designing export functionality into the business system to directly export records and their associated metadata to an identified records management system.
These options are not exhaustive and others may be explored by organisations in determining a suitable approach.

For business systems that manage distinct digital objects, ‘fixing’ a record can be done through system controls, such as setting the object as ‘read only’, and applying record metadata that documents the record’s management and use over time, for example, event history metadata.

In contrast, database systems usually contain data that is frequently updated, manipulable and non-redundant or current, and therefore can pose challenges for ensuring the fixity of a record. Strategies to address this could include:

- Designing controls that prevent the overwriting or deletion of specific data into the system. For example, this could involve permitting the updating of data but recording the previous values in a history status field. The record is
formed by the combination of specified fields and the associated event history information. This does not mean all changes to data in the system are required to be retained. It is only applicable to those data elements that have been identified as forming the content of the evidential requirements.

For example:
A staff member enters details of a new client into the system. The client later changes their name and the staff member updates the system with the new details. The original name is still retained by the system and is managed and maintained as part of the record accordingly.

For example:
The value of assets for an insurance policy is automatically indexed each year and the ‘asset value’ field is automatically updated. To prove the value of the assets at the time of a claim, the information from the ‘asset value’ field is moved to a ‘previous value’ field when the update occurs. The system maintains previous values for the past three years (as a claim must be made within three years of an event), and for every year where a claim was made, in accordance with an approved disposition authority. The system logs the deletion of expired data, including appropriate approvals.

- Bringing together the selected data elements (this may be from within the same table or selected data from rows in different tables) and creating a distinct digital object that is fixed and unalterable. This strategy could be satisfied by the generation of a report or a read-only ‘historical’ version of the database.

For example:
An organisation uses a business system with a workflow engine to support the processing of loan applications. When the application is finalised, the system automatically generates a report giving details of the process, which is then stored as a record in their electronic records management system. The appropriate contextual information of the process, in the form of metadata, was gathered as it was routed through the engine and exported with the record to the electronic records management system.

Regardless of what strategy is selected, it is essential to ensure all core recordkeeping processes are addressed so that records are not only created and managed, but can also be appropriately disposed of.
For example:
A database is used to maintain customer orders. According to the organisation’s disposition authority, order details are required to be retained for two years after the order is completed. Once a year, a query is run on the system to identify all orders that were completed more than two years previously. The results of this query are checked by relevant staff to ensure they do not relate to any outstanding issues, and once approved, relevant fields are deleted. The report, sign off and confirmation of deletion are kept as evidence of this process.

The process was carefully designed to ensure only fields relevant to the order are deleted, and customer details (which are required to be retained for longer) are not affected.

Part 3: Functional requirements covers these core requirements. They are also outlined in Section 2.4.1: Key outcomes.

The decision as to which approach to take for a particular business system will be affected by a number of factors:

- the business needs, including the risk level for the particular business function. High-risk functions require more stringent documentation and records management controls;
- the overarching records management framework, including whether a distributed or centralised approach to records management is preferred; and
- consideration of what is technically feasible, given the particular systems concerned, for example, this may include whether the organisation has an electronic records management systems, how easy integration with it would be, the existing functionality of the business system and what changes would be necessary, the anticipated lifespan of the existing system and whether upgrading the system to include the necessary functionality is feasible.

Table 1 provides some indicative challenges and benefits for each of the system management options.

Table 1: Some considerations when selecting an approach for managing records created in business systems

<table>
<thead>
<tr>
<th>System options</th>
<th>Benefits</th>
<th>Challenges</th>
</tr>
</thead>
</table>
| Designing the business system to internally perform the records management functions | • Makes creating and managing records a core component of the business process  
• If a component-based technical architecture is used, the records management component can be reused for other systems  
• Provides additional historical data capability | • Storage issues  
• Increased development costs  
• Ensuring consistent management of related records across the entire organisation |
| Integrating with an identified records management system, such as an electronic | • Business systems records can be managed collectively with records created by other systems | • Seamlessness of process may be affected by the capability of the identified records |
records management system (federated records management) • Exploits re-use of external records management system

management system • Complexities arising when upgrading either system • Challenges for disaster recovery and maintaining appropriate audit trails • May require customised interface

Designing export functionality into the business system to directly export records and their associated metadata to an identified records management system • business systems records can be managed collectively with records created by other systems • May be more suited to existing systems • Duplication of records in the business system and identified records management system • Possible shortcomings in the import/export process • Users will need to know two systems – the business system for active information, and the records system for older information – unless a continued interface is provided

2.3.6 Risk and options assessment

Risk is a key factor to incorporate into the assessment of appropriate strategies. Risks may arise from not creating records in the first place, from disposing of records too soon, or from not ensuring the accessibility and readability of records over time. Possible consequences arising from these risks may include adverse publicity, inefficient business activity and a reduction in the organisation’s capacity to prosecute or defend allegations.

A robust risk assessment will inform the level of evidence required and how stringent recordkeeping controls need to be. Organisations may have jurisdiction-specific risk management frameworks in place that define different levels of risk, which can be used to prioritise the identified requirements for evidence.

It is particularly necessary to undertake a risk assessment where part of the evidence or record is supplied by an external organisation, or where information is held in systems shared by multiple organisations. Consideration needs to be given as to whether that external organisation or shared system can be relied on to maintain the necessary evidence for the required period. Strategies to mitigate this risk may involve ensuring the necessary evidence is kept within systems under the control of the organisation, or that agreements for shared systems include these requirements.

A feasibility analysis can help organisations to consider, in a structured way, the financial, technical, legal or operational capacity of the organisation to meet the requirements. A feasibility analysis will facilitate the making of informed and transparent decisions at key points during the developmental process.

Assessing operational feasibility may require consideration of issues such as the nature and level of user involvement in the development and implementation of the system, and management support for the new system. A technical feasibility
assessment may consider the knowledge of current and emerging technological solutions and the availability of technically qualified staff for the duration of the project and subsequent maintenance phase.\textsuperscript{79}

\textbf{2.3.7 Implementation}

As implementation activities are specific to the selected strategies, they are beyond the scope of this document. General system implementation requirements, such as change management, are also beyond the scope.

However, one key aspect of implementation is to ensure that appropriate roles and responsibilities are defined and agreed. Table 2 outlines a possible breakdown of roles. In practice, organisations will need to define further roles. Where business systems are shared across organisations, the roles and responsibilities of all parties should also be explored, and clearly understood and documented.

\begin{table}[h]
\centering
\begin{tabular}{|l|p{0.7\textwidth}|}
\hline
\textbf{User} & Any person with permission to access the business system application. That is, anyone who creates, receives, reviews and/or uses records stored in the business system. This is the standard level of access that most employees of an organisation will possess. \\
\hline
\textbf{Records administrator} & An authorised user with special access permissions that allow additional access to, and/or control over, records contained in the business system application. Record administrators may in some instances be assigned permissions to undertake tasks similar to those of the business system administrator, such as the ability to close and re-open records, create, extract of records and edit record metadata. The powers assigned to record administrators will vary depending on the business needs of the organisation and the level of responsibility of the role. \\
\hline
\textbf{business system administrator} & A person or role with designated responsibility for the operation of the business system, for example, configuration and administration functions. The business system administrator will have responsibility for assigning and removing the permissions allocated to users and records administrators. \\
\hline
\end{tabular}
\caption{User roles}
\end{table}

Table 3 provides an example of a matrix of roles and a snapshot of some possible permissible functions they may perform. It will require further development by organisations. ‘Yes’ means the business system \textbf{must allow} this combination of roles and functions. ‘No’ means the business system \textbf{must prevent} this combination of roles and functions. ‘Optional’ indicates that the business system may allow or prevent this combination of roles and functions, and that the organisation must determine whether its policies and procedures will allow or prevent this combination.


\hspace{1cm} 110
Table 3: Roles and functions

<table>
<thead>
<tr>
<th>Function</th>
<th>User</th>
<th>Records administrator</th>
<th>System administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create new records</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Add/edit record metadata when identifying the record(^{80})</td>
<td>Yes</td>
<td>Yes</td>
<td>Optional</td>
</tr>
<tr>
<td>Allocate disposition authorisation to a record or, where applicable, an aggregation of records</td>
<td>No</td>
<td>Optional</td>
<td>Yes</td>
</tr>
<tr>
<td>View audit trails</td>
<td>Optional(^{81})</td>
<td>Optional</td>
<td>Yes</td>
</tr>
<tr>
<td>Edit audit trail data(^{82})</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

2.4 Using the functional requirements

The functional requirements can be used by organisations for a number of purposes. These include:

- developing requirements for functionality for records to be included in a design specification and for evaluation purposes when building, upgrading or purchasing business system software; and
- reviewing the functionality for records or assessing the compliance of existing business systems.

Prior to using the functional requirements set, the records and records management needs will need to be identified as outlined in Section 2.3.

---

\(^{80}\) The business system administrator may determine which metadata elements users and authorised users can contribute to at the time of identifying the record. This includes determining which automatically inherited metadata elements, if any, can be amended or over-ridden.

\(^{81}\) Organisations need to determine whether there are valid operational reasons for allowing users to view audit logs.

\(^{82}\) The system should prevent any modification of the audit trail, including amendments by the business system administrator.
2.4.1 Key outcomes

The functional requirements are arranged into four key areas.

Figure 5: Key outcome areas

- **Creating records in context** – information systems that enable business activities or transactions need to capture evidence of that activity. In business systems, this involves identifying a set of electronic information to serve as the evidential record. Records have to be linked to their business context.

- **Managing and maintaining records** – electronic records have to be actively managed as evidence of business activity, maintaining their authenticity, reliability, integrity and usability. Much of the functionality required for ensuring the authenticity, reliability and useability of records is inherent in the design of business systems and is therefore beyond the scope of the document, although their importance is acknowledged. The ‘managing and maintaining records’ component of the functional requirements instead focuses on less common functionality.

- **Supporting import, export and interoperability** – systems have to ensure interoperability across platforms and domains and over time. As such, record information must be encoded in a manner that is understood and able to be modified, if necessary, for migration to newer technology platforms.

- **Retaining and disposing of records** – records have to be kept and must remain accessible to authorised users for as long as required for legislative, community and business needs, and then disposed of in a managed, systematic and auditable way. A hallmark of appropriate records management is the retention and appropriate disposition of records according to specified rules.
These are further explained in Part 3: Functional requirements.

The importance of records metadata

Records metadata is structured information that identifies, authenticates and contextualises records and the people, processes and systems that create, manage, maintain and use them, and the policies that govern them. While some records metadata is captured at the point of records creation, metadata continues to accrue over the life of the record. As such, it underpins all records processes. Therefore, functional requirements for records metadata are included in all the outcome areas of this document.

2.4.2 Developing a software design specification for a business system with records management functionality

The functional requirements can be used to inform the records management aspects of the design specification. As part of the procurement or design process, the business system software will be evaluated against the requirements stipulated in the design specification, including requirements for records management functionality. As the functional requirements are generic in nature, it is necessary for an organisation to review these requirements in light of its own particular business needs and constraints, and records management requirements. This analysis will help to identify the functionality the business system software will be required to deliver.

It is important that project teams draw on a range of expertise, including business owners, risk experts and records professionals, to ensure that systems are not over-specified, but are appropriate for their risk profile.

Step 1 – assessing the functional requirements

Establish the extent to which the records will be managed within the business system. For example, if the business system will only be responsible for creating the records, with the records subsequently exported to an electronic records management system for ongoing management, the functional requirements will need to be assessed to identify the appropriate and relevant requirements for inclusion in the specification, along with any additional requirements relating to system integration/export.

Also assess the appropriateness of mandatory and optional requirements to determine whether the functionality described is appropriate to the organisation’s business and records management needs.

Questions to consider include:

- Is the requirement appropriate for the organisation’s business and records management needs?
- Will users use the functionality described in the requirement?

83 The evaluation process may be supported by reference site visits that provide opportunities for exploring the nature of the recordkeeping functionality of a business system.
Is it more cost effective or efficient to fulfil the requirement outside the business system software?

Consider implementing extra functionality that will add value to the business system, and assist in performing the organisation’s business activities and transactions. Remove any functionality surplus to the organisation’s needs.

**Step 2 – check appropriateness of the requirements**

Consider whether the phrasing of the functional requirements identified as applicable in Step 1 is appropriate for the organisation. The descriptions of some requirements may need to be adjusted to better reflect the organisation’s business needs.

Where requirements are drawn from these functional requirements, organisations are encouraged to adopt relevant definitions directly from Glossary at Appendix A. The requirements employ highly structured terminology that must be kept in context if they are to retain their intended meaning.

**Step 3 – check appropriateness of the obligation levels**

Evaluate the obligation levels attached to the requirements to determine whether they should be mandatory or desirable, in line with business needs.

The obligation levels attached to the functional requirements provide a guide for use in developing an organisation’s own software design specification. Depending on decisions as to what extent records management functionality will be achieved by building it into the system, or by integrating with an electronic records management system, some requirements (including those recommended as mandatory) may not be relevant.

