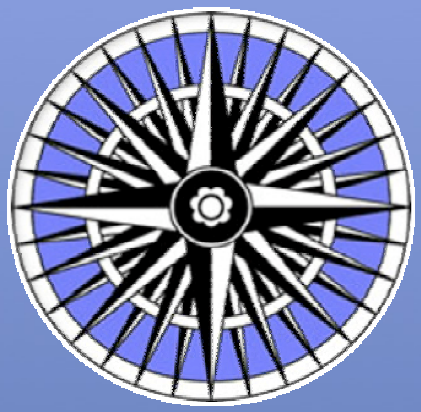
INTERNATIONAL RECORDS MANAGEMENT TRUST



INTEGRATING RECORDS MANAGEMENT IN ICT SYSTEMS

Good Practice Indicators

CONTENTS

FIGURE 1:

Designing a Records Management Improvement Programme

FIGURE 2:

Integrating Records Management in the Systems Development Lifecycle

Designing a Records Management Improvement Programme

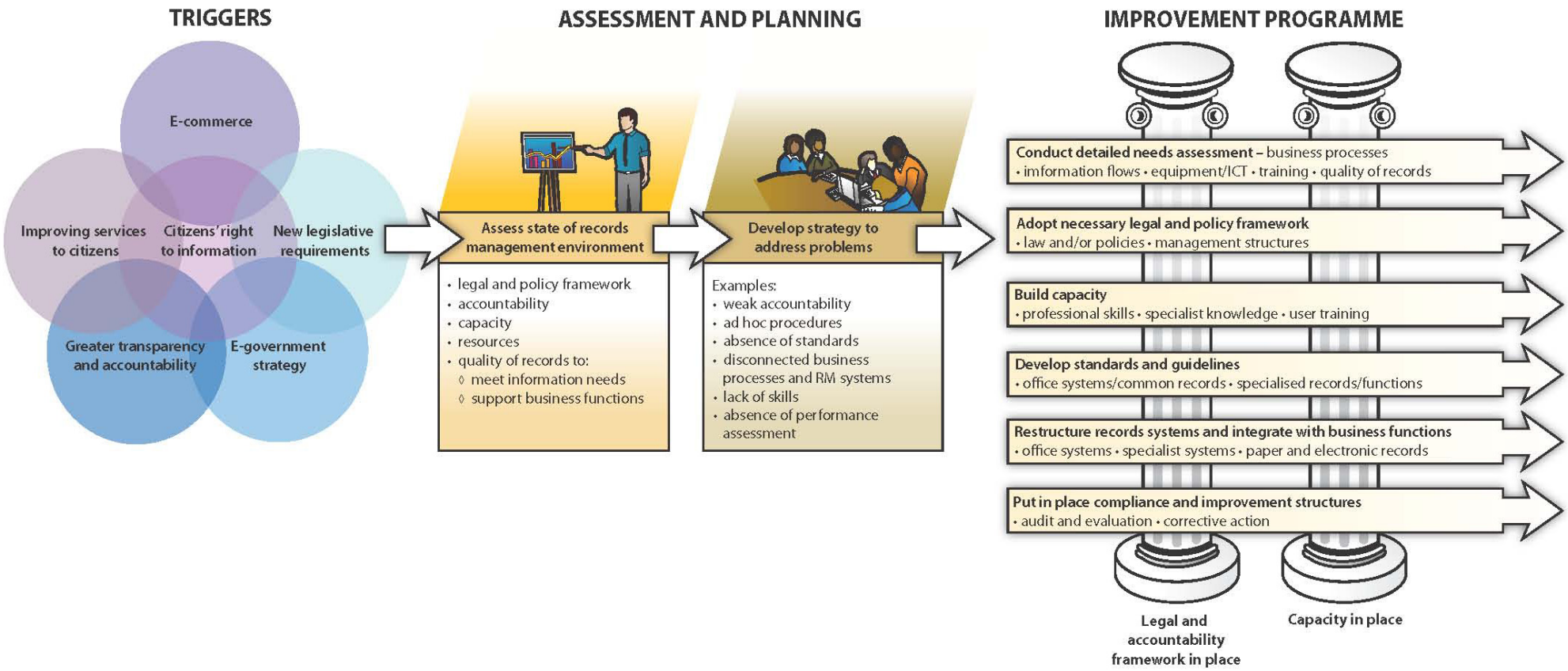


Figure 1

Integrating Records Management in the Systems Development Life Cycle

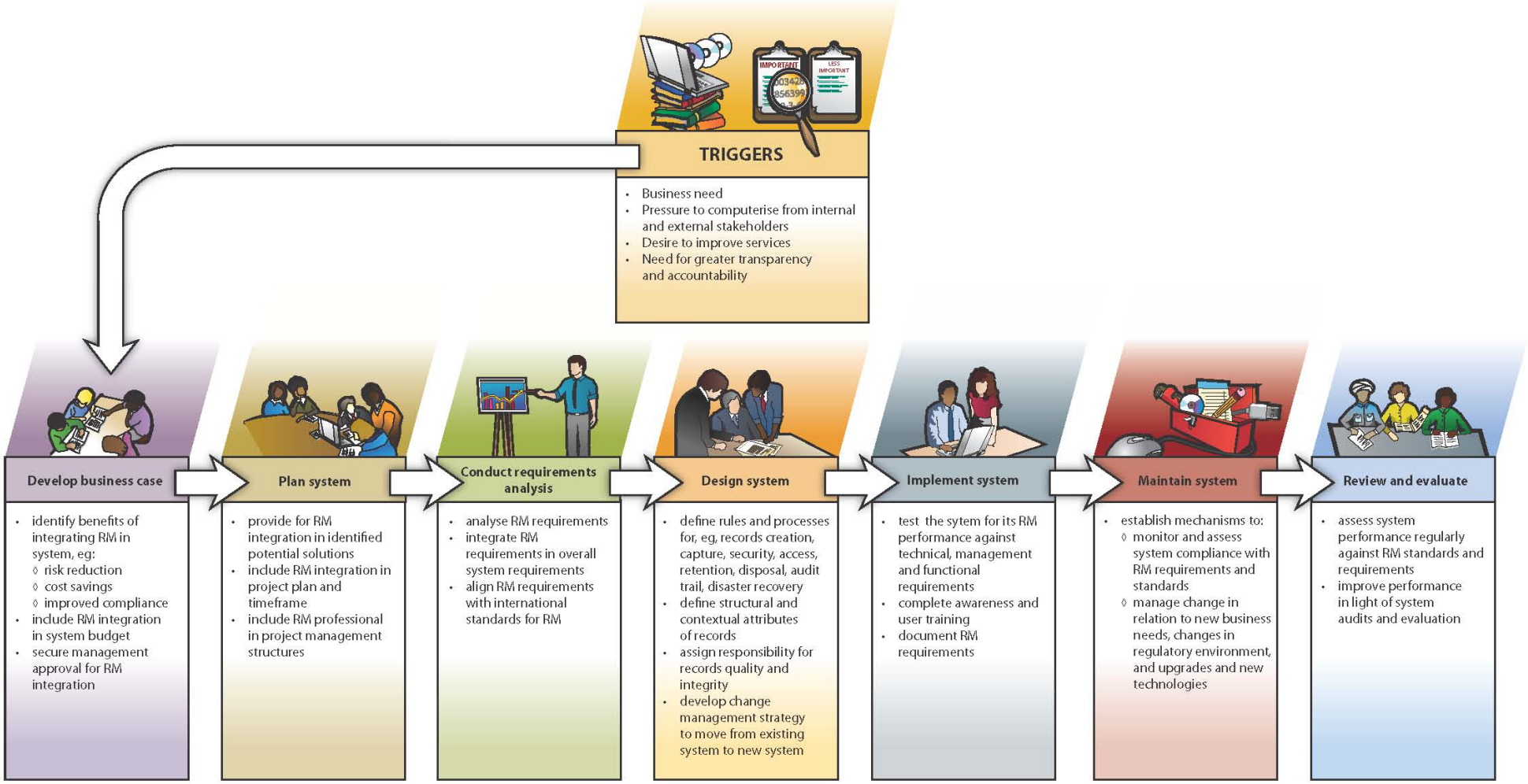


Figure 2

1 Why Records Management is Important

Well managed records are a foundation for good governance. They serve both to document the policies, transactions and activities of governments and to provide a trusted source of information to support decision-making and accountability.

Many government operations that traditionally depended on information derived from paper records have become partially or wholly automated. As governments migrate to an on-line environment, records in electronic form are providing the basis for conducting business, serving the public, managing state resources, measuring progress and outcomes, and protecting their own and others' rights. Records management is becoming increasingly dependent on technology. It is important therefore to have objective means of assessing the strengths and weaknesses of records systems and determining whether they are capable of capturing, maintaining and providing access to records over time

Governments are now more dependent on information in electronic systems to carry out their day-to-day functions and make decisions; common examples include systems designed for:

- human resource management
- financial management
- land administration
- patient/health care management
- licensing
- registration
- benefit delivery.

New technology is making significant contributions to improving government programmes and services, achieving development goals and advancing e-government strategies. However, records management is not being given the attention it requires in the transition to the electronic environment. In too many cases, ICT systems are introduced without the essential processes and controls for the capture, long-term safeguarding and accessibility of electronic records[1]. This undermines the ability of civil servants and citizens alike to trust the information generated by government ICT systems. Governments need to act to ensure that ICT systems provide trusted information that is reliable, complete, unaltered and useable. This requires records management solutions to be integrated in ICT systems during their planning and design, rather than be added on during or after implementation.

[1] 'Digital records' is the more accurate term but 'electronic records' is more commonly used. Digital records include records stored in electronic and non-electronic format such as optical disk.

The challenge for any government is to know whether existing or planned ICT systems are technically capable of supporting records management requirements and protecting the information base on which government depends.

2 Purpose of the Tool

This tool is designed to help governments determine whether or not records management requirements have been integrated in ICT systems. It should assist in identifying good practices and measuring if good practices have been achieved, from the planning and design stage through to implementation. The specific purposes of the tool are threefold:

- to provide a high-level guide to integrating record management in ICT systems
- to define good practices for managing records created and held in ICT systems
- to provide selective indicators that can be used to determine whether or not good records management policies and practices are integrated in ICT systems.

The good practice statements that underpin this tool are derived from generally accepted international standards and records management requirements[2]. The terminology used has in some cases been changed so that non-records and information specialists can easily interpret the statements of good practice and carry out an assessment using the indicators. Technical terms are defined in a glossary at Appendix C. Records management practitioners may also wish to consult a set of training materials, developed by the International Records Management Trust (IRMT), that provide both a conceptual framework and practical guidance on electronic records management. These are all available free to download from the IRMT's website, www.irmt.org.

The training materials are in five modules:

- *Understanding the Context of Electronic Records Management*
- *Planning and Managing an Electronic Records Management Programme*
- *Managing the Creation, Use and Disposition of Electronic Records*
- *Preserving Electronic Records*
- *Managing Personnel Records in an Electronic Environment.*

[2] These include: (1) Module 3, Guidelines and Functional Requirements for Records in Business Systems", ICA; Functional Specifications ... Business Information Systems Software", National Archives of Australia, December, 2006; (2) MoReq 2, *Model Requirements Specification for the Management of Electronic Records.* 2008; (3) ISO 15489: 2001: *Information and Documentation – Records Management;* (4) *The E-Records Readiness Tool*, International Records Management Trust, 2004.

3 Route Map

Two 'route maps' are included at the beginning of this document (Figures 1 and 2) as illustrations with this tool.

- The first, 'Designing a Records Management Improvement Programme', corresponds to the first category of good practice statements in this tool. It is concerned with the records management framework that must be in place to ensure good practices in the electronic environment. It outlines the core elements of a records management improvement programme, starting with the triggers that typically prompt the need for a programme. It indicates the need for an initial assessment and planning phase which is followed by the key components of the improvement programme itself. These components are supported by the two pillars: a legal and accountability framework for records management and the capacity to carry out the programme.

- The second route map, 'Integrating Records Management in the Systems Development Life Cycle', focuses on the second category of good practice statements in this tool. It may be used in combination with the first or on its own. Again, it starts with the triggers that signal the need to strengthen the integration of records management in ICT systems and then continues though the systems development life cycle, outlining the core activities at each stage.

