

Digital Preservation in Lower Resource Environments: A Core Curriculum

Managing Metadata to Protect the Integrity of Records



International Records Management Trust

May 2016

Copyright:



This work is licensed under a Creative Commons Attribution – NonCommercial – Share Alike 4.0 International License.

CONTENTS

Preface	6
Introduction	8
Lesson 1 Concepts and Terminology: What Are Metadata?	12
Lesson 2 Why is Metadata Management Essential?	26
Lesson 3 Where and How are Digital Records Generated?	37
Lesson 4 Practical Steps	60
Additional Resources	89

Figures

Figure 1	Three Entity Model	19
Figure 2	Entity Model Layers	20
Figure 3	Register of Metadata Elements	21
Figure 4	Metadata as the Link	38
Figure 5	The Systems Development Life Cycle	66
Figure 6	Subject-based vs Function-based Classification	78
Figure 7	Relevant ISO Records Management Standards	93

PREFACE

Statement by the Secretary General of the International Council on Archives

As a matter of increasing urgency, records and archives professionals need to re-position themselves as the information managers of modern society, where information is valued as a great asset. They need to be vital players in achieving the key objectives of public policy, including democratic accountability, administrative transparency and protection of citizens' rights. Without efficient record-keeping systems, major public policies such as Open Government and Open Data simply will not get off the ground. In the information age archivists and records managers should be equipped to manage, preserve and to make publicly available records of all kinds created in digital form.

ICA places great emphasis on meeting the challenges of digital preservation. With the International Records Management Trust (IRMT), it believes that practicing records managers and archivists needed to be given as much support as possible in tackling digital preservation and that their role should be explicitly linked to the implementation of wider public policy programmes. In November 2012 the Assistant Director General for Communication and Information at UNESCO asked the ICA and the IRMT to work together to begin developing a model curriculum in digital preservation, emphasising the needs of colleagues working in countries where resources are scarcest. The ICA Programme Commission and Secretariat and the IRMT Board of Trustees endorsed the project warmly. Joint work by IRMT and ICA over the succeeding months led to an Experts Meeting at UNESCO Paris in April 2013, which validated the basic approach that the two organisations had developed.

My own concern is for the hard pressed professional, who does not have easy access to advanced archival education but who is crying out for a good practical guidance. That is the purpose of the curriculum. The ICA membership should now demonstrate professional solidarity in pursuit of these objectives. Our colleagues throughout the world will not forgive us if we fail. I am convinced that our approach, reinforced by the enthusiasm of ICA members worldwide, offers us a good chance of success.

David A. Leitch
May 2016

The International Council on Archives and the International Records Management Trust

International Council on Archives (ICA)

The International Council on Archives (ICA) (www.ica.org), created in 1948, is the international non-governmental organisation that represents the records and archives community on the world stage. It is dedicated to promoting the preservation, development, and use of the world's records and archives and brings together national archive administrations, professional associations, and regional, local and specialist archive institutions, together with individual records professionals. Today ICA has a global network of more than 1,000 institutional members and 400 individual members in 200 countries and territories, making it truly international. Its mission includes advocating for effective records and archives management in the interests of business efficiency, administrative transparency and democratic accountability, raising the profile of records and archives among key decision-makers and the general public, and building the capacity of records professionals to meet the challenges of new technologies. It strongly believes in the value of international cooperation and in fostering professional solidarity with records professionals who are working in challenging situations. It funds a range of projects that are directly relevant to the needs of practicing records professionals across linguistic and cultural boundaries.

International Records Management Trust (IRMT)

The International Records Management Trust (IRMT) (www.irmt.org) is a registered charity created in 1989 to support governments in managing official records as a basis for improving services to citizens, protecting civil and human rights, enhancing access to information, demonstrating accountability and transparency and promoting economic growth. Its activities fall into three main areas: Consultancy Services, Training and Education and Development Research. It has extensive experience of working with governments in lower resource countries, carrying out leading edge research, and developing and delivering educational material appropriate for use in these countries. Its London office manages the delivery of a portfolio of international records management projects for the public and NGO sectors, supported by a team of practicing professionals drawn from the public and private sectors and from academic institutions. Since its establishment, the IRMT has worked in partnership with a wide range of institutions and with donors and lenders to support the transition to digital record keeping. In addition to creating freely available training material, IRMT has helped dozens of countries to build sustainable laws, policies, systems, facilities and procedures for the management of records and archives in support of the goals of information integrity and openness.

INTRODUCTION

In an increasingly digital world, records in digital form are replacing paper records as the source of authentic and reliable information. Like paper records, digital records must serve as the foundation of trust that decisions and actions have been recorded accurately and that the records will continue to provide evidence of those decisions and actions for as long as they are needed. Records are the basis for the trust that societies should be able to have in their governments, that customers and clients need to have in businesses and institutions, and that development partners need to have in one another. Accurate, complete and authentic records are at the heart of these trust relationships.

Creating and protecting digital records and preserving their integrity are challenging for all organisations and all countries worldwide. The fragility of digital media, the absence of accurate and complete metadata¹, and the rapid obsolescence of software and computer systems all place digital records at great risk. While the challenges are the same everywhere, they can be particularly hard to address in lower resource environments, where the issues are just as complex as in well-resourced environments but where material resources, control systems, awareness and professional capacity are often limited. When records are not protected and preserved, the risks for citizens, organisations and governments are very high. This situation requires urgent attention.

One of the greatest challenges to the integrity of digital records is that key stakeholders, including senior managers, programme planners, IT staff, legal specialists and development planners, often are not aware that serious risks exist. Although many organisations have experienced lost or inaccessible data, few stakeholders understand the critical importance of managing digital records effectively. They often assume that technology will 'solve' information problems when, in fact, technology often increases the challenge of accessing and preserving information over time. This lack of awareness makes it hard for organisations to achieve their mandate, deliver their programmes and services or meet the challenges of international development. There is growing emphasis on accountability, transparency, Open Government, Open Data and Access to Information, all of which are based on the assumption that digital records are available for scrutiny; often this is not the case.

The other great challenge is that records professionals², who should be the key agents for improving the management of digital records, often do not have the experience, tools or authority to ensure that organisations understand the issues and adopt practical strategies to address them. Many records professionals have not had exposure to records management standards in relation to IT systems and metadata, making it difficult, if not

¹ Metadata are data about records that provide, for example, the essential context without which a record of a decision, action, transaction or communication cannot be fully understood or used.

² For the purposes of this module, records professional is shorthand for 'records and archives professional'. In many situations around the world, it is the archivists who are taking a lead role in advancing digital records management across their respective jurisdictions.

impossible, for them to take concrete action or to communicate the issues to stakeholders. In lower resource countries, where records management programmes are often poorly resourced, it is often the case that the frameworks needed to support digital records management have not yet been developed. At the same time, digital records are being generated at a rapidly increasing rate.

Managing Metadata to Protect the Integrity of Digital Records is designed to support records professionals working in lower resource countries in a range of organisational types, including public, private and academic organisations. It provides information needed to develop strategies and take practical steps to manage the metadata needed to protect the integrity of digital records through time and to discuss the issues involved with key stakeholders. The module is also designed to support records professionals in engaging with the rapidly emerging themes of transparency, openness and accountability, such as Open Data, Open Government and Access to Information, that are of growing interest to governments and to bilateral and multilateral development agencies around the world.

