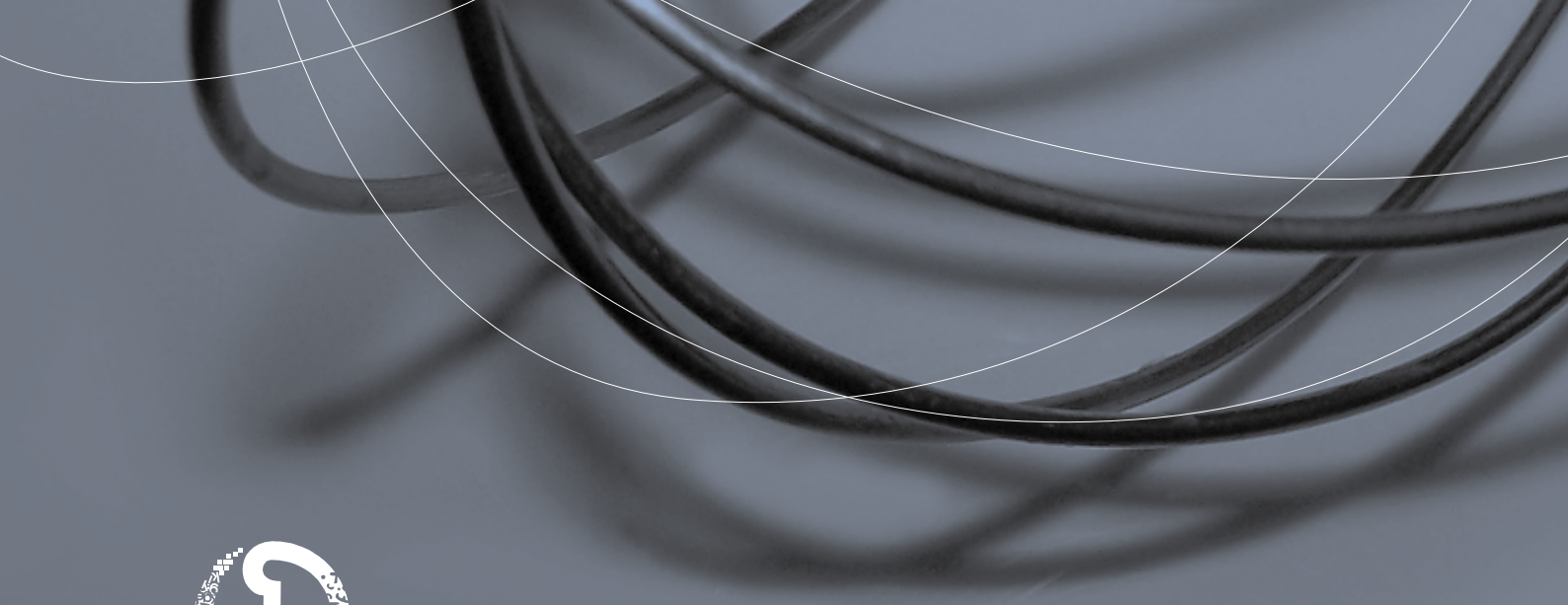


ICA

International Council
on Archives

Principles and Functional Requirements

for Records in Electronic Office Environments

MODULE 3

Guidelines and Functional Requirements for Records in Business Systems

Published by the International Council on Archives. This module was developed by the National Archives of Australia and Queensland State Archives in conjunction with a joint project team formed by members of the International Council on Archives and the Australasian Digital Recordkeeping Initiative.

© International Council on Archives 2008

ISBN: 978-2-918004-02-8

Reproduction by translation or reprinting of the whole or of parts for non-commercial purposes is allowed on condition that due acknowledgement is made.

This publication should be cited as: International Council on Archives, *Principles and Functional Requirements for Records in Electronic Office Environments – Module 3: Guidelines and Functional Requirements for Records in Business Systems*, 2008, published at www.ica.org.

CONTENTS

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),[1] 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;

---

1 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.

- develop requirements for functionality for records to be included in a design specification when building, upgrading or purchasing business system software;
- 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,[2] 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

[2] A formal instrument that defines the retention periods and consequent actions authorised for classes of records described in the authority.

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.

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*
- *Module 3: Guidelines and Functional Requirements for Records in Business Systems.*

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.

The reference metadata standard for these requirements is 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.

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.[3] 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.

[3] International Standard on Records Management, ISO 15489.

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.'[4] 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.[5] 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.[6] It allows records to be located, rendered and understood in a meaningful way. The International Standard on Information and Documentation—Records 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

---

4 International Standard on Records Management, ISO 15489.

5 Philip C Bantin, *Strategies for Managing Electronic Records: Lessons Learned from the Indiana University Electronic Records Project,* available at http://www.indiana.edu/~libarch/ER/ecure2000.pdf, 2003.