4 Organisation of the Tool

The tool[3] is designed to measure the strengths and weaknesses of records management integration in three separate categories:

- the laws, policies, governance, strategies and evaluation mechanisms that must be in place to provide a compliance framework to ensure records management requirements are included in ICT systems

- the integration of records management requirements in ICT systems during the systems development life cycle[4]

- the capability of an existing ICT system to meet record management requirements.

[3] The tool is based broadly on a model developed by the Economic Policy and Debt Management Department of the World Bank, the *Debt Management Performance Tool (DeMPA)*. However, the format and methodology has been adapted to provide a performance assessment that may be applied in a shorter timeframe by non-specialists.

[4] A particular system development model has been used as the basis for identifying the phases of the system development life cycle. However, other system development models may be used. The essential characteristic is that they follow the broadly common sequence of project initiation, planning, development of design specifications and functional requirements, implementation, review and evaluation.

While the tool does not address in detail the broader requirements for an overall records management programme, it recognises that there must be a framework of records management policies, strategies and responsibilities within which records management integration takes place.

Records management in ICT systems must be governed by the same organisational policies and accountabilities as records management in all other forms, including paper filing systems and records created and held by office systems (email, correspondence, memoranda, reports, spreadsheets, etc). The good practice statements can be used for a high-level assessment of the legal, policy and accountability framework that supports all forms of records management.

The statements of good practice and their corresponding indicators are organised in three categories.

1 *Records Management Framework*: A framework must be in place to ensure that recordkeeping is taken into account when designing and implementing ICT systems. The category is subdivided as follows:

- legal and policy framework
- management structure
- records management strategy
- evaluation and audit.

2 *Integrating Records Management in the Systems Development Life Cycle*: This category is based on the premise that the integration of recordkeeping functionality in ICT systems is best accomplished in the context of system planning, design, testing, implementation and review. The sub-categories are:

- project initiation
- planning
- requirements analysis
- design
- implementation
- maintenance
- review and evaluation.

3 *Integrating Records Management Functionality in ICT Systems:* This addresses the extent to which records management has been integrated in existing ICT systems. It considers what the system must do to support the creation, organisation, use, retention and final disposition of records. The sub-categories are:

- creating and capturing records
- managing and maintaining records
- managing hybrid records
- searching, accessing and retrieving records
- retaining and disposing of records.

5 Users of the Tool

Users will include:

- records managers, or those with responsibility for records and information resources in their organisation
- IT staff/advisers and other information specialists who have little exposure to records management issues
- business managers who understand the need for records management but have limited knowledge of the issues
- officials responsible for approving ICT systems, allocating resources, overseeing progress and reviewing evaluations and audits
- development specialists and advisers.

Records and information managers will find the tool useful not only in assessing systems for compliance with records management requirements, but also in making the case for an organisation-wide approach to records management that takes account of both manual and electronic systems.

ICT specialists may use this tool to inform themselves of records management requirements and to ensure compliance with the recognised good practices that maintain data integrity and enable the preservation of essential records through time.

Senior officials with responsibility for information management issues in their organisation may use the tool to highlight the strengths and weaknesses of the records management environment in their organisations.

Donor or lender funded missions responsible for assessing the planning for, or success of, ICT systems and e-government initiatives may also find this tool useful.

In practice, however, the primary audience is likely to be multi-disciplinary teams assembled to plan, design and implement ICT systems in their organisations (whether a ministry, agency or the whole of government). The teams should include IT, legal, records management and information security specialists, as well as the managers responsible for business functions and processes supported by ICT systems. Ideally, such teams should be led by a senior official who appreciates the importance of records management in supporting the successful delivery of functions and services.

6 Scope of the Tool

The tool is intended for use in the ICT systems environments in the public sector. An ICT system is defined as a coherent collection of processes, people and technologies brought together to serve one or multiple business purposes. Typically, the records used as input for, or generated by, these systems can exist in multiple formats: for example, they may be created electronically, they may originate as paper or they may be digitised, that is, converted from paper to electronic records. The systems themselves may rely on a mixture of paper, digitised and 'born-electronic' records. An additional requirement, therefore, may be to manage records in multiple formats as an integrated whole.

The tool is aimed specifically at assessing 'specialist' application systems (such as human resources, financial management or case management systems). However, it may also be used for assessing the design and operation of applications such as enterprise content management systems that are intended to manage unstructured electronic records (emails, word-processed documents, spreadsheets, etc) in compliance with records management standards.

The development of ICT systems should normally proceed through a series of structured steps based on the use of generally accepted tools and techniques used in systems development. These steps address each stage of the systems development life cycle, from planning and design to implementation and review, and records management issues should be addressed as part of each stage.

ICT systems are normally mapped against and support particular business processes. Records, as the product of transactions, are part of a business process (for example, the processing of an application for a licence results in the creation of a licence and a record of the licence being issued). The integration of recordkeeping functionality in ICT systems should be undertaken, therefore, from the perspective of the business process. Business processes that are highly structured, with well defined points at which records are generated or captured, have the greatest potential for integration with good records management.

The tool does not attempt to address records management integration where business processes and workflow are poorly defined. This is frequently the case in organisations

where business and communications are conducted electronically through email, the web, desktop computers and networked information systems, where there are inadequate corporate standards and procedures for managing records or where there is a lack of compliance. In these environments, individuals may have a high level of autonomy in deciding what information they create and share, how they share it, where they hold it, how they organise, describe and retain it, and how long they keep it. In the unstructured electronic environment, it is almost impossible to comply with good records management practices. In addition, there may be a lack of defined business processes for creating records, an absence of technologies capable of supporting records management requirements, and a lack of standards, tools and techniques for designing and developing systems.

7 Attributes of Records

The good practices defined in this tool are consistent with the International Standard for Records Management (ISO 15489). To comply with the standard, an organisation must have in place policies, procedures and practices to ensure that its needs for documentary evidence are met, and that the organisation can be accountable for its activities. The objective is to create and manage records that are authentic, reliable, complete, unaltered and useable[5]. The effective integration of records management policies and practices into the design of ICT systems should result in records, regardless of their physical form, that are capable of reflecting the attributes described below.

Authentic: The record can be proven to:

- be what it purports to be
- has been created or sent by the person purported to have created or sent it
- has been created or sent at the time purported.

To ensure the authenticity of records, organisations should implement and document policies and procedures that control the creation, receipt, transmission, maintenance and disposition of records to ensure that records. Policies and procedures should ensure that creators are authorised and identified and that records are protected against unauthorised addition, deletion, alteration, use and concealment.

Reliable: The content of a record can be trusted as a full and accurate representation of the transactions, activities or facts to which it attests; the record can be depended upon in the course of subsequent transactions or activities. Records should be created at the time of the transaction or incident to which they relate, or soon afterwards, by individuals who have direct knowledge of the facts or by instruments routinely used within the business to conduct the transaction.

[5] ISO 15489: 2001: *Information and Documentation – Records Management*. Part 1: General, sections 6.1-6.2 and 7.2, pp.5 and 7.

Complete and Unaltered: The integrity of a record refers to its being complete and unaltered. Records should be protected against unauthorised alteration. Records management policies and procedures should specify what additions or annotations may be made to a record after it is created, under what circumstances additions or annotations may be authorised, and who is authorised to make them. Any authorised annotation, addition or deletion should be explicitly indicated and traceable.

Useable: A useable record is one that can be located, retrieved, presented and interpreted. It should be possible to demonstrate a direct connection to the business activity or transaction that produced it. The contextual linkages of records should carry the information needed to understand the transactions that created them and how they were used. It should be possible to identify a record within the context of broader business activities and functions. The links between the records documenting a sequence of activities should be maintained.

In summary, the ultimate goal of integrating records management in ICT systems is to enable the systems to generate and manage records that are capable of serving two primary roles:

- They should serve as a source of trusted and contextualised information that can be used to support business functions and decision-making.

- They should be capable of serving as instruments of accountability by providing accurate and reliable evidence of actions and transactions.

The attributes of records, as defined by international standards, are generic to any records environment whether paper based, electronic or a combination of both. The attributes must be respected if the records generated or held in such systems are to be captured, used and maintained as authentic and reliable records through time.

8 How to Use the Tool

Section 10 of this tool includes a set of indicators that organisations can use to assess the extent to which good practices in records management are integrated in their ICT systems and management structures. The tool does not attempt to assess whether every good practice is in place. Rather, indicators have been selectively drawn from the good practice statements so that users of the tool can carry out an assessment within a reasonably short period of time and with limited manpower resources. A full set of good practice statements is provided in Section 11.

Each good practice statement is numbered individually and this number is used to identify the statements in Section 10. Because Section 10 does not include all good practice statements, users of this tool will note that there are gaps in the numbering system in Section 10. Users who wish to conduct a more extensive assessment using more good practice statements can design additional indicators and means of verification as needed. It

is recommended that additional indicators are designed with the help of records management specialists.

Section 10 is organised as a four-column table as follows.

Good practice statement	Indicator	Means of Verification	Level

Each good practice statement has a corresponding indicator, a means of verifying that the good practice is in place, and a level (A, B or C) which enables a simple scoring system to be applied. The scoring system provides a means of making comparisons between systems within the same organisation and between organisations.

The set of indicators used is intended to provide a comprehensive assessment that covers all the main components of records management. All the indicators and their means of verification have been designed to be easy to assess and measure. Though simplified in some cases so that they can be understood by users who are not records or information specialists, the indicators are consistent with international standards and requirements for records management.

The indicators have been designed to be robust, objective and difficult to manipulate. The same results should be found by any two assessors. The indicators have been developed following the 'SMART' methodology; the indicators are:

- **S**pecific
- **M**easurable
- **A**chievable
- **R**elevant
- **T**ime-bound.

The aim in measuring records management integration is not to conduct an audit at the individual record or transaction level in ICT systems, but to assess the extent to which necessary policies and practices are in place. By assessing strengths and weaknesses against the statements of good practice, those areas that need improvement can be identified. This will help guide future planning so that records management can be integrated in ICT systems design through a process of targeted improvements over time.

9 Scoring

A simple scoring system is applied to the indicators so that overall performance in particular areas can be assessed. Each indicator has been assigned a level of A, B or C in the far right

column of the table in Section 10. These three letters represent different levels of achievement:

- 'A' is the highest level and indicates that the most demanding and rigorous good practice requirements are met
- 'B' represents attainment of an intermediate level of good practice requirements
- 'C' indicates that the basic good practice requirements are achieved.

A Score Sheet and Scoring Table are included at Appendix A to help with scoring and analysis. Level D has been added to the Score Sheet to indicate that overall the basic good practice requirements, that is Level C, have not been met.

Total scores for each indicator category should be compared with the Scoring Table to determine which level overall (A, B, C or D) has been achieved for each of the three indicator categories. The overall level may then be checked against Performance Statements in Appendix B to provide a statement of the current state of records management integration. The Performance Statements may be used as a basis for reporting on an assessment exercise using this tool.

Example 1:

A score of seven in Category One (Records Management Framework) indicates:

Level C: Some or all of the necessary laws, policies and governance strategies are in place in the organisation. There is some evidence of implementation and use of these laws, policies and governance strategies. The organisation therefore meets the basic good practice requirements for integrating records management in ICT systems in this area. However, some key components of the records management framework are missing and there is little evidence that there are mechanisms to ensure compliance, review and updating of the records management framework. To improve records management integration, it will be necessary to identify where new laws, policies or strategies are needed or require updating and to promote and measure compliance with a records management framework.

Example 2:

A score of eleven in Category Three (Integrating Records Management Functionality in ICT Systems) indicates:

Level B: The system meets the majority of the necessary functional capabilities for the capture, organisation, use, retention and disposition of records. There is evidence that the system has the functionality to meet particular areas of good practice including, for example, the creation of rules to control the selection of metadata, the management of hybrid records, the central management of access controls or the creation and maintenance of an audit trail. To improve recordkeeping integration, it will be necessary to further develop mechanisms to ensure that the findings of system audits are acted upon and are used to enhance system functionality and performance.

10 INDICATORS

Category 1: Records Management Framework

The integration of records management requirements in ICT systems does not happen on its own. It must be supported by:

- senior officials, managers and staff who understand the importance of records management in supporting government operations
- standards, practices, and technologies that facilitate records management through the records life cycle
- specialists who know how to achieve good records management practices.

However, these key elements alone do not enable records management requirements to be met. There must also be a top-level framework consisting of laws, policies, management and planning structures, strategic objectives and evaluation mechanisms to achieve good records management practices.