Organisations should consider carefully removing a mandatory requirement or altering a mandatory obligation level. This may involve identifying how the functionality described in the requirement can be achieved through a substitute practice. For example, some requirements may outline functionality that could be addressed through the implementation of appropriate business rules rather than a software solution.

**Step 4 – identify gaps in the functional requirements**

Assess the functional requirements identified as appropriate in their totality to determine whether the organisation requires any functionality that is not adequately covered by the requirements. Add any additional requirements necessary to meet the gap in required functionality.

### 2.4.3 Reviewing, assessing and auditing existing business systems

Organisations may use the functional requirements to review and assess the functionality for records in business systems. Such a review will give an organisation:

- an understanding of the records management strengths and weaknesses of its existing business systems;
- an appreciation of its potential exposure to records-related business and accountability risks (resulting from the weaknesses identified in the business systems); and
- an informed basis for developing strategies to improve the records management functionality.

2.4.4 Undertaking the review process

The review process is essentially a ‘gap analysis’, comparing a particular business system with the functional requirements as an established benchmark.

When undertaking the review, it is important to consider the broader system environment including business rules, processes and related physical or electronic systems, not just software functionality, as some records management requirements may be satisfied via supporting infrastructure mechanisms rather than by the software itself.

Where records are being managed in an external system to the business system, assessing compliance with the mandatory elements of the specification should consider the compliance level of both systems holistically.

The focus of the assessment process will vary depending on the nature of the review. A review initiated as part of an audit process will focus on identifying the level of compliance with existing standards and areas where the business system fails to support adequately the records management requirements of the organisation. In contrast, a review conducted as a preliminary step towards upgrading an existing business system will focus on identifying strengths and weaknesses in the existing software and areas of additional functionality that may be incorporated to better meet the organisation’s business needs.

Conducting a review of a business system may comprise the following tasks:

**Preparation and preliminary research**

Identify the business system software application, or applications, that will be the subject of the review, along with their components (including integrated databases) and supporting infrastructure and documentation. Undertake preliminary research so that staff conducting the review can familiarise themselves with the business processes managed or controlled by the business system, the software itself and the objectives of the review.

**Identify the need for evidence**

Before the system can be assessed for its ability to manage records appropriately, first analyse and understand the business processes and identify the requirements for creating evidence of business activities and transactions in the form of records, as outlined in Section 2.3.

---

Create a checklist of requirements

Compile all requirements that are relevant to the organisation’s business and records management needs into a checklist, including relevant obligation levels.

The checklist may consist of a straightforward list of requirements, or may be reframed as a series of questions. Depending on the purpose of the assessment, ‘yes’ and ‘no’ responses to determine a pass or fail for each requirement may be appropriate, or a rating system to measure the degree of compliance (for example, a scale of 1 to 5 for each requirement) could be used. The method employed should allow a clear determination to be made on whether each requirement has been adequately addressed by the business system.

The checklist should include space for comments so that details of how each requirement is met can be included. It is particularly useful to capture information of ‘workarounds’ that have been adopted by staff to deal with any perceived shortcomings of the software itself.

Apply the checklist to the business system

In order to be able to apply the checklist, it will be necessary to have a good understanding of how the system presently manages the records of the identified business processes. An assessment based on AS/NZS/ISO 15504, Information Technology – Process Assessment may be helpful in this regard.

The process of applying the checklist may involve a mix of ‘hands-on’ demonstration of the software as well as discussions with relevant business managers, business system administrators and system users to understand the interplay of software functionality with related processes and procedures, to capture a full picture of how each aspect of records management functionality is, or is not, met.

Where the business system is assessed as not meeting a functional requirement, it will be necessary to determine whether this is because of a fundamental inadequacy of the system or because the system has simply not been configured to perform the identified functionality.

Evaluate the results of the review and prioritise improvements

Evaluate the information collected during the review, identify weaknesses and strengths, and determine recommendations for improving functionality for records. Recommendations may be prioritised based on risk, importance and feasibility, for example, if the system is unlikely to be developed in the near future, greater attention could be paid to improving records management controls through implementing revised processes or business rules, whereas if the review was undertaken to inform system redevelopment, then priority could be given to automated mechanisms to improve records management.

---

85 For example, a requirement may be met through a supporting infrastructure mechanism, such as an integrated software application or manual processes conducted in accordance with the organisation’s information management policies and procedures, rather than the business system software itself.
2.5 Entity relationship models

The functional requirements were developed using entity relationship modelling. Figure 6 outlines the conceptual relationship model for the management of electronic records by a business system. Explanatory information for each entity around the business system is further described below.

Figure 6: Entity model for electronic records management in a business system

2.5.1 Record categories and the records classification scheme

A records classification scheme is a hierarchical classification tool that can facilitate the capture, titling, retrieval, maintenance and disposition of records. It defines the way in which records are grouped together (aggregated) and linked to the business context in which they were created or transmitted. By classifying records in this way, many of the records management processes can be carried out quickly and efficiently.

---

86 A conceptual model used to design information systems.
It is assumed that business systems will generally not support a records classification scheme internally, but that records will need to be mapped to the relevant record categories from the scheme.\(^7\)

However, for some business systems that support a diverse range of business processes it may be desirable to include support for a records classification scheme, or an extract of one within the business system. The functional requirements for records classification schemes in *Module 2: Guidelines and Functional Requirements for Records in Electronic Office Environments* can be used for this purpose.

Figure 6 presents a model where extracts of a classification scheme are within the business system; it would also be appropriate to map records to external categories. Pre-defined system rules established by the business system administrator may provide an appropriate mechanism for enabling the automatic mapping of metadata associated with external record categories to the corresponding electronic records (or aggregations of electronic records – see Section 2.5.2) controlled by the business system. These rules may be established to ensure that when certain types of records are created or received by the system they are automatically assigned a corresponding set of pre-determined metadata elements.

### 2.5.2 Aggregations of electronic records

Aggregations of electronic records are accumulations of related electronic record entities that, when combined, may exist at a level above that of a singular electronic record object, for example, a folder. Aggregations represent relationships that exist between the electronic records controlled by a business system. These relationships are reflected in the metadata links and associations that exist between the related electronic records, and between the electronic records and the system.

A business system may comprise aggregations of records, records that are not aggregated, or both. Aggregating related electronic records can improve the ability of the business system to apply records management processes to those records. Business systems that support the aggregation of electronic records may not necessarily require that all electronic records be assigned to an aggregation on creation of the record. Aggregation may be at more than one level, depending on business needs.

Aggregations of electronic records may reflect relationships such as shared characteristics or attributes, or the existence of sequential relationships between related electronic records. The nature of the relationship between the electronic records of a particular aggregation will vary depending on factors such as the purpose and structure of the business system, and the content and format of the records themselves.

For example, an aggregation of electronic records may collectively constitute a narrative of events (that is, a series of connected business transactions), in which the records may have a sequential relationship with each other. Any such sequential

\(^7\) A *record* category is a subdivision of the *records* classification scheme, which may be further subdivided into one or more lower-level *record* categories. See the Glossary at Appendix A for a more detailed definition.
relationship between electronic records can be determined through the metadata elements associated with the records, such as titles, dates, author, container number (where applicable) and other attributes. Where these relationships exist between records controlled by the business system, the system should be capable of identifying, capturing, documenting and preserving them.

These aggregations may be formal structured relationships, supported by the business system (for example, digital folders containing related digital documents), or may exist as less formalised, tightly bound metadata relationships recognised by the system as establishing links between related records within an aggregation.

The aggregations must be fixed and maintained over time. Any change to an aggregation must be logged with an explanation. This aggregation for records management purposes should not be confused with, or replaced by, the generation of multiple different aggregations in response to search requests or report queries.

2.5.3 Electronic records

The system must be capable of managing multiple electronic records and associated metadata. Management of the electronic records controlled by the system will largely be determined by pre-defined system rules established by the business system administrator. System rules effectively provide the bridge between the business system software and the records controlled by the system. These rules are the means by which records management processes may be applied to the records and essentially determine how the system will operate.

2.5.4 Extracts

An extract is a copy of an electronic record, from which some material has been removed or permanently masked. An extract is made when the full record cannot be released for access, but part of the record can.

A business system may support generating and maintaining one or more extracts of an electronic record. These extracts may be created, retained and managed by the business system or by integrating or interfacing with an external software application.

2.5.5 Components

Components are constituent parts that comprise a digital record, for example, the multimedia components of a web page. Electronic records will comprise at least one component. Electronic records that comprise more than one component may be referred to as ‘compound records’.

The nature of the components that comprise a given electronic record will vary among systems. A component may be a digital object, such as a digital document, or a data element, such as an entry in a database. For example, a component of an electronic record in a system that encompasses the management of documents may consist of a single word-processed document, while components forming an electronic record in a human resource management system may comprise a number of closely linked data entries in a database (such as all data entered in connection with a single staff member’s personnel profile).
3 FUNCTIONAL REQUIREMENTS

This section lists the set of functional requirements for records in business systems. They are divided into four sections according to key records management concepts and processes.

The functional requirements focus on the outcomes required to ensure records are managed appropriately. As such, they do not specify particular processes, as it is recognised that the techniques and strategies to achieve the outcomes will depend on the type of system being used.

Each requirement details a specific aspect of records management functionality. They are divided into the sections and subsections outlined in Figure 5 in Section 2.4.1: Key outcomes. The introductory text to each section aims to provide summary information regarding the records management concept and the overarching aim of the subsequent requirements.

**Records metadata**

Metadata is essential to the appropriate management of records. Unlike resource discovery metadata, records metadata is not static but accrues through time, documenting changes to and use of the record. For this reason, requirements for records metadata are incorporated into all the functional requirements sections.

**Integration with other systems**

As outlined in the Part 2, it is acknowledged that organisations may choose to undertake the management of records externally to the business system. This can be achieved by either directly exporting the records or by integrating with an external records management system, as outlined in Figure 4 in Section 2.3.5.

Choices made about how the records will be managed will influence the extent to which the outlined requirements are selected or amended for inclusion within a business system. While the requirements are phrased in terms of the functionality that a business system ‘must’ or ‘should’ possess, it is acknowledged that, depending on the model chosen, the requirement does not have to be met purely within the business application in question, but may be met through the use of additional tools, operating software or integration with, or export of the reports to, external records management systems.

**Exclusions**

While these functional requirements do not cover common system management and design requirements, such as usability, searching, reporting, access, security and back-up, it is acknowledged that such processes also support the records management functionality of the system. For example, access and security controls help ensure authenticity and integrity of records, and reports can be used to identify records due for destruction.

The functional requirements assume that needs for evidence of business transactions in the form of records have already been identified (see Section 2.3).
Types of requirements

The specification contains two types of requirements:

- **Non-conditional requirements** – stand-alone requirements that are independent of any other requirement listed.

  **For example:**
  The BS must be able to capture and maintain metadata relating to any business classification scheme or records classification tools it supports, in accordance with relevant metadata standards.

- **Conditional requirements** – requirements that depend on the system supporting a specific non-conditional requirement in order for the conditional requirement to apply. Conditional requirements commence with the term: ‘Where the business system [supports or does not support a particular requirement] it must/should/may …’

  **For example:**
  Where the BS supports links between disposition functions and other records management mechanisms supported by the BS, it must warn a business system administrator when control mechanisms linked to disposition classes are updated – and protect disposition classes from amendment until revisions are complete.

Conditional requirements are grouped under the relevant non-conditional requirement, regardless of obligation level or the relevant aspect of records management functionality. For example, disposal requirements that are conditional on support for a records classification scheme appear in Section 3.1.4: Records Classification.

Each non-conditional requirement has been given a simple sequential number (1–1240). Conditional requirements are given a two-part number based on the relevant non-conditional requirement (for example, 3.1, 3.2).

Obligation levels

The obligation levels indicate the relative importance of each of the functional requirements. The keywords ‘must’, ‘should’ and ‘may’ that appear in the specifications are to be interpreted as follows:

- ‘Must’ – requirements that use ‘must’ are an absolute requirement for compliance with the specification.
- ‘Should’ – requirements that use ‘should’ may be ignored if a valid reason exists, but the full implications of ignoring must be understood and carefully weighed before choosing a different course.
- ‘May’ – requirements that use ‘may’ are optional.

Obligation levels must be understood in light of the preceding discussion on integration with other systems.
3.1 Creating records in context

The following list of functional requirements is concerned with ensuring:

A fixed record is created – business systems generate information at each stage of a business process. The identification of needs for records should establish at what point in the process a record should be created. Any further processes that happen in the system after this point must result in the creation of a new record or the augmentation of the existing record, rather than alteration to it. This means that data which needs to be kept to record previous decisions or processes cannot be overwritten but new data can be added. Depending on the assessment of requirements for records, there may be no need to retain the data and it can be overwritten. If possible, it is important to ensure that the system is not ‘locked down’ to such an extent that simple mistakes (such as mis-typing a name) cannot be corrected – although permission for changes may be restricted to a business system administrator.