6 International Standard on Information and Documentation—Records Management Processes—Metadata for Records, ISO 23081.

- 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.

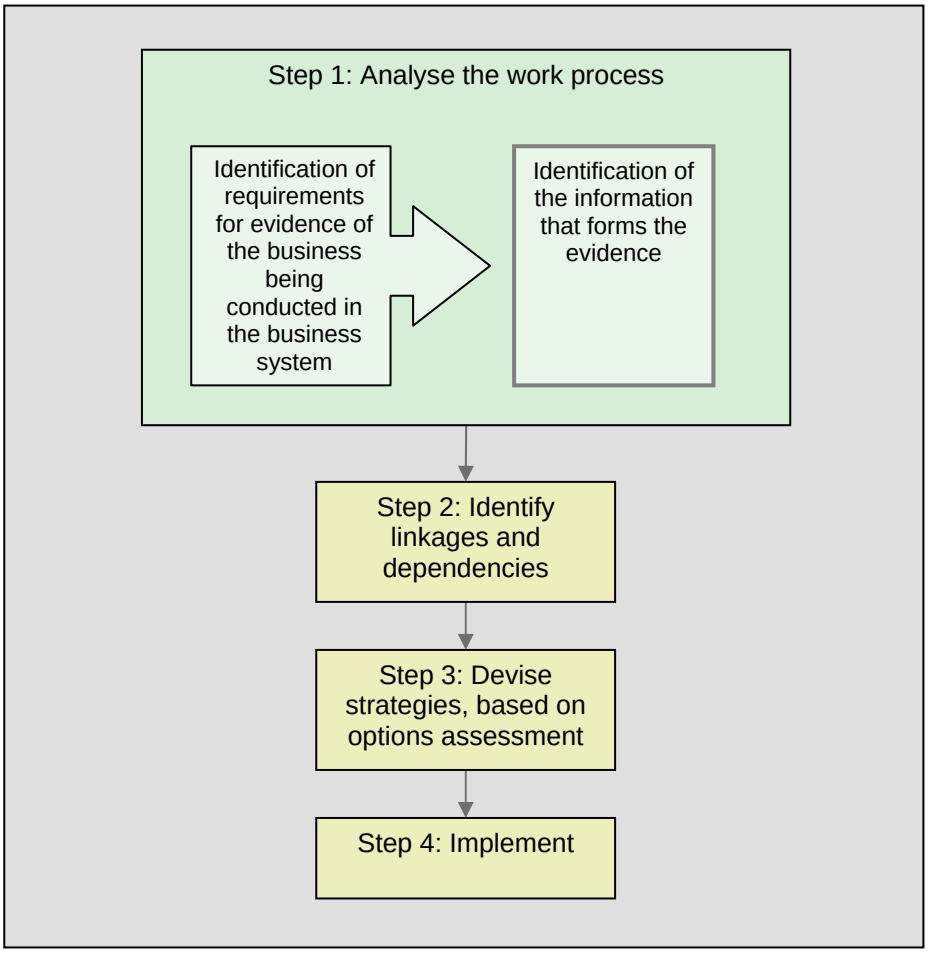
Business processes having the greatest potential for reflecting good recordkeeping are those that are highly structured with well-defined transactions where the identification of where in the business process records should be generated and even what they should look like (for example, forms) is relatively 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;[7]

7 This document primarily focuses on the management of records arising from structured rather than unstructured data.

- 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 regulatory and business requirements, to determine what evidence is required to be kept.[8]

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.[9]

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.[10]

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 business[11]

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.[12] 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.

---

8 Refer to National Archives of Australia, *DIRKS Manual: A Strategic Approach to Managing Business Information,* available at http://www.naa.gov.au/records-management/publications/DIRKS-manual.aspx for further information.

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

10 While tailored to a particular jurisdiction, see Queensland State Archives, *Guideline for the Development of Retention and Disposal Schedules* available at http://www.archives.qld.gov.au/downloads/rdschedule.pdf for guidance on developing a disposition authority.

11 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.

12 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.

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.
- 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.[13]

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.

---

[13] DIRKS stands for Designing and Implementing Recordkeeping Systems. Steps A–C cover this analysis process. For more information, see National Archives of Australia, *DIRKS Manual: A Strategic Approach to Managing Business Information* available at http://www.naa.gov.au/records-management/publications/DIRKS-manual.aspx or State Records NSW, *The DIRKS Manual: Strategies for Documenting Government Business* available at http://www.records.nsw.gov.au/recordkeeping/dirks-manual_4226.asp.