This module has been developed under the joint guidance of the International Council on Archives Secretariat and the International Records Management Trust, working with a committee of records experts drawn from the Caribbean and Africa including experts from Barbados, Trinidad, Côte d'Ivoire, Ghana, Botswana and Kenya. The aim has been to ensure that the module can be used to meet a wide range of professional needs as well as to be used in teaching programmes. The project team has taken care to structure the material to take account of the realities of lower resource environments, to offer practical examples that users can adapt to their own realities, and to use language that can be understood easily. This is an introductory module and therefore cannot fully address the full range of professional issues involved in managing metadata. Rather, it seeks to explain existing international good practices, relate them to the practical requirements of the countries concerned and provide a practical pathway for moving forward toward implementation. It is hoped that the material also will be useful to records professionals in a range of environments across the world.

Purpose and Scope

The effective management of metadata is essential if digital records are to:

- be accessed and understood in the context in which they were created and used
- be protected so that their authenticity is intact over time
- have the required level of integrity to enable them to be trusted as reliable evidence.

Managing Metadata to Protect the Integrity of Digital Records will provide records professionals with the basic information needed to discuss the concepts, issues and possible strategies and practical steps in managing metadata with a wide range of audiences including, in particular, senior managers, programme planners and IT specialists. The goal is

to enable records professionals to work with key stakeholders to develop meaningful and constructive strategies, particularly in organisations where records management programmes are not fully developed and where digital records management is poorly understood or is at an early stage. In brief, the objectives of the module are to help records professionals to:

- explore the concepts associated with the management of metadata to support the integrity of digital records
- understand existing standards for metadata management and the importance of applying standardised processes in relation to the requirements in their countries
- identify the issues and define potential strategies for addressing the management of metadata in a range of digital environments, including those associated with Open Data, Open Government and Access to Information.
- define the practical steps involved in introducing metadata management in organisations that create digital records
- clarify the steps involved in communicating metadata concepts, issues and strategies to key stakeholders and secure their support to incorporate metadata management in work programs and to obtain the resources to fund this work.

Audience

The module is designed to support the requirements of records professionals working in lower-resource environments³, particularly in Africa and the Caribbean, providing them with a fundamental understanding of metadata concepts, issues and strategies in relation to digital records created and held in different IT environments, including office and business systems, databases, networks, desktops and digitised paper records. The issues addressed are common to organisations of all types (including private, academic and public) where digital records management is at an early stage.

The module is designed to help inform the structure and content of a wide variety of learning opportunities, such as university or college courses, professional workshops and management or staff seminars in a wide range of organisations. It can be used to complement existing learning resources within an institution or region, and it can be linked to the wide range of excellent training material that exists elsewhere but that can be difficult to apply in a lower-resource environment. How the module is used will depend on the learners involved and the purpose and scope of the particular learning programme.

³ Lower resource environments are characterised by lack of financial and material resources, low stakeholder understanding and support for records management, and limited skills and practical experience to manage digital records. They can include governments and organisations with low levels of funding, and non-profit or community organisations.

To support this diverse use, each lesson in the module includes a set of suggested assessment questions that can be used to gauge how well the concepts have been understood. Where the material is delivered as part of a structured teaching programme, lecturers and trainers can substitute their own questions or use the questions to develop appropriate assessment exercises, for instance organising debates, developing case studies or conducting surveys.

Content and Structure of the Module

The module contains four inter-related lessons:

Lesson 1: Concepts and terminology: what are metadata and how do they relate to the realities of managing and using records, data and statistics, particularly in lower-resource environments?

Lesson 2: Why is Metadata Management Essential? Why is metadata management important and what are the consequences if metadata are not managed?

Lesson 3: Where and How are Digital Records Generated? How are digital records created, used and retained as the result of typical work processes? What are the characteristics of the various computing environments in an organisation?

Lesson 4: Practical Steps: What to do next? What practical steps should records professionals take to engage a range of stakeholders in supporting improvements in the management of metadata in their organisations?

Additional Resources

The module includes, in the appendices, an overview of relevant standards and guides, a glossary of terms, and a list of core references and sources that support and add to the guidance provided in the individual sections of the module.

LESSON 1 CONCEPTS AND TERMINOLOGY: WHAT ARE METADATA?

Introduction

This lesson provides an overview of fundamental metadata concepts. Students will be required to have a good grasp of the terminology and the concepts that underpin metadata and metadata strategies if the information provided in the remaining lessons is to be understood. The lesson begins with a primer on fundamental records concepts. This provides the context for subsequent sections that explore the concepts behind metadata and the important role that metadata play in the effective management of records.

Records Concepts

Metadata are critical in supporting the management of records throughout their life cycle. It is largely through metadata that the integrity and trustworthiness of records can be established. Before discussing concepts related to metadata, it is necessary to be clear about records and their management in general. The overview of basic records concepts described in Lesson 1 provides the background to a discussion of metadata and an explanation of why metadata are essential if records are to serve their purpose as authoritative sources of information.

Records⁴ are a special form of recorded information. Their fundamental role is to document decisions, actions, activities and communications, to ‘tell the story’ as it happened. Using a fictional example from a government ministry, records can tell the story of the contracting process for a construction project. This begins with tendering the contract and the ministry’s request for proposals, continues with the receipt and evaluation of submissions from construction companies, and ends with awarding of the contract to the company selected to deliver the project.

Based on their role in ‘telling the story’, records are capable of serving multiple business purposes when they are complete and well managed.

- Records serve as evidence: for example, the ministry creates records of the evaluation process to show how it chose one company instead of another.
- Records support decision-making: for example, submissions are in a standard format that allows comparisons to be made between companies in terms of costs, work plans, experience, etc

⁴ Record: information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business (*ISO 15489*); digital record: a document in digital form that is managed as a record (*InterPARES*).

- Records enable the organisation to hold itself accountable: for example, the records can be used to show that the ministry has complied with procurement regulations; the records can also be used to respond to a formal request under the Freedom of Information law about the award of the contract.
- Records support the pursuit of individual rights and entitlements: for example, the records can be used to defend the ministry against a company's claim that it was not fairly treated in the tendering process; or, another example, it can be used to support the claim of a tenant in a building to be demolished during the construction project who was paid insufficient compensation.
- Records are the source of valuable data and information for monitoring, analysis and planning: for example, information taken from the contracting process for the construction project is combined with information on all other contracts for construction projects in the same year; the combined information is then analysed to report on how much was spent, on what types of projects, where and so on.

In order to serve these multiple purposes, records must be capable of being related to one another, for example, all the records created as part of a single contracting process are linked. The records must also be reliable, authentic and accessible for as long as they are required. In records management, the term often used to describe these qualities is *integrity*, meaning the records are whole and without corruption.

Records typically comprise content (eg what the record says), context (eg where the record comes from, how it came to be created, when and by whom) and structure (eg the different parts of the record, the software used to create it). The records' content, context and structure must be assembled and maintained, especially if they are in digital form, to enable them to serve their purposes. Over time, the records' content, context and structure must be preserved intact; otherwise their integrity will be affected and they may no longer have the same 'meaning' or be able to be understood at all. The quality of the information extracted from the records will depend on maintaining the integrity of the records.