Once the records that the organisation needs to serve as evidence of a business process have been identified, it is necessary to ensure that the business system is capable of creating those records.

The type and volume of records that may be created by a business system will vary depending on the nature of the business being conducted by the system and the related records management requirements. Some business systems will be capable of creating a wide range of electronic records using complex data formats (for example, geospatial data systems); while other systems may only support the creation of relatively basic electronic records of a single type.

The electronic records created by a business system may comprise digital objects – such as digital documents (for example, word-processed documents or spreadsheets), websites, audio and video – or other specialised data formats, and/or data elements and related metadata.

Creating the records may involve identifying existing digital objects that are to be managed as records, configuring the system to ensure that transactions are recorded and not overwritten, or identifying certain fields (and the relationships between them) that can be ‘set aside’ as the record of a particular event.

- Metadata for records is captured – to be meaningful as evidence of a business process, records must be linked to the context of their creation and use. In order to do this, the record must be associated with metadata about the business context.

Much of this information can be automatically generated by the system. Metadata integration in the functional requirements has been undertaken at a relatively high level. Rather than specifically detailing every metadata

---

A decision to allow the overwriting of data may be regarded as a disposition action and depending on jurisdictional requirements, may require authorisation through a records disposition authority.
element required, the requirements set instead provides broad references to the need for certain areas of business system functionality to be capable of creating, capturing and maintaining adequate metadata elements. It is expected that each organisation will capture metadata for records in line with an identified metadata standard, in accordance with organisational and/or jurisdictional requirements.

- **Where relevant, aggregations of records can be managed and a records classification tool can be supported** – metadata about the business may be rendered in the form of data values selected from a business or records classification scheme, which can be used to classify records. Typically a business system will not contain an internal classification scheme and therefore detailed requirements have not been included in this document.\(^{89}\)

For systems that only relate to a limited number of transactions, this metadata may be found in the system documentation,\(^{90}\) rather than directly associated with every record within the system.

### 3.1.1 Creating a fixed record

The business system **must**, either alone or in conjunction with other systems:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ensure that electronic records created or received by the BS can be captured and stored along with associated metadata, regardless of format and technical characteristics.(^{91})</td>
</tr>
</tbody>
</table>
| 2 | Support mechanisms for capturing electronic records received by the system that are:  
• automated; or  
• a combination of automated and manual. |
| 3 | Support mechanisms to ensure that it can capture all electronic records that it is likely to receive from external records-generating systems.\(^{92}\) For example, these may include:  
• common office packages;  
• workflow applications;  
• electronic messaging systems;  
• e-commerce systems;  
• web content management systems;  
• imaging and graphic design systems;  
• multimedia applications;  
• corporate systems;  
• security administration systems; and  
• other business information systems.  
Records may also comprise more than one component. |

---

\(^{89}\) For information on functional requirements to support a records classification scheme, see Module 2: Guidelines and Functional Requirements for Records in Electronic Office Environments

\(^{90}\) System documentation may encompass schemas, data dictionaries, and data and class models.

\(^{91}\) Data file formats and document types should be specified according to business needs.

\(^{92}\) Systems to be supported should be specified according to business needs. Each BS will only receive records from a limited number of specific records-generating applications. Furthermore, not all BS are capable of receiving records from external records-generating applications.
3.1 Where the BS captures an electronic record made up of more than one component, it must maintain a relationship between all components and associated metadata so that they can be managed as a single record and retain the structural integrity of the record.

3.2 Where the BS creates or receives electronic records generated by electronic messaging systems, it should be able to capture attachments and embedded objects together with electronic messages as either linked records or a single compound record.

3.3 Where the BS creates or receives electronic records generated by electronic messaging systems, it should be able to undertake the bulk capture of electronic messages relating to the same transaction.

3.4 Where the BS creates or receives web-based electronic records, such as a dynamic web page, it should be able to capture the record as:
   • a single compound record;
   • an aggregation of linked component records;
   • a snapshot – ‘frozen’ in time;
   • a collection of components that can be regenerated or reproduced on request; or
   • a combination of the above.

3.5 Where the BS creates or receives electronic records generated by electronic messaging systems, it may allow electronic messages and attachments to be captured from within an electronic messaging system, such as an email client.

3.6 Where the BS creates or receives electronic records generated by electronic messaging systems, it may be able to indicate whether an electronic message in the system has an attachment, noting Requirement 3.5.

3.7 Where the BS creates or receives electronic records generated by electronic messaging systems, it must be capable of capturing and identifying all incoming and outgoing electronic messages and attachments.

4 Ensure each electronic record is uniquely identifiable and store this identification as metadata with the record.\(^93\)

The business system should, either alone or in conjunction with other systems:

5 Provide an application programming interface or similar to support integration with other systems, including an electronic records management system, so as to:
   • enable electronic records created or received by the BS to be exported to an external system;
   • enable, where required, an electronic records management system to establish an interface with a BS so that it may apply appropriate records management controls on the electronic records contained within the BS; and
   • provide a mechanism to enable the BS to import electronic records directly from an external BS,\(^96\) as required to support the system’s core business functions.

---

\(^{93}\) For example, by means of a symbol or special icon.

\(^{94}\) Some BS, such as e-commerce systems, are capable of creating and sending electronic messages in support of their primary business functions.

\(^{95}\) The identifier must be unique within the system. If a record is to be exported beyond the system, the identifier may need to be unique within the organisation, for example, by adding a prefix to it.

\(^{96}\) It is not uncommon for one or more BS to be closely integrated so as to permit the sharing of information between systems as part of the normal operating practice of the system. This will often involve digital records being transferred between systems as part of a workflow process.
### The business system may, either alone or in conjunction with other systems:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>6</td>
<td>Allow users to capture and store all electronic records received by the system in their native format.</td>
</tr>
<tr>
<td>7</td>
<td>Not limit the number of records that can be captured and retained by the system.97</td>
</tr>
</tbody>
</table>

The business system **may**, either alone or in conjunction with other systems:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Allow the organisation to specify the format or pattern of the unique identifier, either through configuration or through specified requirements.</td>
</tr>
<tr>
<td>9</td>
<td>Be required to convert an electronic record during the course of the capture process from its original format, native to the records-generating system, to a format compatible with the BS.98</td>
</tr>
<tr>
<td>9.1</td>
<td>Where the BS supports the conversion of electronic records from their original formats as part of the capture process,99 it must ensure that the context, content and structure of the original record format are retained and that relevant requirements for conversion are adhered to.100</td>
</tr>
</tbody>
</table>
| 10 | Support the naming of electronic records, either:
|   | • by the manual entry of names by users; or
|   | • through an automatic naming process pre-defined by the business system administrator or through specified requirements.
| 10.1 | Where the BS supports the naming of electronic records, it should provide features to support the process of naming of electronic records. For example:
|   | • an automated spell check; or
|   | • a warning if a user attempts to create a record using a name that already exists within the BS.
| 10.2 | Where the BS supports the naming of electronic records, it should be able to restrict the ability to amend the name of an electronic record to a business system administrator or other authorised user. |
| 11 | Provide mechanisms to ensure that an electronic record received by the system can be captured, even if the generating application is not supported by the operating environment of the organisation.101 |

### 3.1.2 Record metadata

The business system **must**, either alone or in conjunction with other systems:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Support the range of metadata elements detailed in relevant metadata standards and any other metadata required to support the organisation’s business.</td>
</tr>
</tbody>
</table>

---

97 Limitations should only be permitted if needed to meet a specific business requirement for the system. Limitations resulting from technical inadequacies of the system should not be permitted.

98 In some instances the conversion of record formats may be part of a system’s core business function. Alternatively, this situation may occur where a digital record uses a proprietary format that is not supported by the BS, but which may be converted into another format usable by the system.

99 This requirement also applies to format conversion undertaken as part of a bulk import process, as described in Requirement 54.

100 ‘Structure’ is used in the records management sense of the relationship between the component parts of the record, as opposed to data storage structures within a particular system.

101 This requirement applies particularly to transactional BS that regularly receive a wide variety of record formats which must be captured by the system.
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>Be able to automatically capture metadata acquired directly from an authoring application, an operating system, an electronic records management system or generated by the BS itself.</td>
</tr>
<tr>
<td>14</td>
<td>Capture all metadata specified during system configuration, and retain it with the electronic record in a tightly bound relationship at all times.</td>
</tr>
</tbody>
</table>
| 15 | Restrict the ability to amend record metadata, so that:  

- only selected metadata elements can be edited by any user during creation;  
- selected metadata elements can only be edited by an authorised user during creation; and  
- selected metadata elements can be edited by an authorised user.  

The restrictions may be specified in requirements, or through configuration by a business system administrator. |
| 16 | Support the ability for a business system administrator or other authorised user to amend or override metadata inherited by records and, where applicable, aggregations of records. |
| 17 | Allow the manual or automatic updating of all metadata attributes that are determined by classification, following reclassification of a record or, where applicable, an aggregation of records. |
| 18 | Be able to store selected metadata over time, regardless of whether the related record has been archived, deleted or destroyed. |

The business system should, either alone or in conjunction with other systems:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>19</td>
<td>Be able to capture metadata entered manually by a user.</td>
</tr>
</tbody>
</table>
| 20 | Allow the definition of:  

- customised metadata fields for electronic records;  
- selected metadata element set for particular record types; and  
- obligation levels for selected metadata elements  

either through specified requirements or through configuration by a business system administrator. |

---

102 Where the record is received by the BS, rather than being created by the system. The authoring application may in some instances be another external BS, which outputs records directly into the system.

103 Where a BS exports the records it creates or receives to an electronic records management system for storage and management, the record metadata generated by the electronic records management system must be captured and linked to the record. The level of integration between the BS and electronic records management system will determine how the systems manage the record metadata.

104 The BS will generate record metadata relating to records created by the system, as well as generating metadata pertaining to the receipt of records created by external software applications.

105 That is, a robust connection inextricably linking the metadata and the digital record to which it relates.

106 This requirement applies to revisions of all classification schemes that may be applied to the BS, not just those classification schemes defined within the system to manage records held by the BS. Where the BS does not support the definition of a classification scheme, changes to an organisation’s classification scheme may need to be updated manually.

107 Metadata may be stored directly by the BS, in an integrated digital object store or exported to another system.

108 Obligation levels should reflect those specified in relevant metadata standards.
The business system **may**: 

23.1 Where the BS supports the use of pre-defined system rules to assign metadata on capture, the establishment and amendment of such rules must be restricted to the business system administrator.

23.2 Where the BS supports the use of pre-defined system rules to assign metadata on capture, it should enable records, and where applicable aggregations of records, to be assigned metadata retrospectively, following a change to the pre-defined system rules.

### 3.1.3 Managing of aggregations of electronic records

The business system **may**, either alone or in conjunction with other systems:

24.1 Be able to generate a unique identifier for each aggregation of records defined by the system.

24.2 Be able to automatically record the time and date of creation of an aggregation of records, within the metadata profile for the aggregation of records.

24.3 Allow a business system administrator to configure the naming mechanisms for aggregations of records.

24.4 Allow the re-assignment of records from one aggregation of electronic records to another by a business system administrator or other authorised user.

24.5 Ensure that records attached to an aggregation of records remain correctly allocated following reclassification of that aggregation of records, so that all structural links remain in place.

24.6 Ensure that details of any amendments made to the content of an aggregation of records are captured and maintained in the relevant metadata profile.

24.7 Prevent the destruction or deletion of aggregations of records at all times, except as specified in Section 3.4: Retaining and disposing of records as required.

---

109 Noting the usual audit trail requirements for systems.

110 Pre-defined rules may provide a substitute mechanism for assigning metadata at the time of creation. This method is particularly useful for systems that deal with a limited number of record classes and are unable to incorporate or integrate the definition of a records classification scheme.

111 The nature of these aggregations will vary depending on the type and function of the BS.

112 The identifier must be unique within the system. If a records aggregation is to be exported beyond the system, the identifier may need to be unique within the organisation, for example, by adding a prefix to it.
24.8 Ensure that any disposition action applied to an aggregation of electronic records is carried out on all the records that comprise the aggregation.

3.1.4 Records classification

The business system should, either alone or in conjunction with other systems:

| 25 | Allow records, and where applicable aggregations of records, to be classified in accordance with the organisation’s records classification scheme. |

| 26 | Support close linkage and interaction between a record’s classification and other records management processes, such as capture, access and security, disposition, searching and retrieval, and reporting. |

3.2 Managing and maintaining records

Once records have been created, they must be managed and maintained for as long as required. Records must be managed to ensure they have the following characteristics:

- **Authenticity** – the record can be proven to be what it purports to be, to have been created or sent by the person that created or sent it, and to have been created or sent at the time purported.
- **Reliability** – the record can be trusted as a full and accurate representation of the transactions to which they attest, and can be depended on in the course of subsequent transactions.
- **Integrity** – the record is complete and unaltered, and protected against unauthorised alteration. This characteristic is also referred to as ‘inviolability’.
- **Usability** – the record can be located, retrieved, preserved and interpreted.