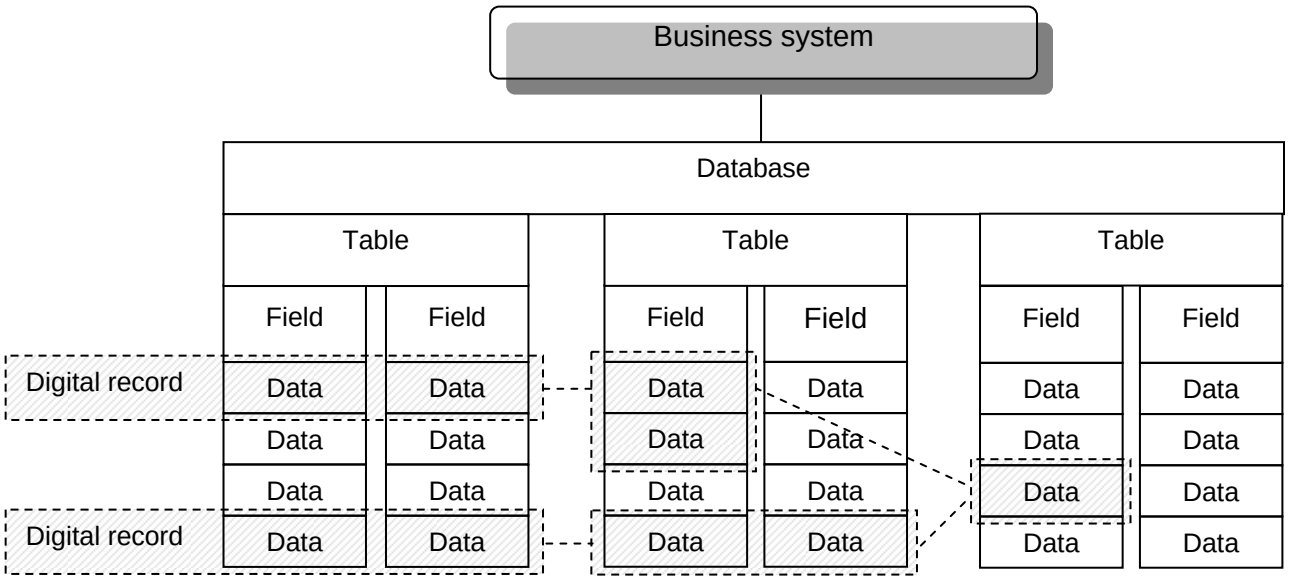
For others, it will require analysis of the data structures, data models and class models that underlie the system to identify the specific data elements that together constitute the content and provide the necessary evidence (see Figures 2 and 3 below for an illustration of this).

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 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.[14] In this example the record[15] 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.

14 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.

15 '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 A: Personnel				
Staff no.	**Surname**	**First name**	**Address**	**City**
0078652	Larsen	Sevren	78/1 Hoddle St, Carlton	Melbourne
0078653	Lee	Jamie	55 Ramsey St, Vermont	Melbourne
0078654	Smith	Bob	7 Pollie Crt, Barton	Canberra
0078655	Schmidt	Helmutt	1/123 North Rd, Balmain	Sydney
0078656	Darcy	Kyra	67 Green St, Mt Lawley	Perth

Table B: Salaries			
Pay code	**Level**	**Year**	**Pay rate**
A41	APS4	Year 1	$45,000
A42	APS4	Year 2	$46,000
A43	APS4	Year 3	$47,000
A44	APS4	Year 4	$48,000
A51	APS5	Year 1	$54,000
A52	APS5	Year 2	$55,000
A53	APS5	Year 3	$56,000

Table C: Cost centres	
Staff no.	**Pay code**
0078652	A53
0078653	A42
0078654	A42
0078655	A41
0078656	A51

Table D: Staff to pay levels		
Centre code	**Cost centre**	**Director**
M001	Melbourne Office	Shay Jones
S001	Sydney Office	Fred Nguyen
P001	Perth Office	Alberta Johnson
C001	Canberra Office	John Wasp

Table E: Staff to cost centres	
Staff no.	**Centre code**
0078652	M001
0078653	M001
0078654	C001
0078655	S001
0078656	P001

Key

Data elements comprising the personnel record of Kyra Darcy

Data elements comprising the record of Bob Smith's address details

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.[16]

---

16 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.