1.1 Legal and Policy Framework

The integration of records management in ICT systems must be authorised. Authorisation should normally be obtained through a formal approval process and derived from a law, ordinance, regulation or policy. In some cases the authorisation will be explicit (eg, an organisation-wide policy states that all ICT systems will account for records management requirements). In other cases it may be implicit (eg, a law, or regulations issued under the law, stipulate that financial information must be capable of being authenticated and must be complete and accurate). In some organisations, laws and regulations prescribe general requirements, leaving more detailed requirements, such as those related to implementation, to policies.

GOOD PRACTICE STATEMENT[6]	INDICATOR	MEANS OF VERIFICATION	LEVEL
1.1.1 Laws, regulations and/or organisation-wide policies are in place to govern the management of records (including records generated in ICT systems) throughout their life cycle from creation to final disposition.	i. There is a legal mandate/policy for records management with which the organisation must comply. *and* ii. The legal mandate/policy covers records in all formats.	Legal mandate or government-endorsed policy for records management, or relevant extract.	**C**
1.1.2 Laws, regulations and/or policies enable the development and issue of standards and guidelines on the management of records.	The legal mandate/policy provides a framework for developing and issuing standards, guidelines and procedures for records management throughout the organisation.	Relevant extract from legal mandate or government-endorsed policy.	**C**
1.1.4 A central authority or agency is assigned responsibility for overseeing the integration of records management in ICT systems (for example, in a law, regulation or organisation-wide policy).	There is a legal mandate/policy enabling a central authority to oversee the implementation of standards or guidelines for integrating records management in ICT systems.	Relevant extract from legal mandate or government-endorsed policy.	**A**

[6] Numbers in this column refer to the sequential number in the full list of Good Practice Statements in Section 10.

GOOD PRACTICE STATEMENT[6]	INDICATOR	MEANS OF VERIFICATION	LEVEL
1.1.5 Laws, regulations or policies are in place which enable the establishment of audit and evaluation processes for measuring the effectiveness of records management practices.	There is a legal mandate/policy for auditing and evaluating records management practices.	Relevant extract from legal mandate or government-endorsed policy.	**C**
1.1.6 Laws, regulations or policies are in place which include provision for the establishment of audit or evaluation processes to measure the effectiveness of records management in ICT systems.	There is a legal mandate/policy requiring the audit and evaluation of records management practices in ICT systems.	Relevant extract from legal mandate or government-endorsed policy.	**B**
1.1.7 Policies, standards or guidelines are in place requiring that: • records management is integrated in ICT systems. • records generated in ICT systems are managed according to records management standards. • the effectiveness of records management integration is assessed regularly.	There are policies, standards or guidelines for integrating records management in ICT systems.	Documented policies, standards or guidelines, or relevant extracts.	**B**

1.2 Managerial Structure (or Records Management Responsibility and Competence)

Integrating records management in ICT systems requires planning, management and resources. There must be people involved with the authority to act and who have the tools and resources needed to establish strategies and plans for integrating of records management in ICT systems. Records management responsibilities must be assigned and skills available across the organisation to support the integration of records management in multiple systems. In addition, corporate-level policies and resource planning will be involved. The management structure established for records management integration must be capable of addressing both strategic and operational needs.

GOOD PRACTICE STATEMENT		INDICATOR	MEANS OF VERIFICATION	LEVEL
1.2.4	Responsibility for records generated by all the business functions and processes of the organisation is assigned to a designated role or office.	There is a designated member of staff in each major functional area of the organisation who is responsible for the operational management of that area's records regardless of the format, structure or medium in which the records are created and kept.	Documented evidence of employment of designated members of staff (organisational chart, job descriptions, etc.)	**C**
1.2.5	At least one member of staff who is assigned responsibility for managing the organisation's records possesses appropriate skills and knowledge.	Designated members of staff possess graduate or post-graduate degrees in archives, records or information management from an accredited institution.	Documented evidence of qualifications.	**B**

GOOD PRACTICE STATEMENT	INDICATOR	MEANS OF VERIFICATION	LEVEL
1.2.6 An official in the organisation has authority to: • provide direction on records management integration at all levels of the organisation • allocate resources to records management integration strategies, plans and initiatives • facilitate the processes of records management integration in cooperation with others (eg, IT managers, business managers)	Job descriptions for designated members of staff include defined responsibilities for the integration of records management in ICT systems.	Documented job descriptions.	**A**
1.2.7 Standards and procedures are in place for records management in the organisation that apply to all records, regardless of format.	There are standards and procedures for records management in all formats including paper, electronic and digital.	Documented standards and procedures or relevant extracts.	**C**
1.2.8 Standards and procedures are in place for integrating records management in ICT systems.	There are standards and procedures for integrating records management in ICT systems.	Documented standards and procedures or relevant extracts.	**A**

1.3 Records Management Strategy

The introduction of ICT systems should be based on a strategy that defines objectives, governance and implementation structures, and mechanisms for identifying needs and measuring performance. It is therefore essential to document why ICT systems are required, how, when and by whom they should be implemented, how much they will cost and how they will be evaluated. Similarly, there is a need to document why records management integration is required; the risks if integration is not done; how, when and by whom the integration is to be undertaken; how much it will cost; and how it will be evaluated. The integration strategy needs to be aligned with the overall ICT and business objectives as set within the organisation's strategic planning framework.

The strategy development process should include consultation with key stakeholders and should be approved at the highest levels of the organisation. The document describing the strategy for integrating records management should include descriptions of:

- the current and future environment for the business of the organisation and ICT systems; assumptions will need to be made about the characteristics of that environment from a records management perspective
- the future end state or vision for records management in ICT systems
- the risks if records management is not integrated in ICT systems (and how these risks can be mitigated)
- the analysis needed to support a recommended records management strategy, including the concepts, roles, and the assumptions used
- the recommended strategy and its rationale, with targets over a projected time period and estimated costs.

The strategy should be reviewed periodically to assess whether the assumptions still hold in light of changing circumstances. A review should be undertaken ideally annually, but at least every five years, in conjunction with an overall review and evaluation of ICT systems, preferably as part of the budget and ICT planning processes.

GOOD PRACTICE STATEMENT	INDICATOR	MEANS OF VERIFICATION	LEVEL
1.3.1 An organisation-wide records management strategy is in place which is consistent with international standards.	i. There is an organisation-wide records/information management strategy *and* ii. The strategy has been issued or endorsed at the highest decision making level *and* iii. The strategy is consistent with ISO 15489:2001 (International Standard, Information and Documentation - Records Management).	Documented records or information management strategy or equivalent document.	**C**
1.3.3 A plan is in place describing the organisation's strategy for integrating records management in its ICT systems.	The organisation-wide records/information management strategy includes a specific objective to integrate records management in ICT systems	Documented records or information management strategy or equivalent document or relevant extracts.	**B**
1.3.5 A mechanism is in place to ensure the strategic plan is regularly reviewed and updated as needed.	The strategic plan is reviewed and updated within five years of implementation. There is a mechanism in place to ensure that it is reviewed at least every five years.	Documentary evidence of mechanism for review and updating.	**B**

1.4 Evaluation and Audit

As well as ensuring that there is a legal and policy framework, a management structure and a records management strategy, it is necessary to measure the extent to which records management integration is taking place and to assess the quality of the integration. There should be performance measures and evaluation or audit mechanisms to help the organisation measure objectively, at any point in time, how well the integration activity has been undertaken and whether it meets (and continues to meet) predefined outcomes.

The requirements for evaluating and auditing the integration of records management in ICT systems are as follows:

GOOD PRACTICE STATEMENT	INDICATOR	MEANS OF VERIFICATION	LEVEL
1.4.1 Audit and evaluation mechanisms are in place to assess the effectiveness of integrating records management in ICT systems. These may be either stand-alone or incorporated in the audit and evaluation mechanisms for assessing ICT systems.	Responsibility for auditing and evaluating records management integration in ICT systems is assigned to a designated member of staff or body.	Documentary evidence of relevant responsibility of designated member of staff or body (eg, organisational chart, job description, etc).	**C**
1.4.2 Tools are in place for assessing the effectiveness of records management integration in ICT systems.	The organisation has specific tools for auditing and evaluating records management integration in ICT systems.	Copies of audit and evaluation tools.	**B**
1.4.3 Audits or evaluations are carried out regularly to assess the effectiveness of records management integration in ICT systems.	An audit or evaluation has been carried out in the last 12 months.	Report(s) of audit or other evidence of audit programme.	**A**

GOOD PRACTICE STATEMENT		INDICATOR	MEANS OF VERIFICATION	LEVEL
1.4.5	Mechanisms are in place to enable the findings of audits and evaluations to be used to improve the overall records management function as well as ICT development in the organisation.	i The last conducted records management integration audit or evaluation has been signed off by senior management *and* ii A list of senior management recommendations and next steps has been documented.	Report(s) of audit; management reports identifying records management and ICT development improvements.	A

Category 2: Integrating Records Management in the Systems Development Life Cycle (SDLC)

ICT systems are normally developed through a series of phases that begin with project initiation and planning, continue with the development of design specifications and functional requirements, and conclude with the implementation of the system as well as its review and evaluation. If records management is to be integrated in the design of ICT systems, and the system itself is to ensure data integrity, it is essential that records management considerations are addressed at every phase of the systems development life cycle. Records management requirements cannot simply be added on at a later stage. They must be built in as essential components of the system, starting with project initiation and being mainstreamed into the design and implementation stages. Records management integration must also be aligned with, and supported by, the records management framework described in Category 1.

During the initiation and planning phases, records management issues are identified and confirmed, and resource requirements for records management integration are defined. If a decision is made to tender all or parts of the ICT systems project, records management issues to be addressed by potential contractors will need to be identified during the initiation and planning stages. For example, what are the 'records' that will need to be created or held by the ICT system? What are the relationships between other paper or electronic records management systems on which the business processes will depend?

2.1 Project Initiation

The initiation phase of the systems development life cycle begins when management determines a business process or function needs to be enhanced through the application of information technology. The purpose of the initiation phase is to:

- identify and validate an opportunity to improve business functions and processes or address a deficiency related to a business need
- identify significant assumptions and constraints on solutions
- recommend the exploration of alternatives to satisfy the need.

ICT projects may be initiated as a result of business process improvements, changes in business functions or advances in information technology. They may also arise from external drivers such laws and policies, new strategic directions or opportunities presented by external organisations (eg, technical assistance and development agencies). The sponsor for the ICT systems project (eg, a business manager) normally articulates this need within the organisation and initiates the systems/project life cycle. Then a project manager is appointed who prepares a statement of need or concept proposal.

Decisions about which parts of the ICT project will be supported by contractors outside the organisation are made during this phase. For example, a specific component of the project, the requirements analysis, implementation or overall management of the project may be tendered. High level records management considerations should be addressed as part of this decision-making process. These include, for example, information security and records management issues (eg, ensuring records' authenticity through time, setting retention rules for records, linking paper and electronic records, identifying vital records and disaster planning and recovery). 'Ownership' of the issues should also be identified so that they can be addressed as the project proceeds.

A project manager normally brings together all stakeholders who need to contribute to the development effort. This must include people who can address records management issues and records management integration in the design of the system. The outcome of this phase is a concept proposal (or similar document) and a project charter that assigns responsibility for delivering the project.

GOOD PRACTICE STATEMENT		INDICATOR	MEANS OF VERIFICATION	LEVEL
2.1.1	Records management issues are identified and documented when the need for an ICT system is identified and documented.	Records management issues have been identified and documented.	Project initiation document or relevant extract.	C
2.1.9	A governance structure (such as a project steering committee) is in place to ensure the collaboration of key individuals in planning, designing and developing the system, including the application system manager, project manager, systems developers and records managers.	Record managers are represented within the governance structure for the ICT system and are part of the planning, design and development of the system.	Documented governance structure.	C

2.2 Planning

During this phase the business need and proposed concept for the system are analysed in detail. A 'vision' is developed of how the business will operate once the approved system is implemented. Potential solutions are analysed. Risks are assessed including, for example, those associated with preserving records over time, and recovering records in a useable form in the event of a disaster. Resources, activities, schedules and tendering processes are defined. Other high level requirements, such as those for security and records management are refined based on threat and risk assessments.