The functional requirements detailed below are not sufficient to ensure that records in business systems have all these characteristics. Normal system controls over access and security support the maintenance of authenticity, reliability, integrity and usability, and therefore should be appropriately implemented. However, as noted in Section 3.1, as this functionality is common to business systems, these have not been included in the functional requirements below.

A risk assessment can inform business decisions of how rigorous the controls need to be. For example, in a high-risk environment, it may be necessary to prove exactly what happened, when and by whom. This links to the system’s permissions and audit logging to prove that approved actions are undertaken by authorised people. For example, security, audit logs, access controls (including limits on who can edit and amend information) and search tools are common system requirements that ensure records have the necessary characteristics.

---

113 The incorporation of records classification functionality within BS software will assist in the application of automated records management processes. While the BS software is unlikely to support the full definition of a classification scheme, it may contain relevant categories derived from the organisation’s records classification scheme (see Section 2.5).

114 These are taken from ISO 15489.1 Records Management, Section 7.2 Characteristics of records.
The following list of functional requirements is concerned with ensuring:

- **Metadata for records can be configured** – the business system can handle a range of metadata elements and support processes for their management.

- **Records can be reassigned or reclassified and if required, duplicated and extracted** – records may be classified for management and retrieval purposes. As circumstances change, there must be mechanisms in the business system that allow the reassignment or reclassification of these records.

  Organisations may wish to create a copy of the contents of an existing record in order to facilitate the creation of a new and separate record. They may also wish to create a copy of a record and remove or permanently mask some of the material. This is made when the full record cannot be released for access, but part of the record can. If required, the business system may support these processes.

- **Reports can be produced** on records and the management thereof.

- **Records can be effectively managed when they have been subject to encryption and digital signatures** – particular consideration needs to be given to the ongoing maintenance of records that have been subject to encryption or where digital signatures have been used.

  While encryption and digital signatures have a valuable role to play in ensuring the authenticity and integrity of records in transmission, they also present risks to the ongoing useability of the record, as decryption keys and public keys for digital signatures may expire while the record is still required. For this reason, storing records in encrypted form is not recommended. Metadata can record the encryption and decryption processes and attest to the successful decryption of records.

  If such security measures are used as a means of protecting the authenticity and integrity of records, key management must be considered.

The business system **must**, either alone or in conjunction with other systems:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>27</td>
<td>Prevent the destruction or deletion of electronic records and associated metadata at all times, except as specified in Section 3.4: Retaining and disposing of records as required</td>
</tr>
</tbody>
</table>

### 3.2.1 Metadata configuration

The business system **must**, either alone or in conjunction with other systems:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>28</td>
<td>Be able to draw together all elements of metadata to create a metadata profile for an electronic record or, where applicable an aggregation of electronic records.</td>
</tr>
<tr>
<td>29</td>
<td>Allow a business system administrator to define the source of data for each metadata element during system configuration.</td>
</tr>
<tr>
<td>30</td>
<td>Have the ability to use the contents of a metadata element to determine a functional process,(^{115}) where the element can be related to the functional behaviour of the BS.</td>
</tr>
</tbody>
</table>

\(^{115}\) This functionality may either be incorporated within the BS or provided through integration with an external system, such as an electronic records management system.
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>30.1</td>
<td>Where the BS closely links record metadata to the functionality it represents, the metadata should provide both descriptive information and active support for achieving that functionality automatically.</td>
</tr>
<tr>
<td>30.2</td>
<td>Where the BS supports links between disposition functions and other records management mechanisms supported by the BS, it must warn a business system administrator when control mechanisms linked to disposition classes are updated, and protect disposition classes from amendment until revisions are complete.</td>
</tr>
</tbody>
</table>
| 31 | Support mechanisms for validating the contents of metadata elements, such as:  
• format of the element contents;  
• range of values;  
• validation against a pre-defined list of values; and  
• valid classification scheme references (where supported). |
| 32 | Be able to manage a metadata profile over time – maintaining links to the record and adding process metadata about records management activities. |
|   | The business system should, either alone or in conjunction with other systems: |
| 33 | Be able to manage a metadata profile as a single entity. |
| 34 | Place no practical limitation on the number of metadata elements allowed for each record or component of a record within the system. |
| 35 | Allow specification of which metadata elements are to be manually entered and maintained, either through requirements specification or through configuration. |
| 36 | Support several formats or combinations of formats for metadata elements, including:  
• alphabetic;  
• alphanumeric. |

116 These records management mechanisms may be incorporated within the BS itself or provided through integration with specialised software applications or other BS, such as an electronic records management system.

117 The BS may have the ability to independently manage metadata profiles, regardless of whether the digital records are maintained within the BS or within an external digital object store. Where the BS is unable to independently manage a metadata profile over time, and the electronic records are maintained within the system, the BS must be able to either:

• export the metadata profile to an external system, such as an electronic records management system, capable of managing the profile appropriately and allowing it to be linked to the records contained within the original BS. In this case, it is also mandatory that the external BS supports the import of metadata from the original BS. The importing BS must be capable of managing the metadata profile in accordance with the requirements for adequate recordkeeping functionality set forth in this specification; or

• permit an interface with an external system, such as an electronic records management system, so that the external system can manage the metadata profile maintained within the original BS. The external BS must be capable of supporting the ongoing management of the metadata profile in accordance with the requirements for adequate recordkeeping functionality outlined in this specification.

Where the BS is unable to independently manage a metadata profile over time, as per Requirement 32, and the electronic records are maintained externally to the system, the BS must be able to export the metadata with the electronic records to a centralised digital object store, such as an electronic records management system, for ongoing management.

118 This requirement may not be relevant if the system has been specifically designed to meet the needs of the organisation, including metadata requirements.
The business system may:

Support validation of metadata using calls to another software application.

3.2.2 Record reassignment, reclassification, duplication and extraction

The business system should, either alone or in conjunction with other systems:

Support the movement of electronic records by providing mechanisms for the reassignment or reclassification of records within the system (including reassignment of records from one aggregation of records to another, where the aggregation of records is supported).

Support mechanisms to enable the duplication of electronic records. \(^{119}\)

- Where the BS is able to copy the contents of an existing electronic record in order to create a new and separate electronic record, it must ensure that the original record remains intact and unaltered. \(^{40.1}\)
- Where the BS supports the duplication of electronic records, it may provide a controlled copy facility or allow the BS to link to an external system capable of providing a controlled copy facility. \(^{40.2}\)
- The BS may facilitate the tracking of copies made of an identified electronic record, recording information on access to copies in the audit log. \(^{40.3}\)

The business system may, either alone or in conjunction with other systems:

Allow the creation of an extract from an electronic record, whereby sensitive information is removed or hidden from view in the extract, while the originating record remains intact.

- Where the BS supports extraction, it must note the creation of an extract in the metadata of the originating electronic record, including date, time, creator and reason for creation of the extract. \(^{41.1}\)
- Where the BS supports extraction, it must be able to copy metadata attributes from the originating electronic record to an extract – allowing selected elements to be amended as necessary. \(^{41.2}\)
- Where the BS supports extraction, it may create a navigable link between an extract and the electronic record from which it was taken. Such a link should preserve the relationship between the extract and the electronic record without compromising the access and security controls applicable to the record. \(^{41.3}\)

\(^{119}\) Duplicates may be made within the BS or created outside of the system. Where duplicates are created outside the BS, their existence may be noted in the record metadata profile of the original record.

\(^{120}\) The audit log may keep details of copies created outside the BS, as well as copies created within the BS.

\(^{121}\) Whether the extract itself needs to be maintained as a record depends on the analysis of business processes (see Section 2.1).

\(^{122}\) For example, an extract may have a different security category from the originating record.
Provide solutions for expunging sensitive information by producing redacted copies of records in all formats supported by the system, including audio and video.

### 3.2.3 Reporting on records

The business system must, either alone or in conjunction with other systems:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>43</td>
<td>Be able to report the actions carried out on electronic records, or where applicable aggregations of electronic records, either by the system itself or by an integrated or interfaced external records management mechanism, during a specified period of time.</td>
</tr>
</tbody>
</table>

The business system should, either alone or in conjunction with other systems:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>44</td>
<td>Be able to produce a report listing the details and outcome of any migration process to ensure the integrity of electronic records.</td>
</tr>
</tbody>
</table>

The business system may, either alone or in conjunction with other systems:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>45</td>
<td>Be able to produce statistical information about electronic records, or where applicable aggregations of electronic records, captured and maintained by the system, such as the number and location of electronic records by application type and version.</td>
</tr>
</tbody>
</table>

### 3.2.4 Online security processes

Online security processes include two subsections on encryption and digital signatures. The majority of these requirements are conditional on the business system having a business requirement to support any online security process.

The business system must, either alone or in conjunction with other systems:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>46</td>
<td>Automatically record the details of all online security processes (for example, in an audit trail).</td>
</tr>
<tr>
<td>47</td>
<td>Support date and time stamping for all records subject to online security processes.</td>
</tr>
</tbody>
</table>

**Encryption**

The business system may, either alone or in conjunction with other systems:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
</table>
| 48 | Support encryption of electronic records. Where the BS supports the encryption of electronic records, it must, either alone or in conjunction with other systems:

48.1 Support the capture of metadata for electronic records created or received in encrypted form in accordance with relevant standards, including:

- the serial number or unique identifier of a digital certificate;
- type of algorithm and level of encryption; and
- date and time stamps relating to encryption and/or decryption processes.

48.2 Ensure that an encrypted record can only be accessed by those users associated with the relevant cryptographic key, in addition to other access controls allocated to the record. |

---

123 As migration may be an infrequent occurrence, the reporting may involve manual intervention.

124 If this requirement is meant through integration with an external system.
Where the BS supports the capture, identification and/or transmission of encrypted electronic records and associated metadata, it must support the implementation of a key management plan.125

Where the BS supports the capture, identification and/or transmission of encrypted electronic records and associated metadata, it must be able to maintain cryptographic keys for the life of the electronic record, or records, with which they are associated.

Where the BS supports the capture, identification and/or transmission of encrypted electronic records and associated metadata, it must support the separate, secure storage of encrypted records and their associated decryption keys.

Where the BS supports the encryption of electronic records, it should, either alone or in conjunction with other systems:

- Be able to store encrypted electronic records in unencrypted form.
- Allow encryption to be removed when a record is captured or identified, unless the encryption is required to maintain the security of the record while within the BS.126

Digital signatures

These requirements only apply if the system is sending or received signed records. The requirements do not apply if the system is only using digital signatures to establish a secure channel. This document does not cover requirements specific to systems that manage digital signatures.

The business system should:

Where the BS is able to store digital certificates for encrypted records and digitally signed records, it should warn a business system administrator of any certificates approaching expiry.

The business system may, either alone or in conjunction with other systems:

Be capable of ensuring that any electronic records created or received by the BS that employ the use of digital signature technology can be captured and identified by the system along with associated authentication metadata.127

Where the BS supports the use of digital signatures, it must, either alone or in conjunction with other systems:

- Support the use of metadata for electronic records transmitted or captured bearing digital signatures, in accordance with relevant metadata standards. At a minimum this metadata must note the fact that a digital signature was authenticated.

125 Either by incorporating the key management plan within the BS or by integrating the system with an external BS or specialised software application capable of supporting a key management plan.

126 Some BS may have legitimate requirements to capture and store digital records in encrypted format for evidential or security purposes. Where the BS itself provides adequate access and security controls, it should be possible to store both the unencrypted and encrypted digital records along with the necessary encryption keys within the BS, noting Requirement 48.6.

127 This requirement is primarily of concern for BS that routinely send or receive digital records using digital signature technology.
50.2 Be able to check the validity of a digital signature at the time of capturing an electronic record.

50.3 Be able to store with the electronic record:
   • the digital signature associated with that record;
   • the digital certificate authenticating the signature;
   • any other confirmation details;
   in such a way that they can be retrieved with the record, but without compromising the integrity of a private key.

50.4 Allow a business system administrator to configure the extent to which authentication metadata is routinely stored with the electronic record. For example:
   • retain the fact of successful authentication only;
   • retain metadata about the authentication process; and
   • retain all authentication metadata, including signatures.

50.5 Be able to demonstrate the continued integrity of a digitally signed record, whether or not authorised changes have been made to the metadata of the record.\(^\text{128}\)

Where the BS supports the use of digital signatures, it should, either alone or in conjunction with other systems:

50.6 Be able to support incorporation of, or interfacing with, digital signature technologies so that authentication metadata can be automatically captured by the system.