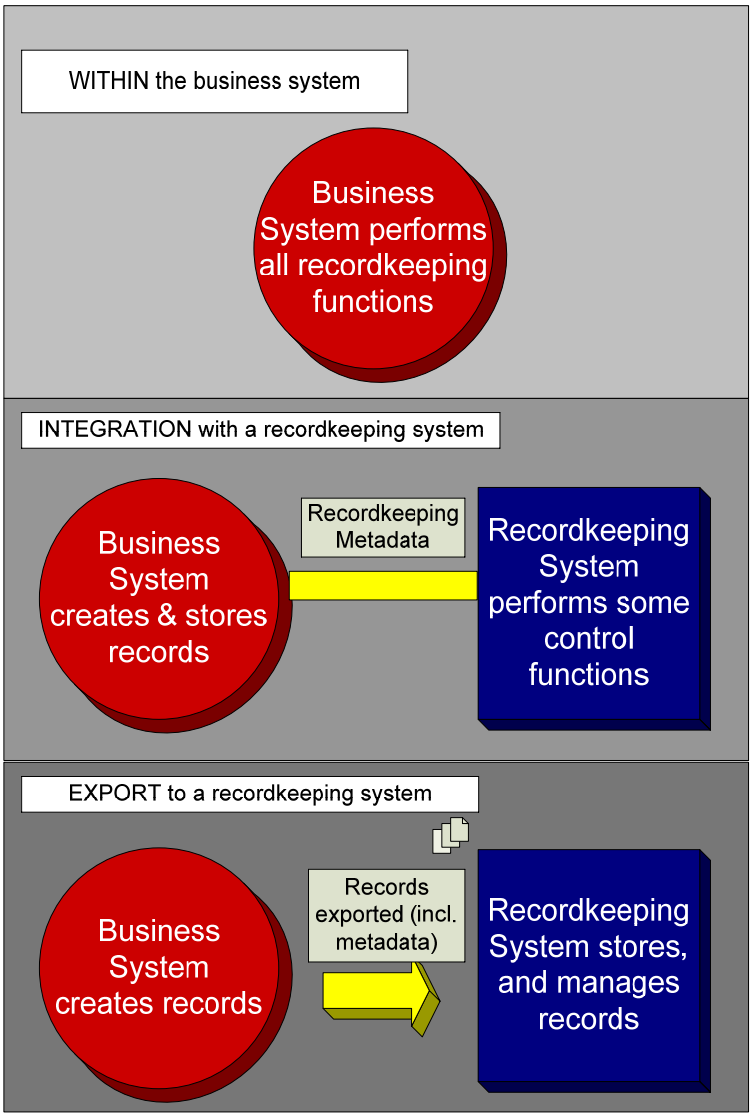
To be considered authentic and reliable evidence, content must be fixed to a point in time and unalterable. Because business systems generally contain dynamic, current data that is subject to regular updates, strategies for maintaining a 'fixed' record must be implemented. These strategies will be influenced 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.

Figure 4: Possible system options for managing records created in business systems



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

System options	Benefits	Challenges
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 re-used 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 records management system (federated records management)	• Business systems records can be managed collectively with records created by other systems • Exploits re-use of external records management system	• Seamlessness of process may be affected by the capability of the identified records 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.[17]

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.

Table 2: User roles

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.
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 extracts of records and edit record metadata. The powers assigned to records administrators will vary depending on the business needs of the organisation and the level of responsibility of the role.
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.

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 **must allow** this combination of roles and functions. 'No' means the business system **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.

---

17 For further information on feasibility analysis, refer to National Archives of Australia, *DIRKS Manual: A Strategic Approach to Managing Business Information* available at http://www.naa.gov.au/Images/dirks_A12_feasibility_tcm2-940.pdf.

Table 3: Roles and functions

Function	User	Records administrator	System administrator
Create new records	Yes	Yes	Yes
Add/edit record metadata when identifying the record[18]	Yes	Yes	Optional
Allocate disposition authorisation to a record or, where applicable, an aggregation of records	No	Optional	Yes
View audit trails	Optional[19]	Optional	Yes
Edit audit trail data[20]	No	No	No

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.

18 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.

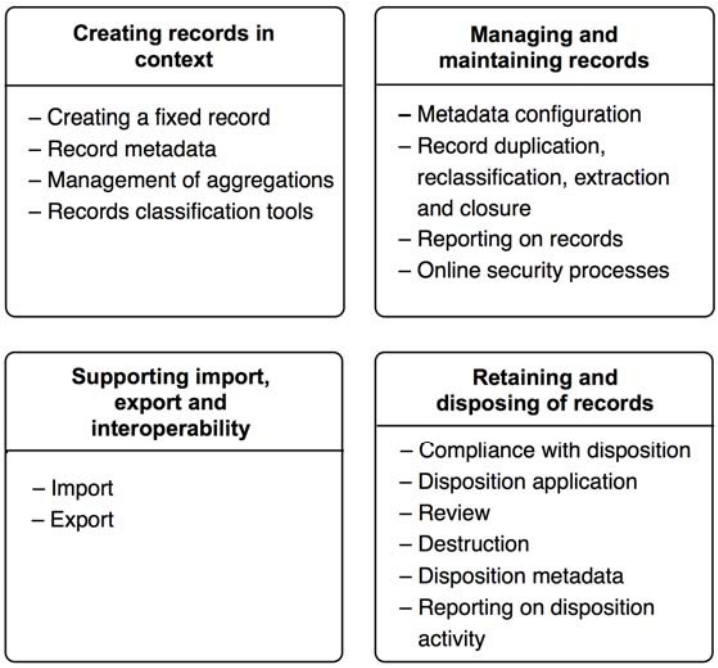
19 Organisations need to determine whether there are valid operational reasons for allowing users to view audit logs.