GOOD PRACTICE STATEMENT	INDICATOR	MEANS OF VERIFICATION	LEVEL
2.2.1 The analysis of business needs includes records management issues; potential solutions incorporate records management considerations.	i A business needs analysis has been carried out *and* ii The analysis includes a consideration of records management issues.	Business needs analysis or relevant extract.	**B**
2.2.2 In assessing risks associated with the potential solutions, risks associated with records management are also taken into account.	Risks associated with records management in the potential solutions have been assessed and documented.	Risk assessment document or relevant extract.	**B**

2.3 Requirements Analysis

This phase emphasises determining what functions must be performed rather than technically how those functions are performed. Functional user requirements are formally defined and specified in terms of inputs, processes, outputs, interfaces, system performance and system maintainability. At the same time, functional requirements for records management are defined and integrated as part of the wider functional

requirements of the system. All requirements, including records management requirements need to be defined to a level of detail sufficient to support systems design in the next phase. All requirements should also be capable of being measured and tested, and they should relate to the business need or opportunity identified in the Initiation Phase.

GOOD PRACTICE STATEMENT	INDICATOR	MEANS OF VERIFICATION	LEVEL
2.3.1 An analysis has been conducted of the records management requirements for the ICT system based on the records management issues identified during the planning stages.	An analysis of the records management requirements of the ICT system has been conducted and documented.	Records management requirements document or overall requirements document incorporating records management requirements.	C
2.3.4 The analysis of records management requirements for the ICT system makes reference to internationally recognised standards.	The analysis makes reference to international records management standards or other internationally recognised sets of requirements (eg, ISO 15489, MoReq, DoD 5015, DIRKS, etc).	Relevant extracts from requirements document.	B

2.4 Design

During this phase, the physical characteristics of the system are specified and a detailed design is prepared. The operating environment is established and major sub-systems are defined to create a detailed structure of the system. Everything requiring user input or approval is documented and reviewed by users.

The design stage must account for the functional requirements for records management and other related requirements (eg, legal, management, procedural, technical and disaster recovery) identified as a result of the previous 'requirements analysis' phase. Recordkeeping

design specifications should be woven seamlessly into the physical and logical design specifications for the system (ie, data architectures, data models, process models, etc).

GOOD PRACTICE STATEMENT	INDICATOR	MEANS OF VERIFICATION	LEVEL
2.4.2 The points in the process where records are expected to be generated and captured are defined and reflected in the functional requirements of the ICT system.	All transactions that result in the creation of records with the ICT system have been defined and documented.	Documented rules for the creation and capture of records.	**C**
2.4.13 Performance measures are developed for assessing the records management performance of the ICT system.	Performance measures are in place to assess the ability of the system to meet records management requirements.	Documented performance measures.	**B**
2.4.16 The system creates an audit trail that keeps a complete history of the creation, use and retention of all records within the system.	The system creates an audit trail to provide a complete record of the creation, use and retention of records within the system.	View system in operation; copy of system documentation.	**C**
2.4.18 Performance measures are carried out regularly to assess the ability of the system to meet records management requirements.	The system's records management performance has been assessed within the last 12 months.	Documented performance assessment(s).	**A**

GOOD PRACTICE STATEMENT	INDICATOR	MEANS OF VERIFICATION	LEVEL
2.4.19 A designated member of staff has been assigned responsibility for monitoring the system audit trail.	Responsibility for monitoring the system audit trail is documented and assigned to a designated member of staff.	System administrator manuals or relevant extracts; job descriptions of system administrators.	**B**
2.4.20 The audit trail is analysed regularly to monitor access to the system, changes to access and security controls, and the integrity of records within the system	The system audit trail has been analysed within the last 12 months.	Documented analysis of audit records.	**A**

2.5 Implementation

The Implementation Phase translates the system design produced in the Design Phase into a working system capable of addressing system requirements. The development phase includes activities for building and testing the system to ensure that it satisfies the defined functional requirements. Regardless of whether these activities are carried out 'in-house' or by contracted resources, the results require signoffs by appropriate officials and, in the case of records management issues, by records specialists.

Several types of tests are conducted in this phase. System tests should be conducted and evaluated to ensure the developed system meets all technical requirements, including performance requirements. Tests to assess the capability of the system to capture and maintain records (in accordance with the functional requirements) should be conducted and should form part of the overall testing and assessment process. Tests focusing on data integrity from a security and records management perspective should validate the system's capacity to respect requirements for the authenticity, reliability and completeness of records. Finally, users should participate in acceptance testing to confirm that the developed system meets all user requirements, including those for access and retrieval.

Once the system is accepted it moves into 'production' mode. End users are formally notified of implementation, training is conducted and data entry or conversion is undertaken.

GOOD PRACTICE STATEMENT	INDICATOR	MEANS OF VERIFICATION	LEVEL
2.5.1 The developed system has been tested for its records management performance against technical, management and functional records management requirements (see 2.3.2). Testing included a 'live' test in an operational context. An acceptance test has been conducted to confirm that the system meets records management requirements.	Acceptance tests have been carried out for records management requirements; acceptance tests for records management requirements may be separate or incorporated in acceptance tests for the whole system.	Acceptance test reports or relevant extracts from acceptance test reports.	C

2.6 Maintenance

During this phase the system is monitored for continued performance in accordance with user requirements. System modifications are incorporated as needed. The performance of any contractors responsible for maintaining the system is reviewed on a regular basis and contract agreements are updated to reflect changes in requirements. The system is periodically assessed to determine how it can be made more efficient and effective.

Changes to records management requirements (resulting, for example, from new laws, changing business requirements or changes in business processes) must be accommodated in the monitoring and change process activities undertaken during the Maintenance Phase.

Providing user support is an ongoing activity. New users will require training. Other training may be needed, such as refresher and more advanced training, or training in new processes. The emphasis of this phase is to ensure that the users' needs are met and that the system continues to perform to the required standard. When modifications or changes are identified as necessary, including those that impact on records management, the system development life cycle may need to be re-applied.

If the system is terminated, steps must be taken to preserve the vital information about the system so that some or all of the information (including information in records) can be reactivated or accessed in the future. Where valuable records are migrated to other systems (including those supported by an archive) records management regulations and policies must be followed.

GOOD PRACTICE STATEMENT		INDICATOR	MEANS OF VERIFICATION	LEVEL
2.6.1	Mechanisms have been established to assess system compliance with records management requirements through time.	There is a documented mechanism for assessing the system for compliance with records management requirements; compliance assessment for records management requirements may be separate or incorporated in compliance assessment for the whole system.	Compliance assessment document or relevant extracts.	**C**
2.6.4	Assessments for system compliance with records management requirements are regularly carried out.	An assessment for records management compliance has been carried out in the last 12 months.	Report of assessment of records management compliance.	**A**

2.7 Review and Evaluation

Review and evaluation of the system occurs from two perspectives. Firstly, 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 (including those related to records management). These 'in-process' reviews must be supported by agreed performance measures and assessment methods. For example, the capability of the system to generate, capture and manage records must be evaluated against records management performance measures.

Secondly, the methodology used to develop the systems must be evaluated. How well did it work in this systems development project? Is the tendering process effective in terms of its ability to integrate records management in the ICT system? Again, records management considerations, including performance measures and other criteria, must be developed and integrated in the tools and techniques employed to assess ICT systems development.

	GOOD PRACTICE STATEMENT	INDICATOR	MEANS OF VERIFICATION	LEVEL
2.7.1	There are performance standards to assess whether the ICT system meets records management requirements, for example in relation to records security, data quality and data completeness. These may be separate records management standards or systems standards that include records management standards. The standards should be related to records management requirements (see 2.3.1).	There are documented performance standards to measure whether the ICT system meets records management requirements.	Documented performance standards.	**B**

GOOD PRACTICE STATEMENT		INDICATOR	MEANS OF VERIFICATION	LEVEL
2.7.3	Performance assessments are conducted to assess the system's compliance with records management standards.	A performance assessment has been carried out to assess the system's compliance with records management standards within the last 12 months.	Performance assessment report(s) or copy of performance assessment programme.	A

Category 3: Integrating Records Management Functionality in ICT Systems

Properly implemented, an ICT system that has integrated records management will permit the capture, organisation, use, retention, and disposition of records. The ICT system must operate within a trusted environment that supports the organisation's business and information while respecting organisation-wide records management policies and practices.

Good practice statements in this category are expressed as functional requirements. The generic requirements that follow[7] complement the 'records management framework' requirements in Category 1. They also complement the requirements for records management integration in the systems development life cycle (Category 2) and should be addressed during each phase of the systems development life cycle.

The requirements are expressed as what the ICT system must have the capability of doing: the business processes the ICT system supports must generate authentic, reliable, complete and usable records that can be managed through their life cycle.

However good its functionality, no system can be successfully implemented unless all technical, user and other procedures are defined, documented and followed. The following requirements assume that in each case, an implemented system must have such documentation. Some of the indicators will assess the presence, use and audit of documented procedures.

[7] The functional requirements described in this section are derived from: a pre-publication draft of "Principles and Functional Requirements for Records in Electronic Office Environments, Module 3, Guidelines and Functional Requirements for Records in Business Systems", International Council on Archives, June, 2008; and, "Functional Specifications for Recordkeeping Functionality in Business Information Systems Software", National Archives of Australia, December, 2006.

3.1 Creating and Capturing Records

Records must provide evidence of the actions and transactions that generated them, and they must serve as a trusted source for future decision making and information needs. If records are to serve these purposes, the ICT system must incorporate defined rules and processes for creating and capturing records. For example, where in the business process will a record need to be created and what information about the record must be captured along with the record's content itself?

Records must have certain attributes: they must be authentic, complete and usable. In order to ensure that they have these attributes, the ICT system must have the capability to generate or capture the required 'metadata'. The preservation of the record with its associated metadata is necessary to maintain the integrity of the record through time. The metadata gives individual records their context within the business process that generated them, and it links the records together so that they can serve their purpose in documenting individual cases within the business process.

GOOD PRACTICE STATEMENT	INDICATOR	MEANS OF VERIFICATION	LEVEL
The system must be capable of:			
3.1.3 Assigning unique identifiers to the records that will remain unchanged as long as the records exist.	It is not possible to assign the same number to two records.	Test system by attempting to assign the same number to two records.	C
3.1.6 Supporting and applying security and access controls during the process of capturing records to ensure that the records are protected from unauthorised access, alteration and destruction/deletion.	Access controls are automatically or manually assigned to complete the creation and capture of a record.	View system in operation to confirm access controls are assigned to newly created records.	C

3.2 Managing and Maintaining Records

Once records are created and captured, they must be maintained in such a way that their attributes of authenticity, reliability, completeness and usability are preserved for as long as the records are needed to serve the organisation's business needs, and to meet accountability requirements prescribed by law or policy. They must be organised, classified and described in a manner that facilitates their access and retrieval, and they must be protected to ensure that they are secure from unwarranted alteration and destruction.

GOOD PRACTICE STATEMENT	INDICATOR	MEANS OF VERIFICATION	LEVEL
The system must be capable of:			
3.2.2 Validating metadata, for example against a range of pre-defined values such as a classification scheme.	The system is designed to control the selection of metadata from pre-defined values (eg, in relation to classification of records).	Documented procedures or screen shots for creating or entering metadata values.	**B**
3.2.3 Creating rules to control the selection of metadata.	The system has the functionality to create rules to control the selection of metadata (eg, in relation to classification of records).	Documented procedures or screen shots to show that some metadata is selected from a pre-defined range of values.	**B**

GOOD PRACTICE STATEMENT	INDICATOR	MEANS OF VERIFICATION	LEVEL
3.2.6 Assigning appropriate retention and disposition rules to records during record creation.	To complete the creation and capture of a record, a retention rule must be assigned.	Test system by attempting to complete the creation or capture of a record without assigning a retention rule from a pre-defined set of values, or by initiating a process that will lead to the assignment of a retention rule.	**B**
3.2.14 Creating and maintaining an audit trail that tracks user access to records contained within or managed by the system	There is an audit trail that tracks access to the records contained within or managed by the system. Whenever a user accesses a record audit metadata is created. This audit metadata includes at least the date and time of access and the user's ID.	Test system by accessing a record and examining the resulting audit metadata.	**C**
3.2.15 Creating and maintaining an audit trail that tracks changes to records and record metadata.	The audit trail captures any changes made to records or metadata contained within or managed by the system.	Test system by changing a record and examining the resulting audit metadata.	**B**
3.2.16 Providing an easy method of checking the audit trails for changes to records and records' metadata within the system.	A system audit is carried out every six months. This audit examines the audit trail for any changes made to records and records' metadata.	Audit reports or copy of audit programme.	**A**

3.3 Managing Hybrid Records

ICT systems generate records in multiple forms. Some records may be in paper form (for example, a completed application form submitted by an individual), some may be in electronic form (for example, a verification notice indicating that the application is accepted and registered) and others may be in digitised form (for example, a scanned image of a letter of an educational qualification). In many cases ICT systems must also account for paper-based records generated as a result of an earlier manual system. If records are to be complete and if the complete 'evidence' of a set of transactions or case is to be maintained, links must be established between the electronic and related paper, digitised and other forms of records.