Records are the product of *work processes*, also called *business processes*. It follows that the quality and integrity of records depend on the quality and integrity of the work processes that generate them. Clearly, if the work processes are poorly defined or inconsistent or not followed correctly, the records produced may not be adequate.

A work process is a set of related *tasks*. *Workflow* refers to the order in which these tasks are done and how they are done. Work processes support a given *function* (ie what the organisation does). The organisation's functions and processes are managed by *accountable* individuals. The organisational structure is, therefore, in one sense, a management structure for the organisation's functions, processes and tasks. The organisation should have an *accountability* framework (who is responsible and accountable for what) derived from a *mandate(s)* and/ or an enabling *law(s)* or some other authority. In other words, the organisation's mandate says what it should do; the accountability framework determines who is responsible; and the processes and tasks are how it is done.

In the example of awarding a contract, the work process begins with a construction company submitting a formal response to the ministry's tender. The tender itself, issued by the ministry and inviting companies to respond, may include detailed instructions about how to submit proposals and there may be a number of standard documents to be completed as part of the response. Officials in the ministry carry out the steps required (based on formal procurement rules) to review the submissions from all the companies that have responded to the tender and either approve or reject them. An intermediate stage may include shortlisting and another round of responses, this time in greater detail. The process concludes with notifying the successful company of the ministry's decision. Before the issue of the contract there may be contract negotiations to ensure that the successful company and the ministry are in agreement about how the project will be delivered.

All these steps are part of the work process of awarding a contract to a successful bidder. In this example the process is highly structured because rules are in place to control what happens at each step and, as far as possible, apply standard procedures to allow comparisons between the companies responding to the tender and to enable the ministry to be accountable for its decision. This ensures that the steps are carried out properly and fairly, and that each step can be audited. The records created at each step are the means by which the entire process can be shown to have integrity. Some of the records may be hard-copy and others may be in digital form. Their physical format (paper, digital) should make no difference to their integrity.

As noted, records can serve different purposes when they are properly managed. In the example just given, the records of each step provide accurate and authoritative information about the progress of awarding a contract. They enable the whole process to be audited and they serve as instruments of accountability. Collectively the records and the work process (ie the contracting process) can be thought of as supporting a sub-function called government construction projects. Government construction projects are part of a broader function called public works. Public works are managed by an organisational entity called, for example, the Ministry of Public Works and Government Services. The mandate of the Ministry is derived from a law, which requires the Government, through the Ministry of Public Works and Government Services, to manage its property and public works programmes (including construction projects) in a fair and equitable manner to meet the needs of Government, foster economic development while protecting the environment, and respect the interests and concerns of citizens and others who have a stake in Public Works. The function, public works and its sub-function government construction projects are *what* the Ministry does to respond to its mandate. The work process is *how* the functions are carried out. The records underpin all of this.

Work processes can be highly structured, for example, the processing of tenders leading to the award of a contract for a construction project, or less well-structured such as developing a policy. Ultimately the steps in the work process depend on the nature of the function being supported (processing tenders through a formal procedure or developing a policy through less formal and more variable processes).

The steps involved in developing a policy may be less well defined. While there are formal

review and approval steps, there are likely to be many steps where the *how* can take a number of different forms. Developing a policy involves, for example, discussions, research, formal and informal communications, drafting documents, review, more discussions, approvals, etc). Some of the communications in the work process may be done via email messages, which are stored and managed according to the personal preferences of the individual or the institution. In such a work process (communicating by email) there often are few controls over the management of the records. However, the email messages may be just as important as, for instance, hardcopy memos in documenting all the steps in the development of the policy.

It is important to control record-creating processes achieved so that all records are well managed. The integrity of the records and the work processes, structured or less well structured, depends upon the quality and integrity of the *records management framework*. In summary, the framework consists of a combination of *laws and policies, standards and practices, enabling technologies* (eg IT systems) and qualified/trained *people* supported by an effective *accountability and management* structure comprising people who are aware of and understand the importance of records in achieving the goals and priorities of their business. The records management framework exists, or should exist, within the overall accountability framework for the organisation.

In the example of the Public Works and Government Services Ministry, the work process for tendering, processing and awarding contracts is defined and managed according to *policies, standards and procedures* established at the ministry-wide and government-wide level. These policies, standards and practices define the separate steps in the work process and the documentation that needs to be prepared at each stage. A computer system supports part of the process, for example, by logging the receipt of responses and recording basic information about the responses as they are processed. The computer system is developed and maintained according to a systems development methodology that involves planning, designing, testing, implementing, maintaining and reviewing the system. Together, the policies, standards, procedures and system ensure the integrity of the work process and the records generated.

Accountability is assigned across the organisation to all of those involved with the process. For example, there is a Tender Board comprising senior managers, technical staff and procurement specialists that oversees the conduct and integrity of the process. Officials within the Ministry's Procurement Department ensure that the separate steps in the process are followed and that the supporting records are received or generated, including those captured by the computer system. All those involved have a high level of *awareness* of the importance of ensuring the integrity of the work process and records.

Metadata Concepts

Literally, metadata are *data about data*⁵. In the records management context, metadata are data or information about the records, for example, about the context of the records' creation, the systems and processes that generate and manage them, and about the activities that the records support. Metadata are the glue that binds the various components of a record together and relate the record to other records that are relevant to their understanding and use.

A more technical and precise definition of metadata is:

structured or semi-structured information that enables the creation, registration, classification, access, preservation and disposition of records through time and within and across domains. Recordkeeping metadata can identify, authenticate and contextualise records and the people, processes and systems that create, manage, maintain and use them and the policies that govern them. 'ISO 23081-1: Metadata for Records, 2006'

According to *ISO 23081-1*, metadata are used to:

- access, retrieve, share, exchange, transmit records
- identify, retain, preserve and dispose of records
- understand records in terms of their context
- establish relationships among records in order to support accessibility, understandability and use
- support interoperability
- protect records and respect security requirements
- support the evidential value of records
- ensure authenticity, reliability and integrity
- respect privacy and rights
- identify the policy, management and technological environment to which the records relate

⁵ Data is the plural of the Latin word 'datum'. In general usage, the word 'data' is often treated as a singular noun, as in 'the data does not support the theory'. In this module, the words 'data' and 'metadata' are treated as plurals, as in 'the metadata are the glue the binds records together'.

- respect archival requirements.

Record-keeping metadata includes information about:

- *Registration*: metadata give a record its unique identity
- *Content, structure and context*: metadata provide information about a record's *content*, for example title and description; about *structure*, for example its type and format; and about *context*, for example its classification, information about who created it, and its relationship with other records.
- *Processes*: metadata provide information or evidence about the processes a record may have undergone during its lifetime, such as viewing, accessing or transmitting or transferring custody.

The concept of *metadata* is not new. Although it has not been called metadata, the practice of *registering* records goes back several centuries, beginning with simple lists that recorded incoming and outgoing correspondence. Formal registers and indexes, usually very large volumes, were widely in use in the nineteenth century to organise, classify, track and locate records and led directly to the development of the registered file system used by many countries.