20 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.[21] 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?

---

21 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:[22]

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.

---

[22] Further information on the process of assessing existing systems can be found in Step D of National Archives of Australia, *DIRKS Manual: A Strategic Response to Managing Business Information* available at http://www.naa.gov.au/records-management/publications/DIRKS-manual.aspx.

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.[23]

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

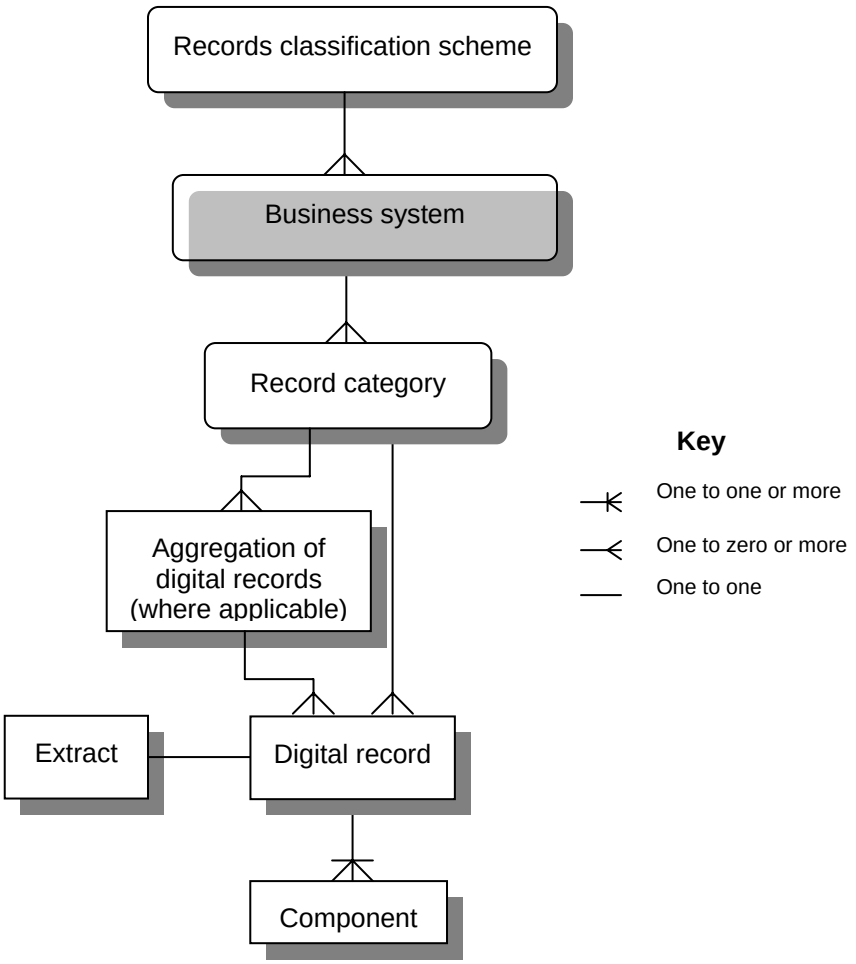
Evaluate the information collected during the review, identify weaknesses and strengths, and determine recommendations for improving functionality for records. Recommendations may be prioritised based on risk, importance and feasibility, for example, if the system is unlikely to be developed in the near 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.

23 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.[24] 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.

24 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.[25]

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

---

[25] 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 **as**sessment of requirements for records, there may be no need to retain the data and it can be overwritten.[26] 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

26 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.[27] For systems that only relate to a limited number of transactions, this metadata may be found in the system documentation,[28] 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:

1	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.[29]
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.[30] 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.

27 For information on functional requirements to support a records classification scheme, see *Module 2: Guidelines and Functional Requirements for Records in Electronic Office Environments*

28 System documentation may encompass schemas, data dictionaries, and data and class models.

29 Data file formats and document types should be specified according to business needs.

	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[31] 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,[32] 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.[33]

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

30 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.

31 For example, by means of a symbol or special icon.

32 Some BS, such as e-commerce systems, are capable of creating and sending electronic messages in support of their primary business functions.