Where the BS supports the use of digital signatures, it may, either alone or in conjunction with other systems:

50.7 Be able to apply a digital signature to:
   • an electronic record; or
   • an aggregation of electronic records;
   during a transmission or export process in a manner that supports external authentication.\(^\text{129}\)

**Authentication**

The business system may, either alone or in conjunction with other systems:

<table>
<thead>
<tr>
<th>51</th>
<th>Be able to support authentication through interface with PKI-based security technologies.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Where the BS supports authentication interface with PKI-based security technologies, it must:</td>
</tr>
<tr>
<td>51.1</td>
<td>Be able to store metadata about the process of authentication, including:</td>
</tr>
<tr>
<td></td>
<td>• the serial number or unique identifier of the digital certificate;</td>
</tr>
<tr>
<td></td>
<td>• the registration and certification authority responsible for authentication; and</td>
</tr>
<tr>
<td></td>
<td>• the date and time of authentication.</td>
</tr>
</tbody>
</table>

\(^{128}\) Changes may be made to the metadata, but not to the content of the record.

\(^{129}\) This requirement will only apply to BS with in-built digital signature capabilities that are required to create and transmit digitally signed records in support of their primary business functions.
51.2 Where the BS supports authentication, it must allow authentication metadata to be stored either:
• with the electronic record to which it relates; or
• separately but closely linked to the electronic record.

52 Provide a flexible architecture in order to accommodate new online security technologies as they are released.

### 3.3 Supporting import, export and interoperability

The ability to import and export records from the business systems, and interoperability with other systems, are frequently required functionality. Records may need to be exported to a different system such as an electronic records management system, or exported to other organisations in the event of mergers or, in the government sector, machinery of government changes.

Many records may need to be retained for longer than the lifespan of the software system itself, and therefore there is a need to be able to export records when transitioning to a new business system. There may also be a need to import records from other business systems, particularly in collaborative business environments. Transfer of records to an archival institution or to a secondary storage system should also be considered.

For ease of import and export, use of open formats and industry standards will increase levels of interoperability and reduce the cost and difficulty of any import/export process.

While the need for this functionality may be most evident when decommissioning a system, it is important to consider it at the design stage.

Useful resources include the Centre for European Normalization’s Record Exchange Standard business Requirement Specification and the Australasian Digital Recordkeeping Initiative’s Digital Records Export Standard.

### 3.3.1 Import

The business system should, either alone or in conjunction with other systems:

53 Be able to import any audit trail information that may be directly associated with electronic records, and where applicable aggregations of electronic records, captured and maintained by the system and guarantee the integrity of the imported information.

The business system may, either alone or in conjunction with other systems:

54 Be able to undertake a bulk import of electronic records exported from records-generating systems, capturing:
• electronic records in their existing format, maintaining their content and structure;
• electronic records and their associated metadata, so as to maintain the relationships between them and map the metadata to the receiving structure; and
• the system structure to which the records and associated metadata, and where

---


131 These may include records exported from an electronic document management system or an electronic records management system.
applicable aggregations of records, are assigned, maintaining all relationships between them.

54.1 Where the BS supports the bulk import of electronic records, it may allow the use of mechanisms to support the import process, including:
- pre-defined batch file transaction imports;
- edit rules to customise automatic identification of records;
- data integrity validation processes; and
- input queues, including multiple queues for different document types.

55 Be able to perform an indirect import of electronic records with no associated metadata, or metadata that is presented in a non-standard format, mapping this to the receiving structures.

### 3.3.2 Export

The business system **must**, either alone or in conjunction with other systems:

<table>
<thead>
<tr>
<th>Section</th>
<th>Requirement</th>
</tr>
</thead>
</table>
| 56 | Be able to export electronic records and associated metadata, and where applicable aggregations of electronic records, to:  
- another system within the organisation;  
- a system in a different organisation; or  
- an archival institution or program for the long-term preservation of electronic records appraised as having archival value. |
| 57 | Ensure that any export action is able to include:  
- all electronic records, and where applicable aggregations of electronic records;  
- all metadata associated with exported electronic records and, where applicable aggregations of electronic records; and  
- all audit trail data associated with exported electronic records. |
| 58 | Be able to export electronic records, and where applicable aggregations of electronic records, in one sequence of operations such that:  
- the content and structure of electronic records, and where applicable aggregations of electronic records, are not degraded;  
- associations are retained between exported electronic records and their associated metadata; and  
- relationships are maintained between exported components of an electronic record, between exported electronic records, and where applicable aggregations of electronic records, so that their structural links can be re-built in the receiving system. |
| 59 | Be able to export all the types of records it can capture, regardless of format or the presence of the generating application. |
| 60 | Allow objects to be exported more than once. |

The business system **should**, either alone or in conjunction with other systems:

<table>
<thead>
<tr>
<th>Section</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>61</td>
<td>Ensure that any export action is documented in metadata associated with the record.</td>
</tr>
</tbody>
</table>

The business system **may**, either alone or in conjunction with other systems:

<table>
<thead>
<tr>
<th>Section</th>
<th>Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>62</td>
<td>Be able to export electronic records that have been converted into open, fully documented file formats.</td>
</tr>
</tbody>
</table>

---

132 While a business decision may be made to delete information in the system after export, the purpose of this requirement is to ensure that the system itself does not limit the export process.
3.4 Retaining and disposing of records as required

The following list of functional requirements is concerned with ensuring:

- **Compliance with disposition authorisation regimes** – part of the process of assessing records management involves determining how long the records should be kept to account for legal obligations, business needs and community expectations. A disposition schedule sets out the retention periods for various groups of records. These retention decisions, documented in the disposition schedule, should be authorised at a senior level in accordance with jurisdictional requirements. These functional requirements assume the existence of a disposition schedule that covers the records in the business system.

- **disposition is effectively applied** – provision must be made for facilitating retention and disposition either in the system, or through the integration with external software components. Keeping everything for the entire lifespan of the system can be expensive and impair the operations of the system.

  There may be some circumstances where a cost-benefit analysis and risk analysis conclude that it is preferable to retain records for the lifespan of the system. However, this simply postpones decision-making about the appropriate retention of records until the time of decommissioning.\(^{133}\)

- **Records ready for disposition can be reviewed** – prior to taking any disposition action, users must be able to review the disposition action and be able to amend it/apply a different action.

- **Records are appropriately destroyed** – it should not be possible for records to be deleted except in accordance with an authorised disposition schedule, and then only after agreed sign-off by authorised staff.

- **Metadata of the destroyed records is retained** – evidence of the implementation of disposition actions must also be maintained, either through metadata within the business system or through integration with another system.

- **Reporting can be undertaken** on the disposition activity.

It is noted that some disposition requirements are related to the use of aggregations. As these requirements are conditional on the use of aggregations, they are in Section 3.1.3.

### 3.4.1 Compliance with disposition authorisation regimes

The business system must, either alone or in conjunction with other systems:

---

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>63</td>
<td>Support the controlled disposition of records legally authorised for disposition.</td>
</tr>
<tr>
<td>64</td>
<td>Allow the definition of disposition classes, which can be applied to electronic records and associated metadata and, where applicable aggregations of electronic records, either through the internal functionality of the BS software or via an automatic or manual external mechanism (noting Requirement 77).</td>
</tr>
</tbody>
</table>
| 65 | Ensure that the definition of each disposition class consists of:  
• a disposition trigger to initiate the retention period;  
• a retention period to establish how long the record must be maintained; and  
• a disposition action, to prescribe the fate of the record. |
| 66 | Support the definition and application of the following disposition actions:  
• review;  
• export;  
• transfer; and  
• destruction. |
| 67 | Enable flexibility in the definition of disposition classes to allow the business system administrator to assign non-standard retention periods and disposition actions. |
| 68 | Allow a unique identifier to be assigned to each disposition class and, where applicable, allow the disposition class to be associated with the appropriate disposition authority. |
| 69 | Allow retention periods to be defined from one day to an indefinite length of time. |
| 70 | Restrict the ability to create, edit and delete disposition classes and disposition authorities to the business system administrator or other authorised user. |
| 71 | Be able to maintain a history of all changes to disposition classes, including date of change and reason for change. |
| 72 | Ensure that amendments to a disposition class take immediate effect on all records and associated metadata, and where applicable aggregations of electronic records, to which that class has been applied. |

**The business system should**, either alone or in conjunction with other systems:  

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>73</td>
<td>Be able to import and export a set of disposition classes in a standard format.</td>
</tr>
</tbody>
</table>

---

134 A BS must support a minimum of one disposition class for each classification of records it manages. These disposition classes must be defined so that they can be mapped to the appropriate records and applied.

135 Some BS will be capable of providing in-built functionality to support the definition and application of disposition classes applicable to the records created or received by the system.

136 An automatic external mechanism may comprise an external BS with adequate recordkeeping functionality, such as an electronic records management system, or an external software application designed specifically to support disposition functionality. The automatic external mechanism will integrate or interface with the BS to support the definition and application of disposition classes.

137 Where a BS does not support an automated disposition mechanism, it may still adequately address this requirement by providing a workable manual mechanism for supporting the definition of disposition classes. This will require manually mapping disposition classes from a disposition authority to the relevant digital records created or received by the BS.

138 Transfer consists of confirmed export followed by destruction, once the success of the transfer process has been confirmed.

139 For example, ‘destroy when superseded’, ‘disposal not authorised’.
Be able to manage a many-to-one relationship where multiple disposition classes may be linked to a single electronic record, or where applicable an aggregation of electronic records.

74.1 If the BS is unable to support a many-to-one relationship for disposition classes, it must as a minimum support the ability to allocate a one-to-one relationship for linking a disposition class to an electronic record, or where applicable an aggregation of electronic records, and must permit the business system administrator, or other authorised user, to manually determine and map the appropriate disposition class with the highest applicable retention period.  

The business system **may**, either alone or in conjunction with other systems:

<table>
<thead>
<tr>
<th>Table Cell</th>
<th></th>
</tr>
</thead>
</table>
| 75 | Support the definition of disposition classes from multiple disposition authorities.  

<table>
<thead>
<tr>
<th>Table Cell</th>
<th></th>
</tr>
</thead>
</table>
| 76 | Allow one or more disposition authorities to be merged during an import process.  

### 3.4.2 disposition application

The business system **must**, either alone or in conjunction with other systems:

<table>
<thead>
<tr>
<th>Table Cell</th>
<th></th>
</tr>
</thead>
</table>
| 77 | Allow disposition classes to be systematically applied to electronic records and associated metadata, and where applicable aggregations of electronic records. The means employed by the BS to apply disposition classes and related disposition processes may include:

  * the incorporation of disposition functionality within the BS software;
  * the integration of external software applications with the BS so as to enable the application of disposition functionality;
  * manual mapping and application of disposition authorisation to the records of the BS by the business system administrator or other authorised user;  

140 That is, import an authorised set of disposition classes into the BS, or where applicable the relevant external disposition management mechanism, so as to remove the need for the business system administrator to manually configure disposition classes.

141 The ability to export a set of authorised disposition classes from the BS, or where applicable, the relevant external disposition management mechanism, so that they may be transferred to another system, such as an electronic records management system.

142 A structured set of disposition classes issued by an archival authority may be known as a disposition authority or disposition/retention schedule.

143 Manual mapping of disposition classes may be quite time consuming where large numbers of disposition classes need to be mapped to digital records held within the BS.

144 To support organisations that may have more than one current approved disposition authority.

145 The level of sophistication of the disposition functionality incorporated within the BS will vary depending on the nature and complexity of the system.

146 This may include the use of specialised disposition management software or integration with an external BS with adequate recordkeeping functionality, such as an electronic records management system. Records may either be exported to the external mechanism where they may be captured and appropriate disposition management controls applied, or alternatively, the external mechanism may interface with the BS so as to apply appropriate disposition management controls to the records retained within the BS itself.

147 Where a BS is not capable of supporting adequate automated disposition processes it may be necessary to manually map disposition authorisation to the records controlled by the system and
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>77.1</td>
<td>Where the BS supports the use of pre-defined system rules, it must enable the manual update or retrospective inheritance of disposition classes when a new disposition class is applied following a change to the pre-defined system rules.</td>
</tr>
<tr>
<td>78</td>
<td>Allow disposition classes to be applied to any and all electronic records and associated metadata, or where applicable aggregations of electronic records, captured by the system.</td>
</tr>
<tr>
<td>79</td>
<td>Record all disposition actions in a metadata profile.</td>
</tr>
<tr>
<td>80</td>
<td>Automatically track the initiation and progress of retention periods, in order to determine disposition dates for electronic records and associated metadata, or where applicable aggregations of electronic records.</td>
</tr>
<tr>
<td>81</td>
<td>Allow a business system administrator or other authorised user to apply a different disposition class to an electronic record at any time.</td>
</tr>
<tr>
<td>82</td>
<td>Restrict the ability to apply and reapply disposition classes to the business system administrator or other authorised user.</td>
</tr>
</tbody>
</table>
| 83 | Support a disposition process consisting of:  
  - identification of electronic records and associated metadata, and where applicable aggregations of electronic records, for which the retention period has elapsed;  
  - notification of a business system administrator or other authorised user;  
  - reapplication of a disposition class if required;  
  - execution of the relevant disposition actions after confirmation by a business system administrator or other authorised user;  
  which may be applied automatically or manually as determined by the disposition mechanism employed by the BS, as noted in Requirement 77. |
| 84 | Restrict the operation of the disposition process to a business system administrator or other authorised user. |
| 85 | Support a range of disposition triggers based on active metadata. For example:  
  - date of record creation;  
  - date of last retrieval of a record;  
  - opening or closing date of an aggregation of records (where applicable);  
  - date of last review of a record, or where applicable an aggregation of records. |
| 86 | Support external disposition triggers based on notification of a defined event either manually entered into the system by a user or automatically acquired via an external BS integrated with the disposition mechanism. |
| 87 | Ensure that a retention period is calculated in real time and cannot be artificially advanced. |
| 88 | Allow a disposition freeze to be placed on an electronic record and associated metadata, or where applicable an aggregation of records, in order to prevent any disposition action from taking place for the duration of the freeze. |

Automated solutions to the application of disposition classes may not be flexible enough to meet all situations, making it necessary to manually implement disposition in the case of some non-standard disposition actions.