These record-keeping practices were, and still are, based on metadata about the records. The columns of an incoming correspondence register are designed to capture different metadata: for example, the date of a letter, who sent it, the signature of the sender, the date it was received, the receiving office's *receipt stamp*, a brief description of its contents and an index entry. The title and number of the file on which the letter is placed are metadata. Within the file, the incoming letter can be related to other records that are relevant to its understanding, for example, the outgoing letter to which it replies. The outgoing letter includes the file number as reference. The incoming letter is date stamped, and the file number is written within it if it is not already included in the letter. These are all examples of metadata. The numbering and classification scheme used to generate the file number and part of its title is still called a *file classification scheme*. It can also be called a *metadata schema* (discussed later in this lesson). Both names refer to the same thing.

Based on a long tradition, records professionals are well equipped with the skills of identifying, describing and classifying records. While the terminology may have evolved and while the digital environment introduces new challenges, the principles remain the same. In the digital environment, metadata similar to the paper world's file numbers or document descriptions, facilitate access and retrieval, support security, protection and preservation, and provide the context required to enable digital records to be understood and used.

An example can be used from the process already described of tendering a construction project. In that example, the Ministry uses a simple computer system to record the receipt of companies' responses to the tender and basic information about the responses as they are processed. The system includes, for instance, a *date received* field, a field for the *name of the company*, a field to show that the response has been acknowledged and when, and a

checklist to ensure that the response is complete and that all the required documents are present. These are some of the metadata that provide context for the response. Bound together, they form the record of a transaction (eg receiving a response to a tender) in a work process (steps involved in receiving and evaluating the responses). They can exist in either paper or electronic form. For instance, they exist in a combination of the response to the tender received from the company in paper form, the Ministry's database with receipt details and an email sent by the Ministry to the company acknowledging receipt of the response.

The Ministry maintains a file or several files for the tender, evaluation and selection process. The file number connects together all the records generated as a result of the application process. The file number itself may form part of the tender number and is required to be quoted in all communications between the Ministry and companies responding to the tender. The file itself may contain the tender document and specifications for the work, responses received, emails and other documents generated as a result of the evaluation and selection process, such as notification of short-listing or rejection. Each record contains metadata to enable the record to be identified, understood, accessed and related to other records in the process. When metadata are well managed, they enable the story to be told and for the actions in the story to be trusted and to be trusted through time.

The integrity and trustworthiness of records are dependent on the integrity and trustworthiness of the work processes that generate the records, the record-keeping systems and the metadata that connect together the related records. Metadata enables organisations to prove the integrity and trustworthiness of the records. At a higher level, the integrity and trustworthiness of the records depend on the *records management framework* (policies, standards, systems, people, etc) for as long as the records are required.

In presenting this example (tendering a construction project), it is important to note that records management metadata are not a static profile of a record. Records management metadata initially defines a record at the point of capture, but it is also dynamic and may be added to through time, to provide information on how a record has been used or managed. This characteristic of records management metadata is essential for preserving the authenticity of records. For example, once all the responses to the tender have been received and the time limit for receipt has passed, the evaluation process begins. Copies are made of the responses and a Tender Board is convened. At the first meeting of the Tender Board, some responses are rejected and the remainder are shortlisted. This information (shortlisted or rejected) is related to the responses and from this point on, the Tender Board is only interested in the shortlisted companies. The rejected responses are given a standard destruction date. This is new metadata added to the rejected response records.

Records management metadata is also used as an active tool to manage records through time. In this respect, metadata is about managing processes. For example, in the tender example, metadata provide the trigger for future disposal actions on certain kinds of records.

Metadata can be human readable (eg paper) or machine readable (eg digital). In the

example of the responses to the tender for a construction project, they can be in the form of the paper based classification scheme for the filing system used to store paper records associated with the tender, and the file title and number themselves. The same classification scheme could be used for the electronic folder titles to store digital records, for example, the emails and other digital records exchanged between the Ministry and the companies responding to the tender. The classification scheme is used to relate the paper records to the digital records by using the same or similar title for the file and folder.

Metadata can be created manually or through automatic means. For instance, a records officer opens a new file for the tender, creates the file number using the classification scheme and writes the file number on the file cover. The database used to record receipt of the responses has a checklist completed online with the date of receipt for each response filled in automatically by the computer. Workflow systems, standard office software, e-mail systems and other business systems are examples of where metadata can be generated automatically by the computer.

In summary, metadata can comprise:

- metadata that document the business context in which records are created or captured, as well as the content, structure and appearance of those records
- metadata that document records management and business processes in which records are subsequently used or managed, including any changes to the content and structure, and data about access and disposition.

This is illustrated in the *Three Entity Model*. *Entity* is simply the term used here to refer to a single example of how people, functions and records work together. According to the model, records document transactions in an activity (or work process) supporting a function of the organisation. The organisation (agent) or people working in the organisation carry out (perform) the transactions and create records as a result. It also uses the records for multiple purposes after they have been created.

In the Three Entity Model, metadata (ie information about) is required to identify the three parts and link them together: metadata for the *agent*, the *function, activity and transaction*, and the *records*. Each part of the entity (agent, function, record) can exist at different levels of aggregation. For example, a record may be a single document, a file or folder, a series of records, or a record-keeping system. An agent can be a single person, a workgroup, a department or the whole organisation. A single transaction can be part of an activity or work process, a function or the entire mandate of the organisation. These levels can be seen as *layers*, where the higher layer builds on the lower and the lower is placed in the context of the higher level. For example, a member of staff belongs to a work group that is part of a department of the organisation.