33 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.

	records contained within the BS; and • provide a mechanism to enable the BS to import electronic records directly from an external BS,[34] as required to support the system's core business functions.
6	Allow users to capture and store all electronic records received by the system in their native format.
7	Not limit the number of records that can be captured and retained by the system.[35]

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

8	Allow the organisation to specify the format or pattern of the unique identifier, either through configuration or through specified requirements.
9	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.[36] 9.1 Where the BS supports the conversion of electronic records from their original formats as part of the capture process,[37] 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.[38]
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.

34 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.

35 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.

36 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.

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

38 '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.

	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.[39]

3.1.2 Record metadata

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

12	Support the range of metadata elements detailed in relevant metadata standards and any other metadata required to support the organisation's business.
13	Be able to automatically capture metadata acquired directly from an authoring application,[40] an operating system, an electronic records management system[41] or generated by the BS itself.[42]
14	Capture all metadata specified during system configuration, and retain it with the electronic record in a tightly bound[43] relationship at all times.
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 over-ride 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.[44]

39 This requirement applies particularly to transactional BS that regularly receive a wide variety of record formats which must be captured by the system.

40 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.

41 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.

42 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.

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

44 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

18	Be able to store selected metadata over time, regardless of whether the related record has been archived, deleted or destroyed.[45]

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

19	Be able to capture metadata entered manually by a user.
20	Allow the definition of: • customised metadata fields for electronic records; • selected metadata element set for particular record types; • obligation levels[46] for selected metadata elements either through specified requirements or through configuration by a business system administrator.
21	Allow user-defined metadata fields for the entry of descriptive information about the records or, where applicable, aggregations of records.
22	Retain a history in the metadata profile of the reclassification of a record, or where applicable an aggregation of records, including the original location of an aggregation of records.[47]

The business system **may**:

23	Allow the business system administrator to configure pre-defined system rules[48] for the assignment of metadata on capture of a record, or where applicable, an aggregation of records of a particular record type. 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	Support the creation and/or receipt of aggregations of electronic records, whereby associated electronic records may be linked together through record metadata so that records management processes may be applied to all records within the aggregation.[49] Where the BS supports the aggregation of records, it **must**:

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.

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

46 Obligation levels should reflect those specified in relevant metadata standards.

47 Noting the usual audit trail requirements for systems.

48 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.

	24.1	Be able to generate a unique identifier for each aggregation of records defined by the system.[50]
	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.
	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.[51]
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:[52]

- **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.

---

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

50 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.

51 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).

52 These are taken from ISO 15489.1 Records Management, Section 7.2 Characteristics of records.

- **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.

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:

27	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

3.2.1 Metadata configuration

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

28	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.
29	Allow a business system administrator to define the source of data for each metadata element during system configuration.
30	Have the ability to use the contents of a metadata element to determine a functional process,[53] where the element can be related to the functional behaviour of the BS. 30.1 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. 30.2 Where the BS supports links between disposition functions and other records management mechanisms supported by the BS,[54] 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.
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.[55]

[53] This functionality may either be incorporated within the BS or provided through integration with an external system, such as an electronic records management system.

[54] 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.

[55] 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

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.[56]
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; • numeric; • date/time; and • logical (i.e. Yes/No or True/False).
37	Allow metadata values to be obtained from look-up tables or from calls to the operating system, application platform or other software applications, as required.

The business system **may**:

38	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:

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.

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

39	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).
40	Support mechanisms to enable the duplication of electronic records.[57] 40.1 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. 40.2 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. 40.3 The BS may facilitate the tracking of copies made of an identified electronic record, recording information on access to copies in the audit log.[58]

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

41	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. 41.1 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.[59] 41.2 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.[60] 41.3 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.
42	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:

43	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.

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

---

57 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.

58 The audit log may keep details of copies created outside the BS, as well as copies created within the BS.

59 Whether the extract itself needs to be maintained as a record depends on the analysis of business processes (see Section 2.1).

60 For example, an extract may have a different security category from the originating record.

44	Be able to produce a report listing the details and outcome of any migration process to ensure the integrity of electronic records.[61]

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

45	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.

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:

46	Automatically record the details of all online security processes (for example, in an audit trail).
47	Support date and time stamping for all records subject to online security processes.

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

Encryption

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

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.[62] 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. 48.3 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.[63] 48.4 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. 48.5 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: 48.6 Be able to store encrypted electronic records in unencrypted form. 48.7 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.[64]

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.

62 If this requirement is meant through integration with an external system

63 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.

64 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.

The business system **should**:

49	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:

50	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.[65] Where the BS supports the use of digital signatures, it **must**, either alone or in conjunction with other systems: 50.1 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. 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.[66] Where the BS supports the use of digital signatures, it s**hould**, 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.[67]

65 This requirement is primarily of concern for BS that routinely send or receive digital records using digital signature technology.