GOOD PRACTICE STATEMENT	INDICATOR	MEANS OF VERIFICATION	LEVEL
ICT systems that manage hybrid records must be capable of:			
3.3.5 Searching for and retrieving all physical, hybrid and digital records registered by the system.	System rules are consistent for physical, hybrid and digital records (eg, records are labelled or described for searching and retrieval purposes).	Documented rules or procedures.	**A**

3.4 Searching, Accessing and Retrieving Records

Information needs cannot be met unless the records can be accessed and used when needed. It must be possible to locate and retrieve records easily. It should be possible to narrow the search for a certain record or set of records out of the mass of records generated by the system. However, it may also be necessary to limit access to certain records because of different levels of security. The ability to search for, access and retrieve records will depend on the techniques used to organise and classify the records, but it will also depend on the performance of the system. The system must ensure that the right records are provided to the right person, at the right time, in the right format and at the right cost.

GOOD PRACTICE STATEMENT	INDICATOR	MEANS OF VERIFICATION	LEVEL
The system must be capable of:			
3.4.7 Retrieving and listing a set of digital records and associated metadata that meet the search criteria.	At least two criteria may be used to search for records in the same system, either using the record content or its metadata (eg, unique identification number, date of creation and capture, record type, user ID of creator).	Test system by searching and retrieving records using two different criteria	C
3.4.16 Restricting the definition and maintenance of access and security controls to an authorised system administrator.	Responsibility for managing access controls is assigned to a designated member of staff or office.	Documentary evidence of employment of designated office or member(s) of staff (organisational chart, job descriptions, etc.)	C
3.4.17 Supporting central management of access and security controls; applying these controls to users, records and associated metadata.	There are documented standards and procedures for applying system access controls.	Standards and procedures or relevant extracts.	B

3.5 Retaining and Disposing of Records

Records generated in ICT systems must be retained for as long as they are required to support business requirements. These may include:

- the need to provide evidence of a transaction or series of transactions
- the need to have authoritative and reliable information available to support decision-making, management reporting and accountability requirements.

Retention of records must also comply with relevant legislative and policy requirements concerning the length of time records must remain in existence.

Retention rules must consistent for all forms of records. For example, though they may be different, rules need to take account of the existence of electronic and paper versions of the same record. In order to ensure continued access, electronic records may have to be migrated to accommodate changes in the technology supporting ICT systems. Retention therefore needs to be planned for and integrated carefully into the design and ongoing management of ICT systems.

When records are due for disposition steps must be taken to ensure that they are deleted or destroyed properly (ie, electronic records are removed from all relevant databases, back-up tapes, etc) and that records of archival value are transferred systematically to the control of an archives in accordance with schedules and other agreements. Disposition can also include transfer of the records beyond the control of the organisation to some other jurisdiction, such as another government agency or the private sector. Transfer is normally accomplished through an agreement.

GOOD PRACTICE STATEMENT	INDICATOR	MEANS OF VERIFICATION	LEVEL
The system must be capable of:			
3.5.2 Providing backup for all records and the records' metadata within the system.	i. There is a daily backup of all system data *and* ii. The backup is stored externally from the main system.	Examine backup procedures.	**C**
3.5.4 Enabling an authorised individual to create, maintain, modify and manage retention and disposition rules.	A designated member of staff or office has documented responsibility for managing retention and disposition rules.	Documentary evidence of employment of designated office or member of staff (organisational chart, job descriptions, etc.).	**C**

GOOD PRACTICE STATEMENT		INDICATOR	MEANS OF VERIFICATION	LEVEL
3.5.8	Applying retention instructions to records and triggering the appropriate disposition event when the retention period expires.	There are documented policies and procedures for assigning retention and disposition instructions to records. .	Policies and procedures.	**B**
3.5.11	Creating an audit trail of records retention and disposition rules and actions; enabling an authorised individual to carry out regular audits.	There is a documented audit of records retention and disposition rules and actions at least every 12 months.	Audit report(s) or copy of audit programme.	**A**

11 GOOD PRACTICE STATEMENTS

What follows is a comprehensive list of good practice statements for integrating records management in ICT systems. Not all the statements are supported by indicators. Where an indicator has been provided, 'yes' has been inserted in the final column. All good practice statements that have associated indicators are listed in Section 10 of this tool.

Category 1. Records Management Framework

1.1	Legal and Policy Framework	INDICATOR
1.1.1	Laws, regulations and/or organisation-wide policies are in place to govern the management of records (including records generated in ICT systems) throughout their life cycle from creation to final disposition.	YES
1.1.2	Laws, regulations and/or policies enable the development and issue of standards and guidelines on the management of records.	YES
1.1.3	The legislative instruments and/or policies governing the development and management of business functions and processes require the effective creation, capture and management of records generated in ICT systems.	
1.1.4	A central authority or agency is assigned responsibility for overseeing the integration of records management in ICT systems (for example, in a law, regulation or organisation-wide policy).	YES
1.1.5	Laws, regulations or policies are in place which enable the establishment of audit and evaluation processes for measuring the effectiveness of records management practices	YES
1.1.6	Laws, regulations or policies are in place which include provision for the establishment of audit or evaluation processes to measure the effectiveness of records management in ICT systems.	YES
1.1.7	Policies, standards or guidelines are in place requiring that: • records management is integrated in ICT systems. • records generated in ICT systems are managed according to records management standards. • the effectiveness of records management integration is assessed regularly.	YES
1.1.8	Legislative instruments and/or organisation-wide policies that deal with information management (eg, data protection, security, access to information, specialised business systems) recognise the need for records management requirements to be addressed regardless of the records format.	

1.2	Management Structure	INDICATOR
1.2.1	Accountability for the integration of records management in ICT systems is assigned to specific agencies or offices.	
1.2.2	There are sufficient financial, human and other resources to plan, organise and control the integration of records management in ICT systems.	
1.2.3	There is an organisation-wide governance committee whose responsibilities include records management integration issues.	
1.2.4	Responsibility for records generated by all the business functions and processes of the organisation is assigned to a designated role or office.	YES
1.2.5	At least one member of staff who is assigned responsibility for managing the organisation's records possesses appropriate skills and knowledge.	YES
1.2.6	An official in the organisation has authority to: • provide direction on records management integration at all levels of the organisation • allocate resources to records management integration strategies, plans and initiatives • facilitate the processes of records management integration in cooperation with others (eg, IT managers, business managers).	YES
1.2.7	Standards and procedures are in place for records management in the organisation which apply to all records, regardless of format.	YES
1.2.8	Standards and procedures are in place for integrating records management in ICT systems.	YES
1.2.9	Programme managers and their staff, IT staff and records management specialists follow standards and procedures for integrating records management in ICT systems.	
1.2.10	A process is in place for approving new or modified standards and practices for integrating records management in ICT systems is in place.	
1.2.11	Specialists are in post who have the knowledge and skills required to integrate records management in ICT systems.	
1.2.12	Training, development or recruitment strategies are in place to fill any gap in the competencies required to integrate records management in ICT systems.	

1.2	Management Structure	INDICATOR
1.2.13	Performance assessment tools and techniques are used to review job performance as it relates to integrating records management in ICT systems.	

1.3	Records Management Strategy	INDICATOR
1.3.1	An organisation wide records management strategy is in place which is consistent with international standards.	YES
1.3.2	A process is in place to guide the development and approval of a strategic plan for integrating records management in ICT systems.	
1.3.3	A plan is in place describing the organisation's strategy for integrating records management in its ICT systems.	YES
1.3.4	The strategic plan for integrating records management in ICT systems is linked to or incorporated in the organisation's strategic ICT and business plans.	
1.3.5	A mechanism is in place to ensure the strategic plan is regularly reviewed and updated as needed.	YES

1.4	Evaluation and Audit	INDICATOR
1.4.1	Audit and evaluation mechanisms are in place to assess the effectiveness of integrating records management in ICT systems. These may be either stand-alone or incorporated in the audit and evaluation mechanisms for assessing ICT systems.	YES
1.4.2	Tools are in place for assessing the effectiveness of records management integration in ICT systems.	YES
1.4.3	Audits or evaluations are carried out regularly to assess the effectiveness of records management integration in ICT systems.	YES
1.4.4	The audit and evaluation process assesses and documents the organisation's performance in integrating records management in ICT systems and in ensuring that records are maintained and managed appropriately.	

1.4	Evaluation and Audit	INDICATOR
1.4.5	Mechanisms are in place to enable the findings of audits and evaluations to be used to improve the overall records management function as well as ICT development in the organisation.	YES

Category 2 Integrating Records Management in the Systems Development Life Cycle (SDLC)

2.1	Project Initiation	INDICATOR
2.1.1	Records management issues are identified and documented when the need for an ICT system is identified and documented.	YES
2.1.2	The benefits of integrating records management in the design of the ICT system have been identified in terms of risk reduction, cost avoidance, cost savings and opportunity gain.	
2.1.3	Senior management understands the records management issues and is prepared to support efforts to find solutions.	
2.1.4	Management approval of the development of a new ICT system must take account of the documented records management issues.	
2.1.5	The funding strategy for the planned ICT system includes funding to address the records management issues.	
2.1.6	The budget established for the ICT system (including funds allocated to tendering all or parts of the project) covers the integration of records management in the design and implementation of the system	
2.1.7	The terms of reference for the planned ICT system (ie, scope, objectives, participants, etc) covers the identified records management issues and the integration of records management in the ICT system.	
2.1.8	Tender documents, if applicable, identify records management issues and requirements to integrate records management in the ICT system.	
2.1.9	A governance structure (such as a project steering committee) is in place to ensure the collaboration of key individuals in planning, designing and developing the system, including the application system manager, project manager, systems developers and records managers.	YES

2.1	Project Initiation	INDICATOR
2.1.10	A communication plan is in place to inform all those involved, most importantly the business managers and system users, of the purpose, benefits, costs and activities of the records management integration initiative.	

2.2	Planning	INDICATOR
2.2.1	The analysis of business needs includes records management issues; potential solutions incorporate records management considerations.	YES
2.2.2	In assessing risks associated with the potential solutions, risks associated with records management are also taken into account.	YES
2.2.3	The tendering processes take account of the integration of records management in the ICT system; this includes all stages, as appropriate, including, for example, 'request for proposal', assessment of contractors, selection, engagement and review of results.	
2.2.4	The resources required to integrate records management are taken into account when potential solutions are considered.	
2.2.5	The project plan and timeframe take into account the resources needed to integrate records management.	
2.2.6	Records management is represented in the internal management of the ICT project. (This could be achieved, for example, by appointing a senior records professional to the internal management body; or by establishing a specialist records team that reports to internal management and/or governance body, such as the project steering committee.)	
2.2.7	Staff (including contracted staff) selected to work on the ICT system include records management specialists.	
2.2.8	Relationships and agreements established with internal and external organisations that will be involved with the ICT project include the appropriate records management or archives authority (eg, the state or national archives).	
2.2.9	The potential solutions (including the associated records management considerations) are analysed and validated.	

2.2	Planning	INDICATOR
2.2.10	A discussion document is developed, based on the system alternatives/potential solutions, describing how the system will be used, operated and maintained; inputs are provided from stakeholders including records management specialists as well as target groups such as the end-user community.	