Reapplication of a disposition class must take immediate effect within the disposition process.

The metadata may either be generated by the BS as a result of internal system functionality, or may be supplied by one or more external records management mechanisms integrated with the BS, such as an electronic records management system.

148 | manully apply disposition actions to the records, or where applicable aggregations of records, as required. |
149 | Reapplication of a disposition class must take immediate effect within the disposition process. |
150 | The metadata may either be generated by the BS as a result of internal system functionality, or may be supplied by one or more external records management mechanisms integrated with the BS, such as an electronic records management system. |
Prevent the deletion or destruction of any electronic record subject to a disposition freeze.\(^{152}\)

Restrict the ability to remove a disposition freeze to a business system administrator or other authorised user.

Be able to identify any conflict of disposition actions and either:
  - automatically apply the correct disposition action according to precedence defined by the organisation;\(^{150}\) or
  - notify the business system administrator or other authorised user and request remedial action.

The business system should, either alone or in conjunction with other systems:

- Be capable of sentencing on creation\(^{154}\) by automatically applying a disposition class to a newly created or received electronic record and associated metadata, or where applicable an aggregation of electronic records, based on a set of pre-defined instructions.\(^ {155}\)
- Be able to notify the business system administrator on a regular basis of all disposition actions due to occur in a specified period of time.

The business system may, either alone or in conjunction with other systems:

- Support automatic sentencing of an electronic record and associated metadata, or where applicable an aggregation of electronic records, based on its contents, specified metadata elements, or a combination of both.\(^ {156}\)
  - Where the disposition is automatic, the BS must automatically seek confirmation from a business system administrator or other authorised user before implementing any disposition action.
- Support an interface with a workflow engine to facilitate the disposition process.

3.4.3 Review

The business system must, either alone or in conjunction with other systems:

\(^{151}\) A disposition freeze may, for example, be placed on records identified as being subject to a pending or ongoing Freedom of Information application or legal discovery process. To meet this requirement the system need not provide specialised disposition freeze functionality. It is sufficient for the BS to simply allow a business system administrator or other authorised user to manually identify affected digital records and implement controls to prevent their disposition until the disposition freeze is no longer in place.

\(^{152}\) Under other circumstances, deletion or destruction may be carried out by a business system administrator or authorised user. See Requirement 86.

\(^{153}\) Usually the longer period is applied.

\(^{154}\) The identification of the retention period of a record at the time the record is created.

\(^{155}\) These instructions may be applied through metadata inherited from higher entities within a records classification scheme, where supported (as per Requirement 23), or alternatively may be established through pre-defined system rules specifically designed to allocate disposition metadata (as per Requirements 25 and 26).

\(^{156}\) It may be possible to establish pre-defined system rules for the automatic assignment of disposition classes based on the characteristics of the records created or received by the BS. Simplistic BS may contain relatively few record classes that can be easily identified and grouped through similar characteristics, enabling the automatic assignment of appropriate disposition authorisation at the time of capture.
Provide a means by which the content of an electronic record, or where applicable an aggregation of electronic records, identified for disposition can be reviewed prior to the application of a disposition action.

Make the entire contents of an electronic record, or where applicable aggregation of electronic records, under review available to the reviewer, subject to applicable access restrictions.

Allow the business system administrator to reapply a disposition class that could:
• mark electronic records, and where applicable aggregations of electronic records, for further retention and later review;
• mark electronic records, and where applicable aggregations of electronic records, for immediate export, transfer, preservation treatment (through a technique such as migration) or destruction;
• mark electronic records, and where applicable aggregations of electronic records, for further retention and later export, transfer, preservation treatment (through a technique such as migration) or destruction;
when a review disposition action is triggered.

The business system should, either alone or in conjunction with other systems:

Make the disposition class details applicable to the electronic record, or where applicable aggregation of electronic records, being reviewed available to the reviewer either by searching or navigation.

Automatically record the date of last review as active metadata, and allow the reviewer to add the reasons for the review decision as descriptive metadata.

3.4.4 Destruction

The business system must, either alone or in conjunction with other systems:

Ensure that destruction results in the complete obliteration or inaccessibility of all electronic records (including all components of each record) as authorised, and that they cannot be restored through operating system features or specialist data recovery techniques.\(^\text{157}\)

Seek confirmation of destruction from a business system administrator or other authorised user as part of the disposition process.

Prevent the destruction of electronic records, or where applicable aggregations of records, until confirmation is received, and allow the process to be cancelled if confirmation is not received.

Distinguish between an ad hoc delete function and the destruction function within the disposition process, so that each can be allocated individually to authorised users.

Prevent the delete function being used within the disposition process, so that immediate destruction of identified electronic records can only be achieved through the allocation of a disposition class.

The business system should, either alone or in conjunction with other systems:

Have the ability to ensure that when an electronic record is authorised for destruction, all

\(^{157}\) While this document does not cover the management of back-ups for business continuity and disaster recovery purposes, it is noted that good practice should ensure that back-ups are not retained for longer than needed for business continuity purposes.
alternative renditions of that record are also destroyed.

106.1 Where the BS supports the destruction of alternative renditions, it should allow a business system administrator to turn off the functionality outlined in Requirement 105 if required.¹⁵⁸

3.4.5 disposition metadata

The business system must, either alone or in conjunction with other systems:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>107</td>
<td>Support the progressive addition of metadata to electronic records, and where applicable aggregations of electronic records, to support disposition as set out in relevant metadata standards.</td>
</tr>
<tr>
<td>108</td>
<td>Actively link disposition metadata to the functionality it represents, so that it can be used to trigger automated processes.¹⁵⁹</td>
</tr>
<tr>
<td>109</td>
<td>Be able to detect any metadata changes that affect the retention period of an electronic record, and calculate a new disposition date according to the disposition class.¹⁶⁰</td>
</tr>
<tr>
<td>110</td>
<td>Be able to restrict the amendment of metadata that affects the retention period of an electronic record to a business system administrator or other authorised user.</td>
</tr>
<tr>
<td>111</td>
<td>Be able to retain metadata for electronic records, and where applicable aggregations of electronic records, that have been transferred or destroyed.</td>
</tr>
<tr>
<td>112</td>
<td>Be able to record the date and details of all disposition actions within the metadata profile of the electronic record, or where applicable the aggregation of electronic records.</td>
</tr>
</tbody>
</table>

The business system should, either alone or in conjunction with other systems:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>113</td>
<td>Allow users to add any metadata elements required for the archival management of electronic records selected for archival transfer.</td>
</tr>
<tr>
<td>114</td>
<td>Be able to maintain a history of the disposition classes that have been applied to a particular electronic record, in the metadata of that electronic record.</td>
</tr>
<tr>
<td>115</td>
<td>Allow a business system administrator to specify a subset of metadata¹⁶¹ to be retained for electronic records, and where applicable aggregations of electronic records, that have been transferred, destroyed or moved offline.</td>
</tr>
</tbody>
</table>

The business system may, either alone or in conjunction with other systems:

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>116</td>
<td>Be able to export metadata as specified by relevant metadata standards.</td>
</tr>
<tr>
<td>117</td>
<td>Support free-text fields for user-definable notes.¹⁶²</td>
</tr>
<tr>
<td>118</td>
<td>Support the entry of management metadata for disposition classes and disposition authorities, including: * a scheduled review date;</td>
</tr>
</tbody>
</table>

¹⁵⁸ For example, if a disposition authority does not cover all renditions, or if an organisation has reason to keep a particular rendition.

¹⁵⁹ This functionality may either be incorporated within the BS or provided through integration with an external mechanism, such as an electronic records management system.

¹⁶⁰ Where this functionality cannot be automatically applied by the BS, either through internal or external mechanisms, the system must at least enable the manual detection and updating of changes to disposition classes.

¹⁶¹ Ideally the mandatory metadata elements, as set out in relevant metadata standards.

¹⁶² For example, to link a disposition decision to retention requirements found in legislation.
<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>119</strong></td>
<td>Allow a business system administrator to archive the metadata retained for electronic records, and where applicable aggregations of electronic records, that have been transferred or destroyed.</td>
</tr>
</tbody>
</table>

### 3.4.6 Reporting on disposition activity

The business system **must**, either alone or in conjunction with other systems:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>120</strong></td>
<td>Be able to produce reports on all disposition activity undertaken by the system, including disposition activity undertaken by external disposition mechanisms integrated or interfaced with the system.</td>
</tr>
</tbody>
</table>
| **121** | Be able to produce reports listing:  
  - all disposition classes currently defined in the system;  
  - all electronic records and associated metadata, and where applicable aggregations of records, to which a particular disposition class is currently applied;  
  - all electronic records for which a particular disposition action will occur over a given period of time;  
  - all electronic records due for disposition within a given period of time (providing quantitative information on the volume and type of records); and  
  - all electronic records that are overdue for disposition at a given point in time (providing quantitative information on the volume and type of records). |
| **122** | Be able to produce a report detailing any failure during an export of electronic records from the system, identifying those electronic records which have generated processing errors or were not successfully exported. |
| **123** | Be able to produce a report detailing the outcome of a destruction process, detailing all electronic records successfully destroyed and identifying those electronic records which were not successfully destroyed. |

The business system **should**, either alone or in conjunction with other systems:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>124</strong></td>
<td>Be able to report on all electronic records subject to a disposition freeze.</td>
</tr>
</tbody>
</table>

The business system **may**, either alone or in conjunction with other systems:

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>125</strong></td>
<td>Be able to report on review decisions over a given period of time.</td>
</tr>
</tbody>
</table>

---

163 That is, take a copy that is outside the control of the BS.

164 Conditions for the successful destruction of digital records are outlined in Requirement 101. Destruction of a digital record is deemed to have been unsuccessful if it can still be restored, either in part or in total, after the application of the destruction process outlined in Requirement 101.

165 A disposition freeze may, for example, include digital records subject to a pending or ongoing Freedom of Information or legal discovery process.
## 4 APPENDICES