Figure 1: Three Entity Model

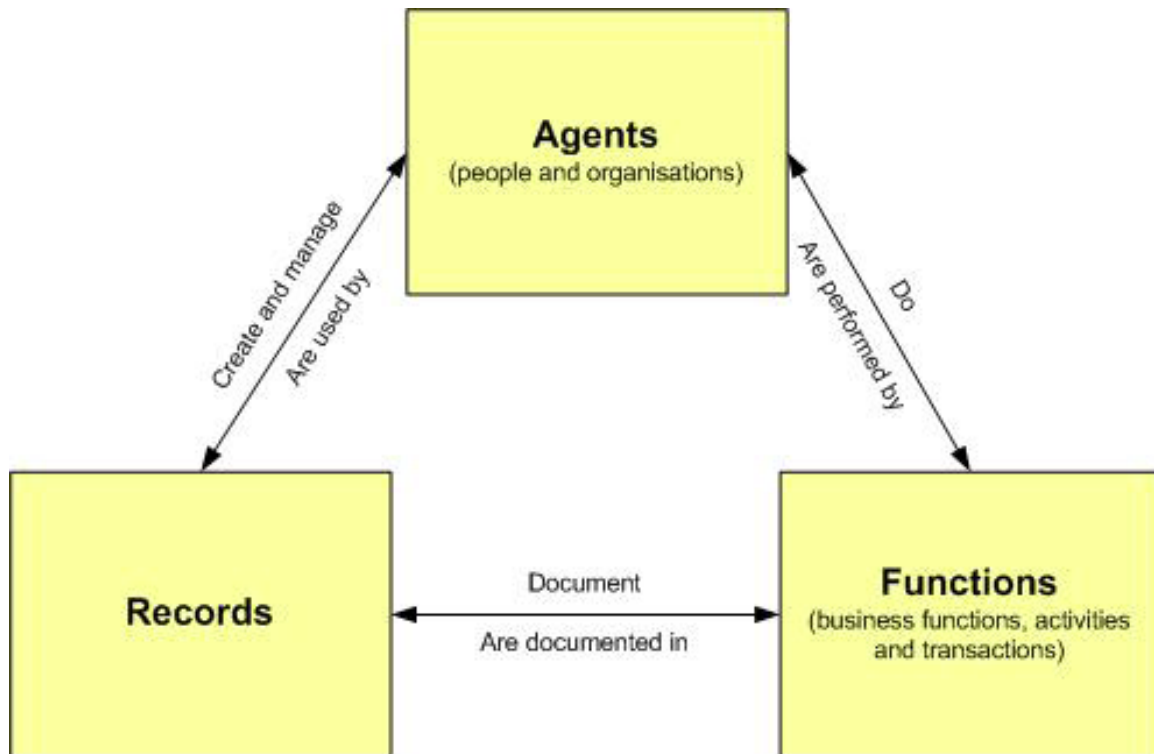
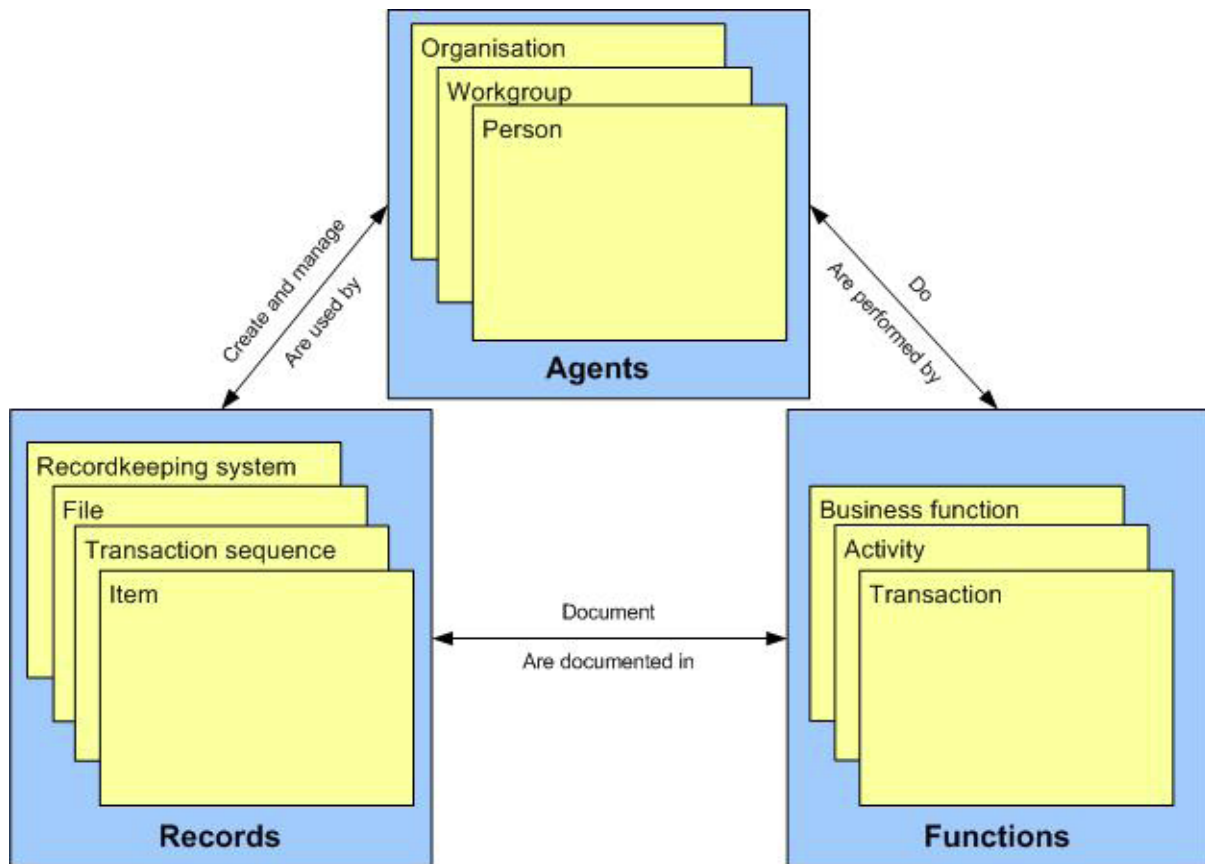


Figure 2: Entity Model Layers



In the tender example, a member of the Ministry's staff is responsible for opening tenders

and recording them in the database. This member of staff works in the Procurement Section, which is part of the Public Works Department of the Ministry of Public Works and Services. Opening one tender is a transaction that is part of the 'receiving tenders' activity. This activity forms part of the procurement process, which results in the issue of a contract to the company selected for the construction project. The construction project is planned and undertaken as part of the Ministry's public works function and meets the requirements of the Ministry's mandate to manage and improve public works and services.

According to the model, when a record is captured, key metadata (information about the record) are also captured either manually or electronically. These may be, for example, classification and registration details (document number, file number, computer generated serial number, etc) or a rule for retention and disposal. This information is associated with the record to facilitate the ongoing accountability of the organisation for the record and the ongoing management of the record.

Much of the metadata are created during the record's capture, registration and classification processes. This defines the record at its point of capture, fixing it into its business context and enabling the management processes to take place. The metadata documenting the business context should be an integral part of the records produced by the records creator. They need to be captured at the same time as records are captured into the record-keeping system.

As noted, metadata creation and capture continues after the record's creation and capture. Metadata need to be updated when records that are part of an activity become related to others (for example, when the next step in the work processes creates another record). Metadata are also updated as management needs change and when records systems are transferred from one organisation to another. Metadata need to reflect these changing circumstances. This is referred to as *process* metadata. Capture and maintenance of these metadata should be done as a normal part of business and records management operations.

Figure 3 below shows a register of metadata that should be captured for any entity being described (as defined in three entity model). The three columns (*record*, *agent* and *function*) list the metadata that is needed to maintain the integrity and trustworthiness of records over time. Some elements are common across the three columns and others are unique to a particular entity. Although these elements are specific to the situation in the particular government, they may be relevant and useful in other jurisdictions.

Figure 3: Register of Metadata Elements

Record Entity	Agent Entity	Function Entity
Category type	Category type	Category type
Identifier	Identifier	Identifier
Title	Title	Title
Description		Description
Date	Date	Date

Subject		
Coverage		
Type		
Format		
Relation	Relation	Relation
Access		Access
Disposal		
Location	Location/address	Location
Event history	Event history	Event history
Integrity check		
		Mandate

It is important to understand that developing registers like this is not a simple task. The Three Entity Model is a vision to which the organisation should aspire if it is concerned about adopting a comprehensive approach to managing metadata. Many organisations will establish models based on two or even a single entity. If it is a single entity, then that entity has to be records, and the metadata will need to include information that links the records to the work processes that generated them (category type, identifier, etc). There will also need to be metadata that links the records to the individual, group or organisation responsible for them.