2.3	Requirements Analysis	INDICATOR
2.3.1	An analysis has been conducted of the records management requirements for the ICT system based on the records management issues identified during the planning stages.	YES
2.3.2	Records management requirements are integrated into the overall ICT system requirements (ie, functional - what the system is required to do), technical and management (eg, training needs, business rules, etc).	
2.3.3	All system requirements, including records management requirements, are approved by the governance structure for the project (eg, project steering committee).	
2.3.4	The analysis of records management requirements for the ICT system makes reference to internationally recognised standards.	YES

2.4	Design	INDICATOR
2.4.1	Business rules for records creation have been developed based on an analysis of the business process.	
2.4.2	The points in the process where records are expected to be generated and captured have been defined and reflected in the functional requirements of the ICT system.	YES
2.4.3	Metadata linking records to the business process and the related computing environment have been identified and integrated in the system requirements.	
2.4.4	Transactions that will create records are identified and defined in the system requirements.	
2.4.5	The structural and contextual attributes of the records that need to be captured are defined and incorporated in the system requirements.	

2.4 Design	INDICATOR
2.4.6 The rules are defined for how records should be captured when a transaction is carried out.	
2.4.7 The system requirements define how rules are created for how long records should be kept.	
2.4.8 Business and operational processes are redesigned as necessary to incorporate the records management requirements.	
2.4.9 Technical requirements for records management have been taken into account in the ICT infrastructure that supports the system. See also 2.3.2.	
2.4.10 Responsibility is assigned for the generation and capture of records within the system.	
2.4.11 Responsibility is assigned for maintaining the authenticity and integrity of records throughout their life cycle.	
2.4.12 Responsibility is assigned for retention and disposal of records within the system.	
2.4.13 Performance measures are developed for assessing the records management performance of the ICT system.	YES
2.4.14 A change management strategy is developed for moving from the existing system to the new ICT system including training needs and changes to business processes. The strategy must address the records management requirements specified in 2.3.2.	
2.4.15 The security features that need to be included are identified; for example, the ability to restrict access to systems functions and records to appropriate staff, or the need to ensure that the transmission of electronic records is secure.	
2.4.16 The system creates an audit trail that keeps a complete history of the creation, use and retention of all records within the system.	YES
2.4.17 Recordkeeping procedures for paper records associated with the system (eg hard copies of system input and output documents) are included in the design specifications for the system.	
2.4.18 Performance measures are carried out regularly to assess the ability of the system to meet records management requirements.	YES

2.4	Design	INDICATOR
2.4.19	A designated member of staff has been assigned responsibility for monitoring the system audit trail.	YES
2.4.20	The audit trail is analysed regularly to monitor access to the system, changes to access and security controls, and the integrity of records within the system.	YES
2.4.21	The organisation's disaster recovery plans for the restoration of records systems are taken into account in the design of the system.	

2.5	Implementation	INDICATOR
2.5.1	The developed system has been tested for its records management performance against technical, management and functional records management requirements (see 2.3.2). Testing included a 'live' test in an operational context. An acceptance test has been conducted to confirm that the system meets records management requirements.	YES
2.5.2	Awareness and training on the records management aspects of the ICT system have been undertaken within the context of the overall awareness and training strategies have been established for the system. Training must be sufficient for the ICT system to be used as designed upon implementation.	
2.5.3	Records management requirements are documented in policies, standards and practices, and technology architectures supporting the new or redesigned system take account of the records management requirements.	

2.6	Maintenance	INDICATOR
2.6.1	Mechanisms have been established to assess system compliance with the records management requirements through time.	YES
2.6.2	Mechanisms are in place for managing changes in records management requirements resulting from new business needs, regulatory requirements, etc.	
2.6.3	A mechanism is in place for monitoring the security of the system.	

2.6	Maintenance	INDICATOR
2.6.4	Assessments for system compliance with records management requirements are regularly carried out.	YES
2.6.5	A mechanism is in place for monitoring the integrity of the records through time.	
2.6.6	A mechanism is in place for managing system upgrades.	
2.6.7	A mechanism is in place for managing the migration of records to new systems and technologies; migration of records must account for changes to the technology upon which the records may be dependent.	

2.7	Review and Evaluation	INDICATOR
2.7.1	There are performance standards to assess whether the ICT system meets records management requirements, for example in relation to records security, data quality and data completeness. These may be separate records management standards or systems standards that include records management standards. The standards should be related to records management requirements (see 2.3.1).	YES
2.7.2	There are performance assessment mechanisms for assessing the ICT system's compliance with performance standards, including records management.	
2.7.3	Performance assessments are conducted to assess the system's compliance with records management standards.	YES
2.7.4	Mechanisms are in place to enable the findings of audits and evaluations to be used to improve the overall records management function as well as the overall ICT development activities of the organisation.	

Category 3 Integrating Records Management Functionality in ICT Systems

3.1 Creating and Capturing Records		INDICATOR
The system must be capable of:		
3.1.1	Identifying the records that need to be created or captured within the business process.	
3.1.2	Associating metadata with the content of records.	
3.1.3	Assigning unique identifiers to the records that will remain unchanged as long as the records exist.	YES
3.1.4	Assessing the authenticity, completeness and usability of the records at the point of capture.	
3.1.5	Capturing the records into a trusted recordkeeping repository that maintains the authenticity, completeness and usability of the records.	
3.1.6	Supporting and applying security and access controls during the process of capturing records to ensure that the records are protected from unauthorised access, alteration and destruction/deletion.	YES
3.1.7	Supporting both the technical and human audit of security and access controls.	

3.2 Managing and Maintaining Records		INDICATOR
The system must be capable of:		
3.2.1	Drawing together all elements of metadata to create a metadata profile for an electronic record.	
3.2.2	Validating metadata, for example against a range of pre-defined values such as a classification scheme.	YES
3.2.3	Creating rules to control the selection of metadata.	YES
3.2.4	Managing a metadata profile over time – maintaining links to the record and adding metadata about records management activities, such as a change to the retention requirement.	

3.2 Managing and Maintaining Records	INDICATOR
The system must be capable of:	
3.2.5 Enabling an authorised official to add to, modify or delete components of a standard taxonomy (business classification scheme, file plan, data model, etc).	
3.2.6 Assigning appropriate retention and disposition rules to records during record creation.	YES
3.2.7 Reporting on the actions carried out on electronic records either by the system itself or by an external records management mechanism.	
3.2.8 Assigning security classifications to records.	
3.2.9 Tracking the current location of records, including checked-out records or copies of records.	
3.2.10 Establishing version control and differentiating original records from copies.	
3.2.11 Providing an individual profile for each user of the ICT system and a facility for managing 'permissions' associated with read, write, modify, delete and disposal rights; restricting those permissions to designated individuals.	
3.2.12 Controlling all permissions at the level of the individual, work group or organisation as well as at the level of the record and its supporting metadata.	
3.2.13 Applying security controls to protect the integrity of records within the ICT system throughout each phase of its life cycle.	
3.2.14 Creating and maintaining an audit trail that tracks user access to records contained within or managed by the system.	YES
3.2.15 Creating and maintaining an audit trail that tracks changes to records and record metadata.	YES
3.2.16 Providing an easy method of checking the audit trails for changes to records and records' metadata within the system.	YES
3.2.17 Exporting electronic records and associated metadata to: • another system within the organisation • a system in a different organisation • an archival program for the long-term preservation of electronic records.	

3.2 Managing and Maintaining Records	INDICATOR
The system must be capable of:	
3.2.18 Ensuring that any export of records is able to include: • all electronic records • all associated metadata • all associated audit trail data.	
3.2.19 Exporting electronic records in one sequence of operations so that: • the content and structure of records are not degraded • associations are retained between records and their metadata • relationships are maintained between exported electronic records, so that their structural links can be re-built in the receiving system.	
3.2.20 Exporting all records regardless of format or generating application.	

3.3 Managing Hybrid Records	INDICATOR
ICT systems that manage hybrid records must be capable of:	
3.3.1 Managing and controlling physical, hybrid and digital records consistently.	
3.3.2 Using the same title and unique identifier for the physical and digital components of a record (such as a folder) but with appropriate markers for physical and digital components.	
3.3.3 Allocating the same access and security controls to the physical and digital components of a hybrid record.	
3.3.4 Maintaining the same access and security controls for the relevant metadata as it applies to hybrid records.	
3.3.5 Searching for and retrieving all physical, hybrid and digital records registered by the system.	YES
3.3.6 Searching for and retrieving physical, hybrid and digital records using the same search interface.	
3.3.7 Retrieving both the physical and digital components of a hybrid record.	
3.3.8 Tracking the physical movement of non-digital records, for example through check-in and check-out facilities.	

3.3 Managing Hybrid Records	INDICATOR
ICT systems that manage hybrid records must be capable of:	
3.3.9 Applying retention and disposition rules to the physical component of a hybrid record that are consistent with retention and disposition rules for the digital component of a hybrid record.	
3.3.10 Coordinating the disposal actions (eg, destruction) carried out on both physical and digital components of hybrid records, taking into account the different processes required.	
3.3.11 Ensuring that destruction of a digital component of a hybrid record results in the destruction of metadata linked to the record; maintaining minimum necessary metadata to provide evidence of the destruction of the record.	
3.3.12 Alerting the relevant authority to the existence and location of the physical component of a hybrid record when such a record or folder is due for transfer, export or destruction.	
3.3.13 Allowing the transfer or export of physical records and hybrid records, retaining associations with the digital component of the hybrid record, and the associated metadata once transferred or exported.	

3.4 Searching, Accessing and Retrieving Records	INDICATOR
The system must be capable of:	
3.4.1 Searching for and retrieving digital records and associated metadata so that they may be rendered for display.	
3.4.2 Indexing paper and electronic records generated by the ICT system for retrieval and access using a standard taxonomy (business classification scheme, file plan, data model, etc).	
3.4.3 Providing search and retrieval mechanisms for digital records and associated metadata.	
3.4.4 Searching all metadata elements.	
3.4.5 Enabling users to request and retrieve records from one or more selected repositories that may contain electronic and related non-electronic records.	

3.4 Searching, Accessing and Retrieving Records	INDICATOR
The system must be capable of:	
3.4.6 Retrieving digital records by their unique identifiers; retrieving records by naming principles supported by the system.	
3.4.7 Retrieving and listing a set of digital records and associated metadata that meet the search criteria.	YES
3.4.8 Displaying records in a manner that accurately renders their original presentation and content, and that renders them accessible and understandable to users.	
3.4.9 Displaying upon request all available metadata associated with a digital record.	
3.4.10 Managing version control of records.	
3.4.11 Retrieving any or all earlier versions of an electronic record as requested by the user.	
3.4.12 Checking in and checking out electronic records and preventing other users from modifying checked-out records, while permitting such users to view the records.	
3.4.13 Automatically calculating recall dates for charge-outs with the ability to override.	
3.4.14 Bringing forward files, volumes, enclosures, and/or documents that can be sent to users on a specified date.	
3.4.15 Placing access and security controls on the system as a whole, preventing unauthorised users from accessing records and associated metadata controlled by the system.	
3.4.16 Restricting the definition and maintenance of access and security controls to an authorised system administrator	YES
3.4.17 Supporting central management of access and security controls; applying these controls to users, records and associated metadata.	YES

3.5 Retaining and Disposing of Records		INDICATOR
The system must be capable of:		
3.5.1	Providing a reliable storage repository(ies) that meets the records' requirements for file formats, storage volume, and retrieval time and is capable of ensuring that the records' metadata is persistently linked to or embedded in the record for its entire lifespan.	
3.5.2	Providing backup for all records and the records' metadata within the system.	YES
3.5.3	Providing adequate security features to prevent unauthorised alteration or deletion of records or records' metadata.	
3.5.4	Enabling an authorised individual to create, maintain, modify and manage retention and disposition rules.	YES
3.5.5	Supporting the progressive addition of metadata to electronic records to support disposition as set out in relevant metadata standards	
3.5.6	Enabling an authorised individual to identify all records due for destruction according to their authorised disposal specifications.	
3.5.7	Enabling an authorised individual to delete records from all repository media (including removable media) such that the records cannot be reconstructed.	
3.5.8	Applying retention instructions to records and triggering the appropriate disposition event when the retention period expires.	YES
3.5.9	Preserving those records that require long-term or permanent retention in accordance with a digital preservation plan and/or transferring them to a storage repository that meets long-term preservation requirements.	
3.5.10	Documenting retention information and disposition events in the record's metadata profile	
3.5.11	Creating an audit trail of records retention and disposition rules and actions, enabling an authorised individual to carry out regular audits	YES

Appendix A

SCORE SHEET

Scoring Table

Each indicator which is met scores one point. To give an overall level for a category, total the score achieved in that category and compare in the below table[8]:

Score Achieved			
Level	**Category 1:** ***Records Management Framework***	**Category 2:** ***Integrating Records Management in the System Development Life Cycle***	**Category 3:** ***Integrating Records Managements Functionality in ICT Systems***
D	0 – 3	0 – 3	0 – 3
C	4 – 8	4 – 8	4 – 8
B	9 – 13	9 – 13	9 – 12
A	14 – 18	14 – 17	13 – 16

[8] These scoring levels were developed following an analysis of the number of available points at each level. In each category to progress from one level to another at least 1 point must be scored at the next higher level. This means that to gain a C, at least four points must be scored in level C or above, to achieve a B, at least two level B or A points must be scored and it is not possible to gain an A without scoring at least one level A point.