66 Changes may be made to the metadata, but not to the content of the record.

Authentication

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

51	Be able to support authentication through interface with PKI-based security technologies. Where the BS supports authentication interface with PKI-based security technologies, it must: 51.1 Be able to store metadata about the process of authentication, including: • the serial number or unique identifier of the digital certificate; • the registration and certification authority responsible for authentication; and • the date and time of authentication. 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.*[68]

---

67 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.

68 Available at http://www.adri.gov.au/content.asp?cID=3.

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,[69] 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 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:

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.

[69] These may include records exported from an electronic document management system or an electronic records management system.

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.[70]

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

61	Ensure that any export action is documented in metadata associated with the record.

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

62	Be able to export electronic records that have been converted into open, fully documented file formats.

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.[71]

70 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.

71 While tailored to a particular jurisdiction, Queensland State Archives, *Public Records Brief: Decommissioning Business Systems* available at http://www.archives.qld.gov.au/publications/PublicRecordsBriefs/DecommissioningB

- **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:

63	Support the controlled disposition of records legally authorised for disposition.
64	Allow the definition of disposition classes,[72] which can be applied to electronic records and associated metadata and, where applicable aggregations of electronic records, either through the internal[73] functionality of the BS software or via an automatic[74] or manual[75] external mechanism (noting Requirement 77.

usinessSystems.pdf outlines some issues that may need to be considered when planning for system decommissioning.

72 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.

73 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.

74 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.

75 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.

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;[76] 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.[77]
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:

73	Be able to import[78] and export[79] a set of disposition classes in a standard format.[80]

76 Transfer consists of confirmed export followed by destruction, once the success of the transfer process has been confirmed.

77 For example, 'destroy when superseded', 'disposal not authorised'.

78 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.

79 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.

80 A structured set of disposition classes issued by an archival authority may be known as a disposition authority or disposition/retention schedule.

74	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.[81]

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

75	Support the definition of disposition classes from multiple disposition authorities.[82]
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:

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;[83] • the integration of external software applications with the BS so as to enable the application of disposition functionality;[84] • manual mapping and application of disposition authorisation to the records of the BS by the business system administrator or other authorised user;[85] or • any combination of the above.[86] 77.1 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.

81 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.

82 To support organisations that may have more than one current approved disposition authority.

83 The level of sophistication of the disposition functionality incorporated within the BS will vary depending on the nature and complexity of the system.

84 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.

85 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 manually apply disposition actions to the records, or where applicable aggregations of records, as required.

78	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.
79	Record all disposition actions in a metadata profile.
80	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.
81	Allow a business system administrator or other authorised user to apply a different disposition class to an electronic record at any time.
82	Restrict the ability to apply and reapply disposition classes to the business system administrator or other authorised user.
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[87] 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.[88] 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.[89]

86 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.

87 Reapplication of a disposition class must take immediate effect within the disposition process.

88 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.

89 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

89	Prevent the deletion or destruction of any electronic record subject to a disposition freeze.[90]
90	Restrict the ability to remove a disposition freeze to a business system administrator or other authorised user.
91	Be able to identify any conflict of disposition actions and either: • automatically apply the correct disposition action according to precedence defined by the organisation;[91] 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:

92	Be capable of sentencing on creation[92] 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.[93]
93	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:

94	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.[94] 94.1 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.
95	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:

96	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.

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.

90 Under other circumstances, deletion or destruction may be carried out by a business system administrator or authorised user. See Requirement 86.

91 Usually the longer period is applied.

92 The identification of the retention period of a record at the time the record is created.

93 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).

94 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.

97	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.
98	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:

99	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.
100	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:

101	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.[95]
102	Seek confirmation of destruction from a business system administrator or other authorised user as part of the disposition process.
103	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.
104	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.
105	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.

95 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.

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

106	Have the ability to ensure that when an electronic record is authorised for destruction, all 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.[96]

3.4.5 Disposition metadata

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

107	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.
108	Actively link disposition metadata to the functionality it represents, so that it can be used to trigger automated processes.[97]
109	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.[98]
110	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.
111	Be able to retain metadata for electronic records, and where applicable aggregations of electronic records, that have been transferred or destroyed.
112	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.

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

113	Allow users to add any metadata elements required for the archival management of electronic records selected for archival transfer.
114	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.
115	Allow a business system administrator to specify a subset of metadata[99] to be retained for electronic records, and where applicable aggregations of electronic records, that have been transferred, destroyed or moved offline.

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

116	Be able to export metadata as specified by relevant metadata standards.
117	Support free-text fields for user-definable notes.[100]

96 For example, if a disposition authority does not cover all renditions, or if an organisation has reason to keep a particular rendition.

97 This functionality may either be incorporated within the BS or provided through integration with an external mechanism, such as an electronic records management system.

98 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.