The metadata about the record and those accruing in its management and use also form a record. This metadata record also has to be managed. It is essential to keep this metadata record at least for as long as the original record exists, just as in the paper world the file registers and indexes must be kept for at least as long as the files. As a minimum, the metadata record must be kept to support processes relating to the disposition of records, either by transfer of custody or ownership, or by destruction. Some metadata about the records may still be needed after final disposition, for example to account for their existence, management and disposition. Again in the paper world, a common disposition strategy is to keep registers and indexes permanently, even if the original records are not preserved after they have served all their business and legal uses.

Maintaining Metadata Over Time

As with digital records generally, metadata need to be managed carefully if their integrity is to be ensured, especially over time. Processes in the maintenance of metadata include the following.

- monitoring to ensure continuing metadata integrity
- security measures controlling access to metadata, such as rules for authorising access for the agents or systems that may need access and for the entities or objects to which they have access; this includes the rules for the personnel with authority to change the access rules

- recovery mechanisms in the case of system failure
- back-up procedures
- migration through information technology environments or changes to, or update of, systems managing records management metadata.

Some formats used for electronic records make it possible to store metadata internally within the object itself. This is referred to as *embedded* metadata. Storing metadata in a database has some advantages for record formats that do not support embedded metadata, but it has the disadvantage of not being directly connected to the records themselves. Hence, the separate storing of metadata requires ongoing maintenance of accurate links from the database to the records.

Links between resources can be made through unique identifiers. Identifiers and links (eg to related resources) will only work for resources being described with a persistent, stable identifier. For example, a unique payroll number may also be used as a unique personnel number used in other records systems, such as personnel files. This number is never changed and can never be reused by another individual.

The Importance of Metadata Schema

A metadata schema is a logical plan showing the relationships between metadata elements. Metadata schemas normally incorporate a set of rules, including rules relating to semantics and syntax that enable the management of metadata. 'ISO 23081---2:2009 Information and Documentation – Records Management Processes – Metadata for Records'

Metadata schemas describe entities (records, agents and functions), their elements and their interrelationships. Conceptually they are little different from the classification schemes developed to identify, describe and organise paper records. The classification scheme used in a filing system for paper records is a metadata schema.

Metadata elements can be further defined with an *encoding scheme*. Encoding schemes define the values or the *syntax* (rules) of a metadata element. Examples of encoding schemes include classification schemes for organisational activities, classification schemes for access and security, and disposition schedules. Again, these are similar to the standard values that are created for paper filing systems, for instance, the use of standard names for subjects such as 'contracts' or the standard way of describing date (MM/DD/YY).

Similar to paper classification systems and schemes, carefully designed and managed metadata schema have many benefits. These include, for example:

enable *integrated and consistent* management of metadata: for example, classification rules ensure that records are titled or described consistently

- enable *interoperability* by comparing or mapping different sets of metadata: for example, records in different record-keeping systems can be directly linked to each other for access by using the same identifying numbers
- express the *interrelationships* of elements and their semantics: for example, the words used to describe records so that they can be linked
- enable more effective *records transfer*: when agencies have agreed on a common metadata schema, records and their metadata can be sent/received more easily
- allow modular development, break-up or linkage of information systems
- provide a basis for the development of information systems or databases.

Assessing Student Understanding of the Lesson

At the end of this lesson, you should begin to have an understanding of the relationship between records and metadata and the role that metadata plays in establishing the context of the records. The following questions should help to test understanding.

- 1 What are the qualities that make records an especially valuable form of information? What distinguishes them from other forms of information?
- 2 What are the advantages of complete and well-managed records?
- 3 How does metadata protect the integrity of the record?
- 4 What is the relationship between the records management framework and organisational accountability?
- 5 How has metadata been used in relation to paper records?
- 6 How is metadata created and captured?
- 7 Explain the Three Entity Model and its significance for explaining the function of metadata and the process of capturing it.
- 8 Why is it important to manage metadata through time, and how is this achieved?
- 9 Why and how are metadata schema significant and how are they used?
- 10 What measures and procedures are required to ensure the maintenance of metadata through time?

Lessons 2 and 3 will expand your understanding of many of these concepts (especially work processes and metadata) through practical examples. It will be beneficial to return to these questions following both lessons and think about the following additional questions:

- 1 Has my understanding of these issues changed? If so how?
- 2 Are my explanations becoming clearer and more convincing?

This last is particularly important. It is essential to be able to communicate these concepts to key stakeholders, including senior managers, programme planners, IT staff, legal specialists, development planners if you are to succeed in creating and preserving metadata.

It is important to practise and regularly refine your explanations so that they are clear and easy for others to understand.

LESSON 2 WHY METADATA ARE ESSENTIAL

Introduction

This lesson discusses the importance of metadata in supporting the mandate and operations of organisations, and their ability to support emerging development priorities in relation to accountability, transparency, Open Government and Open Data. In addition to highlighting the importance of well-managed metadata, the lesson explores the implications for organisations if metadata are insufficient or poorly managed.

Importance of Metadata

Metadata are a powerful tool to help organisations find records, understand them and use them to serve multiple purposes. Metadata are needed to track, retain, protect and preserve records and to manage them through time. They enable an organisation to authenticate and verify the information contained in its records, and they capture important technical details that enable the records to be 'rendered' (ie provided for reading) and to be read.

Metadata document access rights, security considerations, and the quality and integrity of the systems and processes responsible for generating and managing digital records. Properly managed, metadata are the means of protecting the integrity of records. They not only describe the records but also protect them by, for example, by controlling access or triggering alerts in the event of tampering or other actions that threaten the integrity of the records.

Metadata have many other important functions for the organisation by supporting business and programme delivery, technology and investment and by supporting the goal of building a knowledge society.

Without metadata, organisations cannot carry out their mandates, meet their accountability obligations, support emerging themes such as Open Government and Open Data, achieve national and global development goals and protect and preserve the collective documentary memory. Understanding these roles is crucial because it helps the records professional explain why metadata are so important to the work of the organisation.

There are three types of metadata:⁶

⁶ NISO, Understanding Metadata <http://www.niso.org/publications/press/UnderstandingMetadata.pdf>

- administrative metadata – metadata related to the use, management, and encoding processes of digital objects over a period of time. Includes the subsets of technical metadata, rights management metadata, and preservation metadata.
- descriptive metadata – metadata that describes a work for purposes of discovery and identification, such as creator, title, and subject.
- structural metadata – metadata that indicates how compound objects are structured, provided to support use of the objects.

If the support of key stakeholders, especially senior managers, is to be secured, then the importance of metadata must be expressed in business terms. The business-driven approach can be adapted to the circumstances of individual organisations and used to develop the kinds of messages that would appeal to business managers and others such as IT, legal affairs, security and development specialists.

Roles of Metadata

Business and Programme Delivery

Metadata are necessary to ‘tell the story’. They ensure that the paper and digital records that document the delivery of a programme or service can be understood in the context of how they were created and used and can be linked to one another. Metadata define the documentary trail that provides evidence of what was done, when and by whom. In addition to enabling access, retrieval and, above all, understandability of records, metadata protect sensitive information and ensure the integrity of the records and the records control systems needed to manage them. Metadata can enable an organisation to locate important records and ensure their authenticity and integrity through time.