Score Sheet

	Indicator number	Indicator Level			Enter Score of 1 if Indicator Achieved
		C	B	A	
Category 1: Records Management Framework					
1.1 *Legal and Policy Framework*	1.1.1	1			
	1.1.2	1			
	1.1.4			1	
	1.1.5	1			
	1.1.6		1		
	1.1.7		1		
1.2 *Managerial Structure*	1.2.4	1			
	1.2.5		1		
	1.2.6			1	
	1.2.7	1			
	1.2.8			1	
1.3 *Records Management Strategy*	1.3.1	1			
	1.3.3		1		
	1.3.5		1		
1.4 *Evaluation and Audit*	1.4.1	1			
	1.4.2		1		
	1.4.3			1	
	1.4.5			1	
				Category Total:	
Category 2: Integrating Records Management in the System Development Life Cycle					
2.1 *Project Initiation*	2.1.1	1			
	2.1.9	1			
2.2 *Planning*	2.2.1		1		
	2.2.2		1		
2.3 *Requirements Analysis*	2.3.1	1			
	2.3.4		1		
2.4 *Design*	2.4.2	1			
	2.4.13		1		
	2.4.16	1			
	2.4.18			1	
	2.4.19		1		
	2.4.20			1	
2.5 *Implementation*	2.5.1	1			
2.6 *Maintenance*	2.6.1	1			
	2.6.4			1	

	Indicator number	Indicator Level			Enter Score of 1 if Indicator Achieved
		C	B	A	
2.7 *Review and Evaluation*	2.7.1		1		
	2.7.3			1	
				Category Total:	
Category 3: Integrating Records Management Functionality in ICT Systems					
3.1 *Creating and Capturing Records*	3.1.3	1			
	3.1.6	1			
3.2 *Managing and Maintaining Records*	3.2.2		1		
	3.2.3		1		
	3.2.6		1		
	3.2.14	1			
	3.2.15		1		
	3.2.16			1	
3.3 *Managing Hybrid Records*	3.3.5			1	
3.4 *Searching, Accessing and Retrieving Records*	3.4.7	1			
	3.4.16	1			
	3.4.17		1		
3.5 *Retaining and Disposing of Records*	3.5.2	1			
	3.5.4	1			
	3.5.8		1		
	3.5.11			1	
				Category Total:	

Appendix B

PERFORMANCE STATEMENTS

Category 1 ***Records Management Framework***

Level D: There may be some aspects of basic records management framework in place and there are some areas of good practice. However, few of the necessary laws, policies and governance strategies are in place or up to date and there is little or no evidence of implementation and use of the laws, policies and governance strategies that do exist. The organisation is therefore below the minimum standard of good practice requirements.

Level C: Some or all of the necessary laws, policies and governance strategies are in place in the organisation. There is some evidence of implementation and use of these laws, policies and governance strategies. The organisation therefore meets the basic good practice requirements for integrating recordkeeping in ICT systems in this area. However, some key components of the records management framework are missing and there is little evidence that there are mechanisms to ensure compliance, review and updating of the records management framework. To improve recordkeeping integration, it will be necessary to identify where new laws, policies or strategies are needed or require updating and to promote and measure compliance with a records management framework.

Level B: The necessary laws, policies and governance strategies are in place in the organisation and there is evidence that they are widely used. There is some evidence of compliance measurement, review and updating of the records management framework, but more compliance measures, review and updating are needed. To improve recordkeeping integration in ICT systems, compliance and evaluation should be promoted and enforced to a greater degree so that there is a process of continuous improvement.

Level A: All the necessary laws, policies and governance strategies are in place and widely used in the organisation. There is strong evidence of compliance, review and updating of laws and policies which in turn help to promote good governance strategies. The organisation provides a strong example of good practice in integrating recordkeeping in ICT systems in this category.

Category 2 ***Integrating Recordkeeping in the System Development Life Cycle***

Level D: Recordkeeping may be incorporated into some phases of the Systems Development Life Cycle and there may be isolated examples of good practice. However, integration is weak or is not consistent from the initiation phase onwards. The organisation is below the basic level of good practice for integration of recordkeeping in the design of ICT systems.

Level C: Recordkeeping integration may form part of some or all of the phases of the System Development Life Cycle. There is some evidence of good practice and/or

compliance with good practice requirements. The organisation therefore meets the minimum criteria for integrating record keeping in ICT systems in this area. There is, however, little evidence that mechanisms are in place to ensure that the system is designed and developed to meet recordkeeping requirements and has the full functionality to manage records over time. To improve recordkeeping integration in this area it will be necessary to further develop system evaluation, and to promote and measure recordkeeping compliance.

Level B: It is likely that recordkeeping is integrated into most phases of the System Development Life Cycle. There are some mechanisms in place to measure system performance, evaluation, recordkeeping compliance and maintenance. The organisation demonstrates an intermediate level in this area. To improve recordkeeping integration, compliance and evaluation should be further encouraged and enforced.

Level A: Recordkeeping is integrated into all the phases of the System Development Life Cycle. There is strong evidence of measurements of system performance, evaluation, recordkeeping compliance and maintenance. The organisation provides a strong example of good practice in ICT integration in this category.

Category 3 ***Integrating Recordkeeping Functionality in ICT Systems***

Level D: The system may have some of the necessary functional capabilities. Some aspects of capture, organisation, use, retention or disposition of records may be facilitated. However, recordkeeping functionality is weak. The organisation is below the basic level of good practice requirements for integrating recordkeeping in the ICT system.

Level C: The system has many of the necessary functional capabilities. It largely meets the necessary requirements for the capture, organisation, use, retention, and disposition of records. The organisation therefore meets basic good practice requirements for integrating recordkeeping in the ICT system. There is, however, little evidence that mechanisms are in place to measure system performance or carry out system evaluations and audits. The system may also lack functionality in the certain areas, for example, managing hybrid records or applying retention rules, or there may be backup procedures that do not meet good practice requirements. To improve recordkeeping integration in this area it will be necessary to further develop system evaluation and audit mechanisms and improve recordkeeping functionality in particular areas.

Level B: The system meets the majority of the necessary functional capabilities for the capture, organisation, use, retention and disposition of records. There is evidence that the system has the functionality to meet particular areas of good practice including, for example, the creation of rules to control the selection of metadata, the management of hybrid records, the central management of access controls or the creation and maintenance of an audit trail. To improve recordkeeping integration, it will be necessary to further develop mechanisms to ensure that the findings of system audits are acted upon and are used to enhance system functionality and performance.

Level A: The system meets all of the necessary functional capabilities. Good practice requirements are in place for creating rules to control the selection of metadata, managing hybrid records, managing access controls centrally and creating and maintaining an audit trail. In addition there is evidence that the system provides an easy method for reviewing system performance and compliance, for example, it applies appropriate retention and disposition rules to records, and there is a continuous process of evaluation and improvement. The organisation provides a strong example of good practice in recordkeeping integration in this category.

Appendix C

GLOSSARY

A

Acceptance test: See *User acceptance test.*

Access: The right, opportunity or means of finding, using or retrieving information.

Accountability: The requirement to perform duties, including financial and operational responsibilities, in a manner that complies with legislation, policies, objectives and expected standards of conduct.

Activity: The major tasks performed by an organisation to accomplish each of its business functions. An activity can encompass a wide range of different transactions that take place in relation to or in support of that activity. Depending on the nature of the transactions involved, an activity may be performed in relation to one function, or it may be performed in relation to many functions. Similarly, several activities may be associated with each function.

Agency: A generic title for any private or public sector institution that undertakes specific functions and activities and generates and maintains records as a result of its work. In the public sector, an equivalent term may be public office.

Application: Software that automates and manages a range of tasks supporting a work activity and, therefore, a business function. Examples of software applications include software programs designed to assist with human resource management, financial management, licensing or registration. Also referred to as business application.

Architecture: In a computer environment, an enterprise-wide architecture is a logically consistent set of principles that guide the design and development of an organisation's information systems and technology infrastructure.

Archives: Records, usually but not necessarily non-current records, of enduring value selected for permanent preservation. Archives will normally be preserved in an archival repository, which is managed by an archival institution. See also *Archival institution* and *Repository.*

Audit: The process of reviewing, verifying, evaluating and reporting on an organisation, system, process, project or product.

Audit trail: In a records and archives environment, a record showing the transactions within an information management system providing evidence of activities, such as who has accessed a computer system and when, what operations he or she has performed during a given time and the resulting changes to records or information.

Authenticity: In a records and archives environment, the quality of being genuine and not corrupted or altered. The authenticity of a record is typically inferred from internal and external evidence, including the physical characteristics, structure, content and context of that record.

B

Backup: The process of copying a computer file or collection of files to a second medium, usually on a diskette or magnetic tape, so that the data are safe in case the original file is damaged or lost. The resulting copy is also called a backup. Backup copies are usually stored on devices that can be removed from the computer and kept separately from the originals.

Budget: In a business or government environment, a statement of an organisation's financial position over a specified period of time, based on estimates of expenditure and proposals for financing those expenditures.

Business: The core functions of an organisation, intended to contribute to the achievement of the organisation's mission.

Business classification scheme: See *Classification scheme.*

Business manager: Within an organisation, the officer in charge of securing funds for and overseeing the delivery of a specific project or a set of business functions and activities. Also known as project sponsor.

Business process: A task or a set of coordinated tasks and activities that exist to accomplish a specific purpose. For example, the task of recruiting a new staff member to an organisation can be broken down into specific business processes such as advertising the position, interviewing candidates, selecting and appointing the successful candidate, adding him / her to the payroll and so on.

C

Capture: In a computer environment, the deliberate actions that results in the storage of a record in a record-keeping system, including the registration and classification of the record and the addition of metadata about the record. For certain business activities, these actions may be designed into electronic systems so that the capture of records into record-keeping systems takes place when those records are created.

Classification: In a records and archives environment, the process of identifying and arranging business activities and the resulting records into categories according to logically structured conventions, methods and procedural rules. See also *Functional classification* and *Subject classification.*

Classification scheme: A full representation of the business of an organisation, which systematically identifies and documents the organisation's activities and resulting records according to logically structured conventions, methods and procedural rules. Sometimes also referred to as a business classification scheme or file classification system. See also *Retention and disposal schedule.*

Content management: The process of establishing policies, systems and procedures in an organisation in order to oversee the systematic creation, organisation, access and use of large quantities of information, especially in different formats and applications. The process of content management may include, but is not limited to, records management, web management and the creation of collaborative workspaces. Electronic ***Computer program***, sometimes also referred to as electronic information management, also refers more specifically to the software program and supporting hardware used to automate and integrate the information management process, which may include the management of electronic documents.

Contract: In a business or government environment, a legally binding agreement entered into between two parties generally for one or more to receive payment or other benefits in exchange for the supply to the other(s) of goods or services.

Conversion: In a computer environment, the process of changing from an existing computer or software system to another, or changing records from one medium or format to another. For example, an office may convert its word processing software from Word Perfect to Microsoft Word, and it may convert its word processed records from Word Perfect to Microsoft Word.

Creation of records: The first phase of a record's life cycle in which a record is made or received and then captured in a record-keeping system for action or for its evidentiary value. Also referred to as generation of records.

D

Data **(pl.):** Electronic representations of information suitable for communication, interpretation and processing, generally by a computer system. Note: the term 'raw data' is used to refer to unprocessed information.

Database: A structured assembly of logically related data designed to be used in various software applications.

Description: In a records and archives environment, the process of capturing, analysing, organising and recording information that serves to identify, manage, locate and explain records and the contexts and records systems that produced them.

Destruction: The disposal of records through incineration, pulping, shredding, deletion or another method, so that it is impossible to reconstruct the records.

Digital preservation: A series of managed activities undertaken to ensure continued access to digital materials for as long as necessary, including in the event of technological change or the failure of digital storage media.