99 Ideally the mandatory metadata elements, as set out in relevant metadata standards.

118	Support the entry of management metadata for disposition classes and disposition authorities, including: • a scheduled review date; • date and details of revision; and • date and details when superseded.
119	Allow a business system administrator to archive[101] the metadata retained for electronic records, and where applicable aggregations of electronic records, that have been transferred or destroyed.

3.4.6 Reporting on disposition activity

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

120	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.
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.[102]

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

124	Be able to report on all electronic records subject to a disposition freeze.[103]

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

125	Be able to report on review decisions over a given period of time.

---

100 For example, to link a disposition decision to retention requirements found in legislation.

101 That is, take a copy that is outside the control of the BS.

102 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.

103 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

Term	Definition
Access	The right, opportunity, means of finding, using or retrieving information. Source: ISO 15489, Part 3, Clause 3.1.
Access controls	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.
Aggregation	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**.
Audit trail	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.
Authentication	The process of testing an assertion in order to establish a level of confidence in the assertion's reliability. Source: Australian Government Information Management Office, *The Australian Government e-Authentication Framework.*
Business system	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)**.
Business system administrator	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.

Capture	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. Adapted from AS 4390, Part 1, Clause 4.7.
Certification authority	A body that generates, signs and issues public key certificates that bind subscribers to their public key. Source: Australian Government Information Management Office, *The Australian Government e-Authentication Framework.*
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**. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 1.
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**.
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)**. Source: National Archives of Australia, *Recordkeeping and Online Security Processes: Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption*, 2004.

Data	Facts or instructions represented in a formalised manner, suitable for transmission, interpretation or processing manually or automatically. Source: International Council on Archives, *Dictionary of Archival Terminology*, KG Saur, Munich, 1988, p. 48.
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. See also **Data, Component, Database**, **Electronic record**, **Field** and **Table**.
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 1, 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.
Disposition action	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**.
Disposition authority	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**.
Disposition class	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.
Disposition trigger	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**.
Electronic document and records management system (EDRMS)	An electronic records management system capable of providing document management functionality.
Electronic messages	Any communication using an electronic system for the conduct of official business internally, between organisations, or with the outside world. Common examples include email, instant messaging and SMS (short messaging services). Source: National Archives of Australia, *Digital Recordkeeping: Guidelines for Creating, Managing and Preserving Digital Records,* exposure draft, 2004.
Electronic messaging systems	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.
Electronic record	Records on electronic storage media, produced, communicated, maintained and/or accessed by means of electronic equipment.

Electronic records management system (ERMS)	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.
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 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.
ERMS	See **Electronic records management system**.
Evidence	Proof of a business transaction.
Export	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.
Extract	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.
Field	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**.
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.
Identification	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.
Import	To receive electronic records and associated metadata into one system from another, either within the organisation or elsewhere.
Inherit	To take on a metadata attribute from a parent entity. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 4.
Instance	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.
Integration	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. 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.
Interface	A mechanism whereby data can be exchanged between applications. 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.
Metadata	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.
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. See also **Conversion**. 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**. 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.
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 **Electronic 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 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**. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 1.
Record 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. Source: ISO 23081, Part 1, Clause 4.
Record type	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.
Records classification scheme	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.
Records classification tool	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.
Records management	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.
Relational database	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**.
Rendition	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**.

Retention period	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**.
Security category	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.
Security classification system	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.
Security controls	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**.
System access control	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**.
System rules	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.
Table	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**.
Tracking	Creating, capturing and maintaining information about the movement and uses of records. Source: ISO 15489, Part 1, Clause 3.19.
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. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 6.
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**. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 28.
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. Source: Adapted from The National Archives (UK), *Requirements for Electronic Records Management Systems, 3: Reference Document*, 2002, p. 6.

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:[104]

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 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

---

[104] 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.

security and recordkeeping (for example, ensuring that records' authenticity can be 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.

C Further reading

Cornwell Management Consultants (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.

Indiana University,: *Electronic Records Project,* http://www.libraries.iub.edu/index.php?pageId=3313.

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.

International Standards Organization, ISO 154890 – 1: 2001, Information and Documentation – Records Management – Part 1: General.

International Standards Organization, ISO 23081 – 1: 2006, Information and Documentation – Records Management Processes – Metadata for Records, Part 1 – Principles.

International Standards Organization, ISO TR 154890 - 2: 2001 Information and Documentation – Records Management – Part 2: Guidelines.

International Standards Organization, ISO TR 26122: 2008 Information and Documentation – Work Process Analysis for Records.

International Standards Organization, ISO/TS 23081 – 2: 2007, Information and Documentation – Records Management Processes – Metadata for Records, Part 2 – Conceptual and iImplementation Issues.

University of Pittsburgh, *Functional Requirements for Evidence in Recordkeeping: The Pittsburgh Project*, 1996, http://www.archimuse.com/papers/nhprc/BACartic.html.