### A Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access controls</td>
<td>A scheme of non-hierarchical mechanisms, which may be applied to electronic records to prevent access by unauthorised users. May include the definition of user access groups and ad hoc lists of individual named users. See also Security controls, System access controls and User access group. Source: Adapted from The National Archives (UK), Requirements for Electronic Records Management Systems, 3: Reference Document, 2002, p. 28.</td>
</tr>
<tr>
<td>Aggregation</td>
<td>Any accumulation of record entities at a level above record object (document, digital object), for example, digital folder, series. See also Folder and Record category.</td>
</tr>
<tr>
<td>Audit trail</td>
<td>Data that allows the reconstruction of a previous activity, or which enables attributes of a change (such as date, time, operator) to be stored so that a sequence of events can be determined in the correct chronological order. Usually in the form of a database or one or more lists of activity data. Source: Adapted from The National Archives (UK), Requirements for Electronic Records Management Systems, 3: Reference Document, 2002, p. 1.</td>
</tr>
<tr>
<td>business system</td>
<td>For the purpose of this document, an automated system that creates or manages data about an organisation’s activities. Includes applications whose primary purpose is to facilitate transactions between an organisational unit and its customers – for example, an e-commerce system, client relationship management system, purpose-built or customised database, finance or human resources systems. business systems are typified by containing dynamic data that is commonly subject to constant updates (timely), able to be transformed (manipulable) and holds current data (non-redundant). In contrast, electronic records management systems contain data that is not dynamically linked to business activities (time-bound), unable to be altered (inviolable), and that may be non-current (redundant). See also Electronic records management system (ERMS).</td>
</tr>
<tr>
<td>business system administrator</td>
<td>A user role with designated responsibility for the operation of the system, including configuring, monitoring and managing the business system and its use. May exist at various degrees of seniority with a variety of permissions to undertake system administration functions and some records management processes.</td>
</tr>
<tr>
<td>Capture</td>
<td>The process of lodging a document or digital object into a records management system and assigning metadata to describe the record and place it in context, thus allowing the appropriate management of the record over time. For certain business activities this functionality may be built into business systems so that the capture of records and associated metadata is concurrent with the creation of records. See also Registration. Sources: National Archives of Australia, Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records, exposure draft, 2004.</td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Classification                | 1. The systematic identification and arrangement of business activities and/or records into categories according to logically structured conventions, methods and procedural rules represented in a classification system.  
2. Classification includes determining document or file naming conventions, user permissions and security restrictions on records.  
See also **Records classification scheme**.  
Sources: Adapted from ISO 15489, Part 1, Clause 3.5; AS 4390, Part 1, Clause 4.8. |                                                                                               |
| Component                     | Constituent parts that comprise an electronic record (such as the multimedia components of a web page). It is necessary to capture metadata about components to enable a record to be managed over time, for example, for migration purposes. This is not to be confused with the concept of a ‘software’ or ‘system’ component. See also **Digital object, Data element** and **Electronic record**.  
| Compound record               | A record that comprises multiple individual components. For example, web pages with embedded graphics and style sheets.                                                                                     |                                                                                               |
| Control                       | The physical and/or intellectual management established over records by documenting information about their physical and logical state, their content, their provenance and their relationships with other records. The systems and processes associated with establishing control include registration, classification, indexing and tracking. See also **Classification** and **Registration**.  
Source: Adapted from ISO 15489, Part 1, Clause 3.7 and Part 2, Clause 4.3.9.2. |                                                                                               |
| Conversion                    | The process of changing records from one medium to another or from one format to another. Conversion involves a change of the format of the record but ensures that the record retains the identical primary information (content).  
See also **Migration** and **Rendition**.  
Source: Adapted from ISO 15489, Part 1, Clause 3.7 and Part 2, Clause 4.3.9.2. |                                                                                               |
| Cryptographic key             | Data elements used for the encryption or decryption of electronic messages. They consist of a sequence of symbols that control the operation of a cryptographic transformation, such as encipherment.  
See also **Encryption** and **Public Key Infrastructure (PKI)**.  
| Data                          | Facts or instructions represented in a formalised manner, suitable for transmission, interpretation or processing manually or automatically.  
| Data element                  | A logical, identifiable unit of data that forms the basic organisational component in a database. Usually a combination of characters or bytes referring to one separate piece of information. A data element may combine with one or more other data elements or digital objects to form an electronic record. |                                                                                               |
| **Database** | An organised collection of related data. Databases are usually structured and indexed to improve user access and retrieval of information. Databases may exist in physical or digital format. See also Data, Data element, Field, Table and Relational database. |
| **Deletion** | The process of removing, erasing or obliterating recorded information from a medium outside the disposition process. Deletion within electronic systems generally refers to the removal of the pointer (for example, location information) that allows the system to identify where a particular piece of data is stored on the medium. See also Destruction and disposition. |
| **Descriptor** | A non-hierarchical qualifier (for example, 'Personnel') attached to a security category to limit access to particular records. Descriptors may be informative or advisory but cannot actively control access. Source: Adapted from The National Archives (UK), Requirements for Electronic Records Management Systems, 3: Reference Document, 2002, pp. 27–8. |
| **Destruction** | 1 The process of eliminating or deleting records beyond any possible reconstruction. 2 In this document, destruction refers to a disposition process, whereby electronic records, record plan entities and their metadata are permanently removed, erased or obliterated as authorised and approved by a disposition authority schedule. See also Deletion. Source: Adapted from ISO 15489, Part 1, Clause 3.8. |
| **Digital certificate** | An electronic document signed by the certification authority which identifies a key holder and the business entity they represent; binds the key holder to a key pair by specifying the public key of that key pair; and should contain any other information required by the certificate profile. Source: National Archives of Australia, Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption, 2004. |
| **Digital folder** | A set of related electronic records held in a tightly bound relationship within the business system and managed as a single object. A type of aggregation of electronic records. May also be referred to as a container. See also Aggregation and Folder. |
| **Digital object** | An object that can be represented by a computer, such as a file type generated by a particular system or software application (for example, a word-processed document, a spreadsheet, an image). An electronic record may comprise one or more digital objects. See also Component and Electronic record. |
| **Digital signature** | A security mechanism included within an electronic record that enables the identification of the creator of the digital object and that can also be used to detect and track any changes that have been made to the digital object. Sources: National Archives of Australia, Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records, exposure draft, 2004. Adapted from Australian Government Information Management Office, Trusting the Internet: A Small business Guide to E-security, 2002, p. 43. |
| **DIRKS** | The acronym for ‘designing and implementing recordkeeping systems’, a methodology for managing records and other business information that is outlined in the International Standard on Records Management (ISO 15489, Part I, Section 8.4) and elaborated in the 2001 National Archives’ publication, DIRKS: A Strategic Approach to Managing business Information. |
| **disposition** | A range of processes associated with implementing retention, destruction or |
transfer decisions that are documented in disposition or other instruments. Source: ISO 15489, Part 1, Clause 3.9.

<table>
<thead>
<tr>
<th>disposition action</th>
<th>The action noted in a disposition authority indicating the minimum retention period for a record and the event from which the disposition date should be calculated. See also disposition trigger and Retention period.</th>
</tr>
</thead>
<tbody>
<tr>
<td>disposition authority</td>
<td>A formal instrument that defines the retention periods and consequent disposition actions authorised for classes of records described in the authority. See also disposition action, disposition class and Retention period.</td>
</tr>
<tr>
<td>disposition class</td>
<td>A description of the characteristics of a group of records documenting similar activities, together with a disposition action to be applied to the group. The description consists of function and activity terms, and scope notes, record description and disposition action. A component of a disposition authority, implemented within a business system as a set of rules made up of a disposition trigger, a retention period and a disposition action, which may be applied to a record plan entity.</td>
</tr>
<tr>
<td>disposition trigger</td>
<td>The point from which the disposition action is calculated. This can be a date on which action is completed or a date on which an event occurs. See also Retention period.</td>
</tr>
<tr>
<td>Electronic document and records management system (EDRMS)</td>
<td>An electronic records management system capable of providing document management functionality.</td>
</tr>
<tr>
<td>Electronic messaging systems</td>
<td>Applications used by organisations or individuals for sending and receiving, as well as storing and retrieving, electronic messages. These systems generally do not possess records management functionality. Source: National Archives of Australia, Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records, exposure draft, 2004.</td>
</tr>
<tr>
<td>Electronic record</td>
<td>Records on electronic storage media, produced, communicated, maintained and/or accessed by means of electronic equipment.</td>
</tr>
<tr>
<td>Electronic records management system (ERMS)</td>
<td>An automated system used to manage the creation, use, maintenance and disposition of electronically created records for the purposes of providing evidence of business activities. These systems maintain appropriate contextual information (metadata) and links between records to support their value as evidence. The primary purpose of an electronic records management system is the capture and management of electronic records. See also Electronic document and records management system (EDRMS). Source: National Archives of Australia, Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records, exposure draft, 2004.</td>
</tr>
</tbody>
</table>
| Encryption | The process of converting data into a secure code through the use of an encryption algorithm for transmission over a public network. The mathematical key to the encryption algorithm is encoded and transmitted with the data, thus providing the means by which the data can be decrypted at the receiving end and the original data restored. Sources: National Archives of Australia, Digital Recordkeeping: Guidelines for
<table>
<thead>
<tr>
<th><strong>ERMS</strong></th>
<th>See Electronic records management system.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Evidence</strong></td>
<td>Proof of a business transaction.</td>
</tr>
<tr>
<td><strong>Export</strong></td>
<td>A disposition process whereby copies of an electronic record (or group of records) are passed with their metadata from one system to another system, either within the organisation or elsewhere. Export does not involve removing records from the first system. See also Transfer. Source: Adapted from The National Archives (UK), Requirements for Electronic Records Management Systems, 3: Reference Document, 2002, p. 3.</td>
</tr>
<tr>
<td><strong>Extract</strong></td>
<td>A copy of an electronic record from which some material has been removed or permanently masked. An extract is made when the full record cannot be released for access, but part of the record can. Source: Adapted from The National Archives (UK), Requirements for Electronic Records Management Systems, 3: Reference Document, 2002, p. 3.</td>
</tr>
<tr>
<td><strong>Field</strong></td>
<td>A set of one or more related data elements that represent a category of information within a database. See also Data element, Database and Table.</td>
</tr>
</tbody>
</table>
| **File** | 1 (noun) An organised unit of documents accumulated during current use and kept together because they deal with the same subject, activity or transaction.  
2 (verb) The action of placing documents in a predetermined location according to a scheme of control. See also Folder. Note: For the purposes of this document, the records management definition of this term will apply. This differs from the IT definition, which identifies a file as a named collection of information stored on a computer and treated as a single unit. Source: Adapted from J Ellis (ed.), Keeping Archives, 2nd edition, Australian Society of Archivists and Thorpe, Melbourne, 1993, p. 470. |
| **Fixity** | The state or quality of being fixed. |
| **Folder** | An aggregation of records represented in a business system and allocated to a records category within the records classification scheme. A folder is constituted of metadata that may be inherited from the parent (records category) and passed on to a child (record). See also Digital folder. Source: Adapted from The National Archives (UK), Requirements for Electronic Records Management Systems, 3: Reference Document, 2002, p. 3. |
| **Format** | The physical form (such as paper or microfilm) or computer file format in which a record is maintained. See also Native format. Source: Adapted from Department of Defense (US), Design Criteria Standard for Electronic Records Management Software Applications, DoD 5015.2-STD, 2002, p. 14. |
| **Function** | 1 The first level of a business classification scheme. Functions represent the major responsibilities that are managed by the organisation to fulfil its goals. Source: Adapted from AS 4390, Part 4, Clause 7.2.  
2 The largest unit of business activity in an organisation or jurisdiction. |
<p>| <strong>Identification</strong> | The act of giving a record or file a unique identity to provide evidence that it was created or captured. Identification involves recording brief descriptive information about the context of the record and its relation to other records. |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Import</td>
<td>To receive electronic records and associated metadata into one system from another, either within the organisation or elsewhere.</td>
<td></td>
</tr>
<tr>
<td>Inherit</td>
<td>To take on a metadata attribute from a parent entity.</td>
<td>Source: Adapted from The National Archives (UK), Requirements for Electronic Records Management Systems, 3: Reference Document, 2002, p. 4.</td>
</tr>
<tr>
<td>Instance</td>
<td>An occurrence of an electronic record in a particular format or at a particular point in time. For example, one instance of a record may be in its native format while another instance is a rendition. Instances may be created as a product of migration or conversion processes.</td>
<td></td>
</tr>
<tr>
<td>Integration</td>
<td>A tightly bound relationship between the business system and another application or mechanism. Integration implies data being shared between systems, a common look and feel that suggests a single application.</td>
<td>Source: Adapted from NSW Department of Public Works and Services, Request for Tender No. ITS2323 for the Supply of Records and Information Management Systems, Part B: Specifications, 2001, p. 13.</td>
</tr>
<tr>
<td>Interface</td>
<td>A mechanism whereby data can be exchanged between applications.</td>
<td>Source: Adapted from NSW Department of Public Works and Services, Request for Tender No. ITS2323 for the Supply of Records and Information Management Systems, Part B: Specifications, 2001, p. 13.</td>
</tr>
<tr>
<td>Metadata</td>
<td>Structured information that describes and/or allows users to find, manage, control, understand or preserve other information over time. Sources: Adapted from A Cunningham, ‘Six degrees of separation: Australian metadata initiatives and their relationships with international standards’, Archival Science, vol. 1, no. 3, 2001, p. 274.</td>
<td></td>
</tr>
<tr>
<td>Migration</td>
<td>The act of moving records from one system to another, while maintaining the records’ authenticity, integrity, reliability and useability. Migration involves a set of organised tasks designed to periodically transfer digital material from one hardware or software configuration to another, or from one generation of technology to another. See also Conversion.</td>
<td>Source: Adapted from ISO 15489, Part 1, Clause 3.13 and Part 2, Clause 4.3.9.2.</td>
</tr>
<tr>
<td>Native format</td>
<td>The format in which the record was created, or in which the originating application stores records. See also Conversion.</td>
<td>Source: Adapted from NSW Department of Public Works and Services, Request for Tender No. ITS2323 for the Supply of Records and Information Management Systems, Part B: Specifications, 2001, p. 13.</td>
</tr>
<tr>
<td>Record</td>
<td>(noun) Information in any format created, received and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business. See also Electronic record.</td>
<td>Source: ISO 15489, Part 1, Clause 3.15.</td>
</tr>
<tr>
<td>Record category</td>
<td>A subdivision of the records classification scheme, which may be further subdivided into one or more lower-level record categories. A record category is constituted of metadata that may be inherited from the parent (for example, records category) and passed on to a child (for example, folder or aggregation of electronic records). The full set of record categories, at all levels, together constitutes the records classification scheme. See also Records classification scheme.</td>
<td>Source: Adapted from The National Archives (UK), Requirements for Electronic Records Management Systems, 3: Reference Document, 2002, p. 1.</td>
</tr>
<tr>
<td>Record metadata</td>
<td>Identifies, authenticates and contextualises records and the people, processes and systems that create, manage, maintain and use them and the policies that</td>
<td></td>
</tr>
<tr>
<td>Terms</td>
<td>Definitions</td>
<td></td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Record type</strong></td>
<td>Definition of a record object that specifies particular management requirements, metadata attributes and forms of behaviour. A default record type is the norm. Specific record types are deviations from the norm, which allow an organisation to meet regulatory requirements (such as privacy or data matching) for particular groups of records. Source: Adapted from The National Archives (UK), Requirements for Electronic Records Management Systems, 3: Reference Document, 2002, p. 5.</td>
<td></td>
</tr>
<tr>
<td><strong>Records classification scheme</strong></td>
<td>A hierarchical classification tool that, when applied to a business system, can facilitate the capture, titling, retrieval, maintenance and disposition of records. A records classification scheme stems from an organisation’s business classification scheme.</td>
<td></td>
</tr>
<tr>
<td><strong>Records classification tool</strong></td>
<td>A device or method used to assist in classifying, titling, accessing, controlling and retrieving records. May include a records classification scheme, thesaurus, indexing scheme or controlled vocabulary.</td>
<td></td>
</tr>
<tr>
<td><strong>Records management</strong></td>
<td>The field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposition of records, including processes for capturing and maintaining evidence of, and information about, business activities and transactions in the form of records. Source: ISO 15489, Part 1, Clause 3.16.</td>
<td></td>
</tr>
<tr>
<td><strong>Relational database</strong></td>
<td>A collection of data elements organised as a set of formally described tables from which data can be accessed and reassembled in many different ways without having to reorganise the database tables. See also Data element, Database, Field and Table.</td>
<td></td>
</tr>
<tr>
<td><strong>Rendition</strong></td>
<td>Instance of an electronic record made available in another format or on a different medium by a process entirely within the business system control, without loss of content. A rendition should display the same metadata and be managed in a tightly bound relationship with the native format record. Renditions may be required for preservation, access and viewing purposes. See also Conversion.</td>
<td></td>
</tr>
<tr>
<td><strong>Retention period</strong></td>
<td>The length of time after the disposition trigger that a record must be maintained and accessible. At the expiration of the retention period, a record may be subject to a disposition action. See also disposition action and disposition trigger.</td>
<td></td>
</tr>
<tr>
<td><strong>Security category</strong></td>
<td>Hierarchical designation (such as ‘Top secret’ or ‘Protected’) allocated to a user, user role, electronic record or other record plan entity to indicate the level of access allowed. The security category reflects the level of protection that must be applied during use, storage, transmission, transfer and disposal of the record. See also Security controls. Source: Adapted from Cornwell Management Consultants (for the European Commission Interchange of Documentation between Administrations Programme), Model Requirements for the Management of Electronic Records (MoReq Specification), 2001, p. 107.</td>
<td></td>
</tr>
<tr>
<td><strong>Security classification system</strong></td>
<td>A set of procedures for identifying and protecting official information, the disclosure of which could have adverse consequences. The security classification system is implemented by assigning markings that show the value of the information and indicate the minimum level of protection it must be afforded. See also Classification and Security category. Source: Adapted from Attorney-General’s Department, Commonwealth Protective Security Manual, 2000.</td>
<td></td>
</tr>
<tr>
<td><strong>Security controls</strong></td>
<td>A scheme of protective markings that may be allocated to users, electronic records and record plan entities to restrict access. May include a hierarchical security category, possibly in conjunction with a non-hierarchical qualifier. See also Access controls and Descriptor.</td>
<td></td>
</tr>
<tr>
<td><strong>System access control</strong></td>
<td>Any mechanism used to prevent access to the business system by unauthorised users. May include the definition of user profiles, or the use of ID and password login. See also Access controls and Security controls.</td>
<td></td>
</tr>
<tr>
<td><strong>System rules</strong></td>
<td>Policies internal to system software that may be established and/or configured by a business system administrator in order to govern the functionality of a given system and determine the nature of operational processes applied by that system.</td>
<td></td>
</tr>
<tr>
<td><strong>Table</strong></td>
<td>A set of one or more related database fields, each comprising related data elements. One or more tables may combine to form a database. See also Data element, Database and Field.</td>
<td></td>
</tr>
</tbody>
</table>
| **Tracking** | Creating, capturing and maintaining information about the movement and uses of records. 
| **Transaction** | The smallest unit of business activity. Uses of records are themselves transactions. 
The third level in a business classification scheme. 
See also Activity, business classification scheme and Function. 
Sources: Adapted from AS 4390, Part 1, Clause 4.27; AS ISO 15489, Part 2, Clause 4.2.2.2. |
| **Transfer** | A disposition process, consisting of a confirmed export of electronic records and associated metadata, and where applicable aggregations of electronic records, followed by their destruction within the exporting business system. Transfers occur from one organisation to another following administrative change, from an organisation to archival custody, from an organisation to a service provider, from the government to the private sector, or from one government to another. 
| **User access group** | A discrete set of named individuals (users known to the business system) that make up a stable and nameable group. Access to particular records or other file plan entities may be restricted to members of certain user access groups. 
See also Access controls. 
| **User profile** | A summary of all attributes allocated to a user of the business system. Includes all data known to the system, such as username, ID and password, security and access rights, functional access rights. See also Access controls. |
| **User role** | An aggregation or standard set of business system functional permissions that may be granted to a pre-defined subset of system users. 
B Integrating recordkeeping considerations into the systems development life cycle