Digital record: A record maintained in a coded numeric format that can only be accessed using a computer system that converts the numbers into text or images that can be comprehended by the human eye. Digital records include records stored in electronic and non-electronic formats such as optical disk. See also *Born digital*.

Disposal: In a records and archives environment, the actions taken to fulfil the requirements outlined in appraisal reports and retention and disposal schedules to retain, destroy or transfer records. Note that disposal is not synonymous with destruction, though destruction may be one disposal option. Also known as disposition.

Disposition: See *Disposal.*

Document: Information or data fixed in some medium, which may or may not be considered in whole or in part an official record.

Documentation: In a computer environment, the information or instructions needed to develop, use or maintain computer hardware and software systems and to permit access to and retrieval of the data contained in those systems.

E

E-government: The use by government agencies of information technologies (such as Wide Area Networks or WANs, the Internet and mobile computing) to provide services, including: better delivery of government services to citizens; improved interactions with business and

industry; citizen empowerment through access to information; or more efficient government operations.

Electronic record: A digital record that can be stored, transmitted or processed by a computer. See also *Born digital*.

Email: See *Electronic mail.*

Essential record: See *Vital record.*

Evaluation: See *Appraisal.*

Evidence: In a legal environment, information or proof admitted into judicial proceedings and relevant to a specific case to establish an alleged or disputed fact.

Export: In a computer environment, the process of producing a copy of electronic records, along with their metadata, for another system.

F

Field: See *Data field.*

***File* (1):** In a records and archives environment, an organised physical assembly of documents, usually held within a folder, that have been grouped together for current use or because they relate to the same subject, activity or transaction. A file is usually the basic unit within a record series. A file can be found in any format, but the term folder is more commonly used in digital record-keeping environments.

***File* (2):** In a computer environment, a logical assembly of data stored within a computer system. The term file is loosely used to describe a very wide range of assemblies of data from a single document to an entire database.

File plan: In a records and archives environment, a detailed list or inventory of the individual files or file categories within a classification scheme. A file plan allows for the systematic identification, filing and retrieval of records.

Financial management: In a business or government environment, the planning, controlling, implementation and monitoring of fiscal policies and activities, including the accounting and audit of revenue, expenditure, assets and liabilities.

Folder: In the desktop environment, an assembly of one or more documents grouped together because they relate to the same subject, activity or transaction. Also known as a 'directory.' See also *File (1).*

Format: In a computer environment, a structured means of encoding and storing digital information so that it can be interpreted by a software application.

Function: A unit of business activity in an organisation or jurisdiction. Functions represent the major responsibilities that are managed by the organisation in order to fulfil its goals. Functions are high-level aggregates of the organisation's activities. Functions may be derived through legislation, policy or programme development, or they may represent a set of tasks or activities that result in goods or services that the organisation is expected to provide. Also referred to as a business function.

Functional records: See *Operational records.*

Functional requirements: In a computer environment, the tasks a computer application must perform to carry out a process satisfactorily, or the conditions or performance standards that a computer system should meet in order to support the business of the

organisation. See also *Requirements, Technical requirements*, *Management / user requirements* and *Requirements analysis.*

G

Governance structure: In the public sector, a term referring to formal arrangements established to oversee corporate-level decisions about such issues as how the organisation will function, its decision-making processes, how it will expend resources, what policies it will establish and what projects it will undertake.

Group: In a records and archives environment, the primary division in the arrangement of records and archives at the level of the independent originating organisation. Also known as archives group, *fonds* or record group.

Guide: In a records and archives environment, a finding aid giving a general account of all or part of the holdings of one or several archival institutions, including administrative or other background history, usually arranged by groups and series. Some guides identify all holdings, while others may focus on a particular subject, period, geographical area or specific type of document.

H

Hard drive: In a computer environment, the storage area within the computer itself, where megabytes of space are available to store bits of information. Also known as a hard disk.

Hardware: In a computer environment, the physical equipment required to create, use, manipulate, store and output electronic data.

I

ICT system: A coherent collection of processes, people and technologies brought together to serve one or multiple business purposes. ICT stands for information and communications technology; the acronym is used more often than the phrase itself.

Indexing: In a records and archives environment, the process of establishing terms to describe and provide access to records and archives.

Information: Data or knowledge that is communicated.

Information management: The overall process of planning, controlling and exploiting the information resources of an organisation in order to support its operations. Also known as information resources management.

Information manager: A person professionally engaged in the task of information management.

Information system: The combination of information, technology, processes and people brought together to support a given business objective.

Input: In a computer environment, any resource required in order to allow a process to take place; the result of the input and the process will be one or more outputs.

Integration: The process of combining separate parts into a whole that works together.

Integrity: The quality of being whole and unaltered through loss, tampering or corruption.

L

Link: In a computer environment, a reference from one document or source to another document or source in an online environment such as the World Wide Web. Users can go directly from one item to another by selecting the on-screen reference.

M

Maintenance: In a records and archives environment, the daily care of records and archives, particularly current and semi-current records housed in records offices or records centres, in order to protect those records from environmental hazards or other physical dangers.

Mandate: In a business or government environment, the source of authority for an organisation's activities.

Metadata: Data describing the context, content and structure of records and their management through time. The preservation of the record with its associated metadata is necessary to maintain the integrity of the record. Types of metadata include technical / structural, administrative, descriptive, preservation and use.

Metadata profile: A collection of metadata associated with a specific record, allowing the identification, description and retrieval of that record.

Migration: In a computer environment, the act of moving data or records in electronic form from one hardware or software system or configuration to another so that they may continue to be understandable and usable for as long as they are needed.

Mission: In a business or government environment, the purpose for which an organisation exists.

O

Objective: In a business or government environment, a specific goal identified to support an organisation's mission or functions; the objective is intended to be accomplished within a specified time.

Office systems: In a computer environment, software applications that are used in a business or organisation to support such tasks as creating and managing word processed documents, spreadsheets and email.

Organisational chart: In a business or government environment, the diagrammatic representation of the structure of an organisation or organisational unit.

Output: In a computer environment, the product of the transformation of inputs by a process.

P

Performance measure: See *Performance indicator.*

Performance target: See *Performance indicator.*

Permission: In a computer environment, the authority of a user to access, view or make changes to a computer system or the data it contains.

Preservation: In a records and archives environment, the act of protecting records against damage or deterioration. The term is most often used to refer to the passive protection of

archival material in which the item is not subject to any physical or chemical treatment. See also *Conservation.*

***Process* (1):** In a computer environment, a systematic series of actions a computer uses to manipulate data.

***Process* (2):** In a business or government environment, the means whereby an organisation carries out any part its business.

Program: See *Computer program.*

Project: A formally established work effort intended to achieve a specific outcome. A project has a well-defined beginning, clear scope and objectives and a specific end product.

Project charter: A statement of the scope and objectives of a project and a description of the participants and their terms of reference and responsibilities.

Project manager: A person given day-to-day responsibility for planning, organising, and managing a project and managing all associated resources.

Project sponsor: See *Business manager.*

R

***Record* (1):** In a records and archives environment, documentary evidence, regardless of form or medium, created, received, maintained and used by an organisation (public or private) or an individual in pursuance of legal obligations or in the transaction of business.

***Record* (2):** In a computer environment, a complete set of information in a database. Database records are composed of fields, each of which contains one item of information. Note: the term 'database record' is generally used in this study programme to refer to database records, to distinguish the term from record (1), which refers to documentary evidence.

Record keeping: The act of documenting an activity by creating, collecting or receiving records and ensuring that they are available, understandable and usable for as long as they are needed. See also *Records management.*

Record-keeping system: An information system that captures, manages and provides access to records through time.

Records life cycle: See *Life cycle concept.*

Records management: A field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records. Records management includes processes for capturing and maintaining records as evidence of and information about business activities and transactions. See also *Record keeping.*

Records manager: The person in charge of a records management unit or engaged in the records management profession.

Registration: The process of recording standard information about, and assigning a unique identifier to, a document or record. See also *Register.*

Reliability: In a records and archives environment, the quality of being trustworthy; in reference to records, reliability is confirmed by ensuring that a record was created by a competent authority according to established processes and that the record contains all the necessary elements of an official record.

Repository: A storage facility, physical or electronic, where records are held for safekeeping. With reference to paper-based records, a repository is a building or part of a

building in which records or archives are preserved and made available for consultation. Also known as an archival repository or archives. Note: To avoid confusion with the use of the term 'archives' to refer to records with ongoing value, the term 'archives' is not used to refer to a repository.

Requirements: In a computer environment, the conditions or performance standards that a new or altered computer system should meet. See also *Functional requirements*, *Management / user requirements* and *Technical requirements.*

Requirements analysis: In a computer environment, the task of determining the conditions or performance standards that a new or altered computer system should meet. See also *Functional requirements, Management / user requirements* and *Technical requirements.*

Retention: The function of preserving and maintaining records for continuing use. Records may be retained in the system of origin, or transferred to a separate repository such as an offline system, records centre or archival institution.

Retention period: In a records and archives environment, the length of time that records should be retained in an office or records centre before they are transferred to an archival institution or destroyed as obsolete. The retention periods chosen for different records should be based on legislative or regulatory requirements as well as on administrative and operational requirements.

Review: See *Appraisal.*

S

Selection: See *Appraisal.*

Series: In a records and archives environment, the level of arrangement of the files (1) and other records of an organisation or individual that brings together those documents relating to the same function or activity or having a common form or some other relationship arising from their creation, receipt or use. Also known as a file series, records series or class.

Stakeholder: In a business or government environment, any person, group or other organisation that has a claim on an organisation's attention, resources or output or is affected by that output.

Standard: A definition, format, specification, procedure or methodology that has been approved by a recognised standards organisation or is accepted as a *de facto* standard by an industry. Even if not formally recognised, a standard is normally considered an established or acknowledged model of authority or good practice.

Storage: In a computer environment, the area within a computer system where data can be left on a longer term basis while it is not needed for processing.

Strategic planning: In a business or government environment, the process of identifying an organisation's mission, aims and objectives, determining its needs, capabilities and resources, and then developing strategies to achieve those goals. Also referred to as development planning.

System: An arrangement of people, materials, organisations, procedures or other elements associated with a particular function or outcome. A system is made up of inputs, processes and outputs.

System administrator: In a computer environment, the person responsible for the maintenance of the computer system and the use of that system by others within or outside the organisation.

***Systems development life cycle* (SDLC):** A formal planning model used to describe the stages involved in developing or upgrading any system, particularly but not exclusively ICT systems. The steps in a systems development life cycle include conducting an initial feasibility study, planning and designing the system, implementing the system and reviewing and testing the completed result.

T

Tape: See *Magnetic tape.*

Target: See *Performance indicator.*

Taxonomy: The classification of information according to a pre-determined system providing a conceptual framework for retrieval. Typically, taxonomies consist of groups of similar entities organised in a hierarchical structure, related by presumed relationships amongst the different entities.

Technical requirements: In a computer environment, the programming specifications or technological capacity that a computer must have to carry out the functional and management / user requirements identified for the successful implementation of the system. See also *Functional requirements*, *Management / user requirements* and *Requirements analysis.*

Tender: In a business or government environment, an offer by a potential supplier to supply a specified product or service at a specified cost.

Tracking: In a records and archives environment, the process of documenting the movements and uses of records so that their whereabouts are known at all times.

Transfer: In a records and archives environment, the act of changing the location or ownership of, and / or responsibility for, records.

U

Unique identifier: In a records and archives environment, a reference number assigned to a record so that it can be distinguished from all other records. Also known as unique reference number. See also *Persistent (unique) identifier.*

User requirements: See *Management / user requirements.*

V

***Version control*:** In a records and archives environment, the management of documents or records in order to keep track of changes and revisions and ensure the most current version remains available for use.

Vital record: A record that is essential to the organisation's operation or to the resumption of the organisation's operations after a disaster. Also known as an essential record.

Volume: See *Part.*

W

Website: A specific location on the World Wide Web.

International Records Management Trust
4th Floor
7 Hatton Garden
London EC1N 8AD UK

Phone +44 (0) 20 7831 4101
Fax +44 (0) 20 7831 6303
email info@irmt.org
www.irmt.org

Registered Charity Number 1068975
VAT Registration Number 564 4173 37
Company Limited by Guarantee, registered in England Number 3477376

Produced with funding from the UK Department for International Development