Accountability (Management and Legal)

As an important and critical component of a record, metadata enable an individual, a work group and an entire organisation to account for their decisions and actions. When records are well supported by metadata they can provide the evidence required to demonstrate compliance with laws and policies and the achievement of organisational goals and objectives as measured through audits and performance reviews. Organisations need well-managed metadata to be accountable. Courts of law rely on metadata to prove the authenticity of records.

Development Goals

Metadata is essential to achieving and monitoring development goals, particularly the goals for Open Government and Open Data. The objective of Open Government is to support government transparency and accountability by making information that documents decisions and actions actively available to citizens. Many Open Government initiatives go further by seeking to engage citizens in the decision-making process. Metadata are important in describing and contextualising records so that they can be accessed and understood by interest groups and the general public.

Open Data initiatives actively publicise and make available valuable publicly funded data to support a wide range of uses, with an emphasis on those that promote economic and social development. Complete, relevant and accurate metadata make it possible to identify, access, retrieve and understand data sets together with their supporting documentation. They also describe the relationships among different data so that multiple data sets can be accessed and analysed together, thus adding value. Above all, metadata, when properly applied and managed, enable the data in the data sets to be traced back to the source records from which they were generated. The metadata provide the evidence that the data, in spite of having been processed through various stages, are complete and accurate. Although the data may have been extracted from a raw data file, processed to remove personal information and presented in a different form, the information contained in the data can be trusted. The metadata make it possible to trace the transformations and verify the integrity of the data.

Technology Investment

Properly managed metadata enable an organisation to enhance benefits from its investments in information technology (IT). There is the obvious benefit, already discussed, of using metadata to protect the integrity of digital records held by IT systems. The use of metadata standards and standard metadata schema promote technical interoperability. They also promote data interoperability and information exchange and sharing between systems and across organizations. Without metadata standards and standard metadata schema the full benefits to be gained from the ability to aggregate, manipulate and otherwise harness the data resident in often diverse systems cannot be realized.

The security of systems and the protection of records and data will benefit from the use of metadata to control access and use, prevent unwarranted intrusions and inappropriate access to sensitive systems and data, and recover records and data in the event of a disaster. Metadata also enable the managed disposition of records by imposing rules about which records can be disposed of, when and by whom. The systematic disposal of records will free up space thus maximising the performance of the technology.

Finally, effective and relevant records management metadata can contribute to the development of over-arching information architectures. The purpose of information architecture is to enable and promote an information-sharing environment. IT specialists involved in the design of information architectures are beginning to recognise the value and importance of incorporating records management metadata.

Building a Knowledge Society

The value of digital records is not restricted to the organisation that created them. Digital records can have significant value for research, education and social and economic development. If they have archival value they can contribute to a country's cultural heritage and its interests in developing a national (or state, or provincial, or urban) memory. The ability for digital records to support the achievement of these objectives is dependent on metadata. Metadata created in records-creating organisations, when combined with metadata provided by archivists, facilitate access and retrieval and support the management of the records as archival records through time.

Implications of Poorly Managed Metadata

The implications of poorly managed metadata can be understood in relation to the broader issues associated with a weak records management framework. These issues include: weak or non-existent records management policies; weak or non-existent standards and practices; poorly designed or utilised systems and technologies; and a lack of qualified people for managing records, especially those in digital form.

The records management framework supports the consistent and coherent process of managing records from the time of their creation through to their use for operational purposes and finally, if they are selected for permanent preservation, as publicly accessible archives. A solid framework enables the *trusted environment* that supports the capture and continued accessibility of high quality and usable records. With a framework in place, the records are authentic, reliable, accurate, complete, relevant and timely, regardless of the physical format of the records.

Weaknesses in the records management framework expose paper records to risks. These risks are magnified for digital records. Digital records can be difficult to locate and to authenticate. They can also be easily manipulated, deleted, fragmented or lost. Without proper controls:

- Digital records are not protected against falsification or loss: *their evidential value is lost.*
- Digital records are not migrated to new hardware and software environments: *they become inaccessible.*
- Digital records are not related to paper records in a meaningful way: *it is hard to know if the records are complete.*
- Digital records are stored on personal drives: *they are not available as an organisational resource.*

- Digital records are easily copied and filed in multiple locations: *it is not always possible to know which is the final version; systematic disposition is not possible.*
- Critical paper-based documentation may not be retained because of a (misplaced) confidence in the existence of accessible digital records: *there is a loss of organisational information if electronic systems fail or the records cannot be found or accessed.*
- The authenticity and reliability of all records (paper-based and electronic) may be questioned if the management systems are flawed and inconsistent: *the records cannot be trusted and the integrity of the record and its value as legal evidence is compromised.*
- Information systems have to be redesigned and restructured: *resources are wasted; administrative and operational costs escalate.*
- The government's memory deteriorates: *the government cannot be accountable to the public; records of archival value are lost to the nation.*

Weaknesses in the framework of policies, standards, systems and people, will have a negative impact on the quality and integrity of the work processes generating records; on the records themselves; and on the metadata necessary to find the records and to ensure their authenticity and integrity over time.

Insufficient metadata makes it difficult to access and retrieve records. If the context of the records is not clear it may be impossible to understand the records. The lack of adequate metadata about how, when, by whom digital records were created, or how they were managed, undermines the trustworthiness of records. The organisation's activities are not properly documented. Trusted records are not available to support decision-making.

In the paper world, if it is unclear who created a document, under what authority, when and in what context, the document cannot be fully understood, trusted or used as legal evidence. Similarly, the quality and integrity of digital records cannot be trusted if metadata describing who, when and how they were created are missing or open to malicious alteration or deletion. If the standards, procedures and processes that control the creation and management of metadata are themselves weak or missing and generally lack integrity, then the metadata themselves will not be trusted.

The outcome is the inability of the organisation to carry out its mandate and functions, make decisions, provide services, manage its resources and hold itself accountable in keeping with laws, policies and audits. The outcome is also the failure to support emerging themes and priorities such as Open Government and Open Data.

Open Government and Open Data

Metadata lie at the heart of Open Government initiatives in that they support the objectives of openness and transparency and the public's right to access information about government programmes and services and the decisions it has made. An Open Government initiative is generally based on information being made available to the public and to investors through a government portal (a 'gateway to information') or through the portals of individual ministries. The success of these initiatives depends on citizens' ability to identify, access, understand and trust the information that is being made available. Citizens cannot exercise their right to access records unless there is sufficient metadata to enable the records to be found and understood in their proper context.

What happens if metadata are inaccurate or missing? Citizens will conclude that the Government cannot fulfill its promise of openness and accountability and, equally damaging, cannot manage the information it needs to deliver its programmes and services. If trustworthy, reliable and accurate records are to be made available, then the metadata that offers the bridge between citizens and the government's digital records holdings must also be trustworthy, reliable and accurate.

Similarly, Open Data initiatives will fail if the data sets that are generated by extracting data from source records are poorly managed. Poorly kept records result in inaccurate or incomplete data, which in turn can lead to misunderstanding and misuse of information, cover-up of fraud, distorted findings and inaccurate statistics, misguided policy recommendations and misplaced funding, all with serious consequences for citizens' lives. Datasets may appear to be robust and comprehensive, but in reality they may not be traceable to an evidentiary source, usually a record.