Business systems are normally developed through a series of phases that begin with planning and the establishment of a project charter, continue with the development of design specifications and functional requirements, and conclude with the actual implementation and maintenance of the system as well as its review and evaluation. If recordkeeping is to be integrated in the design of business systems, then it is essential that recordkeeping considerations be addressed at every phase of the systems development life cycle. Of all the phases in the life cycle, the planning phase is the most important because it is during this phase that fundamental recordkeeping issues are identified and confirmed, and where generic resource requirements to address the issues are identified.

Attempting to build recordkeeping considerations into business systems at later phases of the life cycle will be difficult. This is because the effort will be seen as an ‘add-on’ requiring extra resources, rather than an essential component of the system where resources will have already been identified and where design and implementation considerations will have already been incorporated into the design and implementation phases of the system itself.

An overview of each phase of the systems development life cycle and the recordkeeping implications follow:166

1 Project initiation

The initiation phase of the systems development life cycle begins when management determines that it is necessary to enhance a business process through the application of information technology. The purposes of the initiation phase are to:

- identify and validate an opportunity to improve business accomplishments of the organisation or a deficiency related to a business need;
- identify significant assumptions and constraints on solutions to that need; and
- recommend the exploration of alternative concepts and methods to satisfy the need.

Business projects may be initiated as a result of business process improvement activities, changes in business functions or advances in information technology, or may arise from external drivers such as laws and policies, the establishment of new strategic directions for the government or the pursuit of opportunities presented by external organisations (for example, development and related assistance organisations). The project sponsor articulates this need within the organisation to initiate the systems/project life cycle. During this phase, a project manager is appointed who prepares a statement of need or concept proposal. Issues such as security and recordkeeping (for example, ensuring that records’ authenticity can be

---

166 Information describing each of the phases of the systems development life cycle was derived from Department of Justice Systems Development Life Cycle Guidance Document, Information Resources Management, US Department of Justice, Washington, DC, 2003.
maintained through time, setting retention specifications for records, linking paper and electronic records, establishing records disposal schedules, etc.) and ownership of the issues are identified at a generic level (that is, as issues that need to be addressed as the project proceeds). As such, the project manager normally brings together all of those who will need to make a contribution to the development effort (that is, those who will need to address the issue of recordkeeping and its integration in the design of the system).

2 Planning

During this phase the needs for the system and the proposed concept for the new or modified system are further analysed in order to inform the development of a ‘vision’ of how the business will operate once the approved system is implemented. To ensure that the remaining phases of the systems development life cycle are capable of being carried out on time and within budget, project resources, activities, schedules, tools and reviews are defined. Other high-level requirements such as those for security (that is, the nature of the security certification and accreditation activities) and recordkeeping are further refined based on threat and risk assessments.

3 Requirements analysis

Functional user requirements are formally defined and delineate the requirements in terms of data, system performance, security and maintainability requirements for the system. All requirements are defined to a level of detail sufficient for systems design to proceed. All requirements need to be measurable and testable, and relate to the business need or opportunity identified in the initiation phase. Documentation related to user requirements from the planning phase are used as the basis for further user needs analysis and the development of detailed user requirements. During the requirements analysis phase, the system is defined in more detail with regard to system inputs, processes, outputs and interfaces. This definition process occurs at the functional level (that is, the system is described in terms of the functions to be performed, not in terms of computer programs, files and data streams). The emphasis in this phase is on determining what functions must be performed rather than how to perform those functions.

4 Design

The physical characteristics of the system are designed during this phase. The operating environment is established, major subsystems and their inputs and outputs are defined, and processes are allocated to resources. Everything requiring user input or approval is documented and reviewed by the user. The physical characteristics of the system are specified and a detailed design is prepared. Subsystems identified during the design phase are used to create a detailed structure of the system. Each subsystem is partitioned into one or more design units or modules. Detailed logic specifications are prepared for each software module.

The design stage must account for the functional requirements for recordkeeping and other related requirements (for example, management, procedural, technical) identified as a result of the previous requirements analysis stage. Similar to security
requirements, recordkeeping design specifications should be woven seamlessly into the physical and logical design specifications (that is, data architectures, data models, etc.) for the system.

5 Implementation
The activities of this phase translate the system design produced in the design phase into a working information system capable of addressing the system requirements. The development phase contains activities for building the system, testing the system and conducting functional qualification testing to ensure the system functional processes satisfy the functional process requirements. An important step prior to installing and operating the system in a production environment is to subject the system to certification and accreditation activities. Several types of tests are conducted in this phase. First, subsystem integration tests are executed and evaluated by the development team to prove that the program components integrate properly into the subsystems and that the subsystems integrate properly into an application. This is where tests to assess the capability of the system to capture and maintain records (in accordance with the functional requirements) are conducted. Next, system tests are conducted and evaluated to ensure the developed system meets all technical requirements, including performance requirements. Again, tests of recordkeeping capabilities would form part of this overall testing and assessment process. Tests focusing on data integrity from a security and recordkeeping perspective would validate the capability of the system to respect requirements for authenticity, reliability, completeness, etc. Finally, users participate in acceptance testing to confirm that the developed system meets all user requirements including the ability of the system to facilitate records access and retrieval. Once the system is accepted, it moves into ‘production’, which is based on formal notification of implementation to end-users, execution of the previously defined training plan, data entry or conversion, and post implementation review.

6 Maintenance
During this phase the system is monitored for continued performance in accordance with user requirements, and required system modifications are incorporated. The operational system is periodically assessed through in-process reviews to determine how the system can be made more efficient and effective. Operations continue as long as the system can be effectively adapted to respond to an organisation’s needs. From a recordkeeping perspective, this means that changes to the recordkeeping requirements (that is, driven by new laws, changing business requirements, changes in the design of business processes, etc.) must be accommodated in the monitoring and change process activities undertaken during this phase. Providing user support is an ongoing activity. New users will require training. The emphasis of this phase is to ensure that the users’ needs are met and the system continues to perform as specified in the operational environment. When modifications or changes are identified as necessary, the system may re-enter the planning phase. Activities associated with the disposition of the system ensure the orderly termination of the system and preserve the vital information about the system so that some or all of the information (including information in records) may be reactivated in the future if necessary. Emphasis is given to proper preservation of the records processed by the
system (that is, migration of valuable records to other systems including those supported by an archive), in accordance with applicable records management regulations and policies, for potential future access.

7 Review and evaluation

Review and evaluation of the system occur from two perspectives. First is the perspective of the business system itself. In-process reviews are conducted at each phase of the systems development life cycle to ensure that the activities undertaken in any given phase achieve their pre-defined goals and meet their performance targets. Such in-process reviews must be supported by agreed performance measures and assessment methods. If the capability of the system to generate, capture and manage records is to be measured, then performance measures for recordkeeping and methods for carrying out assessments of recordkeeping capability must be developed, applied and, wherever possible, integrated in the performance measures and assessment methods employed in the in-process reviews conducted at each phase of the systems development life cycle.

Second is the perspective of the methodology employed to develop the systems. Is the systems development methodology effective, efficient, complete, etc.? The evaluation of the methodology can occur at the conclusion of the business systems project or as part of an overall general assessment of the development and management of business systems. Again, recordkeeping considerations, including performance measures and other criteria, must be developed and integrated in the tools and techniques employed to assess business systems development generally.
Further reading