Do the data have real value? Can it be trusted? Are they up to date? At best, organisations using these datasets can waste resources compiling, analysing and publishing inaccurate or incomplete data. At worst, citizens and stakeholders can be misled and governments can make decisions based on unreliable data. Open Data only works if citizens trust the information provided by government. Publishing inaccurate, incomplete or erroneous data can damage that trust relationship.

Records in digital form are now the lifeblood of organisations. They underpin the achievement of goals and priorities, the protection of individual rights and, on a broader scale, economic and social development and cultural heritage. Accumulated over time, their value increases. Reliable records, and good data, accumulated over time enable organisations to analyse trends and patterns that can in turn inform the development of policy and decision-making. That value, however, is entirely dependent on the quality of the metadata required to facilitate access to records, and to manage the integrity of the accumulated records through time.

Importance of Metadata in Practical Terms

Many examples could be used. The following examples, again using an FMIS and its supporting records-generating work processes, illustrate a few of the consequences of

poorly managed metadata in practical terms.

Illustration: Purchase of Goods or Services from a Supplier

Poor Metadata Example	What Happened	Result
Details of a purchase were entered in the FMIS but there were errors in the company's contact details, held in the vendor database.	When the Purchase Order was generated, it was sent to the wrong address and then couldn't be found by searches for the company's name.	Customer frustration because of slow service (records can't be found) and lack of trust in Government.
Supporting documents were incomplete but this was overlooked.	The company selected to provide the goods or services failed to submit all the required information. This was only discovered at the data entry stage by the FMIS data entry clerk.	The request for goods or services had to be re-tendered, resulting in delays and frustration.
The Procurement Committee failed to complete an accurate log of bidding documents received (ie to record metadata for all the bidding documents).	A company was overlooked in the evaluation process because its bid was not recorded.	The company took the Government to court when the contract was awarded to another company.
Lack of retention rules for unsuccessful bids.	Unsuccessful bids were destroyed before the end of the appeal period.	The Government was unable to defend itself when taken to court because critical records of the procurement process were missing.

Illustration: Addition of an Employee to the Payroll

Example of Poor Metadata	What Happened	Result
A unique payroll number was reused.	Officials connived to add an employee to the payroll by reusing the payroll number of a deceased employee.	A ghost worker was created, the government was defrauded.

A default date of birth (01-01-2000) was entered in the date-of-birth field.	The retirement date of the employee was not calculated correctly and the pension claim process was not initiated.	The employee could not claim his pension at retirement age.
Security controls were not managed correctly.	A member of staff is able to give access to an unauthorised person.	Personal details of a new employee are accessible to an unauthorised person and are given out.
Grade data was not entered consistently following a change in grade titles.	The employee's grade was incorrectly described.	Documentation generated by the FMIS showed the wrong grade for the employee, leading to confusion over his/her job title and position.

Illustration: Production and Dissemination of Human Resources Statistics

Example of Poor Metadata	What Happened	Result
The database included default metadata (dates of birth were not accurate)	Each payroll entry required a date of birth. This information sometimes was not available so data entry clerks entered default dates so that the employee record could be saved.	The age profile of the work force, based on HR statistics, was unreliable and could not be used as a basis for planning long term recruitment; data made public was unreliable and not trusted.
Employment locations were recorded in free text.	Different descriptions were entered for the same locations. Despite data cleaning, there were still many anomalies in the location statistics.	The public could see from the published analysis that the geographical distribution of employees was not accurate. The public lost trust in all other employment statistics.
Grade details were entered inconsistently.	When a grade restructuring exercise took place, the analysis of grades could not be used because it contained too many anomalies.	Much time and effort was wasted in a manual data clean up exercise that involved checking each database entry.
Incompatible software and formats meant that statistics could be consolidated from different datasets.	The Government attempted to produce an analysis of national employment statistics but failed.	A lot of media attention was given to the Government's failure to keep its promises about producing labour statistics.

Illustration: Development Policy

Example of Poor Metadata	What Happened	Result
Records were not linked by their descriptions (eg consistent paper file and electronic folder titles).	The draft of the new security policy was based on complaints and comments received and reviews of the drafts. The comments were kept in different record-keeping systems by a number of individuals and some technical comments were overlooked and not taken into account.	The new security policy was flawed and had to be immediately withdrawn and revised.
Records were kept in record-keeping systems that were not easily available to the organisation.	A Freedom of Information request could not be answered properly within the time limit because not all the necessary information could be accessed.	The public lost trust in the Government's ability to manage its information; the Government was unable to comply with the FOI law.

Discussion

An organisation's digital records and metadata, when well managed, are a strategic asset that supports efficiency, cost-effectiveness, accountability, audit, access to information, privacy, security and policy compliance. When poorly managed, information is often incomplete, difficult to locate and cannot be authenticated; and it can be easily manipulated, deleted, fragmented or lost. Poorly managed records and metadata result in lack of trust, and wasted time, effort and resources

Digital records are difficult to preserve through time if basic controls are not in place. The outcome is that the organization is unable to carry out its mandate, make decisions, manage the systems that support its business processes, and hold itself accountable pursuant to laws, policies and audits. It is also needed to adequately support Open Government, Open Data and Access to Information initiative.

Open Government initiatives will fail if the records are not complete, accurate, understandable and accessible and retained for as long as they are of value. The objectives of openness and transparency and the public's right to access information about Government performance will fail. The outcome is the serious erosion and potential collapse of open government initiatives and the recognition by citizens that government is unable to manage the evidence it needs to demonstrate accountability and deliver its

programmes and services. If citizen engagement in the digital environment is to be meaningful, then on-going access to trustworthy, reliable and accurate records is essential.

Similarly, Open Data initiatives will fail if records and the datasets are retained in a poorly managed state as already noted; poorly kept records result in inaccurate or incomplete data. Open Data initiatives only work if citizens trust the information provided by government. Publishing inaccurate, incomplete or erroneous data can seriously damage that trust relationship.

The accumulation of data over time can enable organisations to analyse trends and patterns that can in turn inform the development and implementation of policy and decision-making. This powerful opportunity will be lost if the records and datasets are not properly retained or if they are rendered inaccessible because the records community is not equipped to keep pace with changes in technology.

Assessing Student Understanding of the Lesson

At the end of this lesson, you should be able to discuss the relationship between metadata and records in terms of the importance of metadata to organisational goals and operations and to emerging international goals for openness through Open Government, Open Data and access to information.

Consider the ways in which poorly managed metadata could impact:

- business and programme delivery
- accountability (management and legal)
- development goals
- technology investment.

Using the table below, give specific practical examples of the impact of poor metadata on organisations and development goals in your country. Draw on your practical experience or use the knowledge you have gained to define possible risks.

	Business and Programme Delivery	Accountability (Management and Legal)	Open Government and Open Data	Technology Investment
--	---------------------------------	---------------------------------------	-------------------------------	-----------------------

It is unclear who created a document, under what authority and when				
Records and the information they contain cannot be found and are not available as an organisational resource				
Links between records are lost				
It is impossible to tell if a record is complete or not				

You have now identified some of the ways in which you can make a case for the proper management of metadata, but you will also need to be able to outline solutions. This will be covered in Lesson Three.

Return now to the questions asked at the end of Lesson 1 and ask yourself:

- 1 Has my understanding of these concepts changed? If so how?
- 2 Are my explanations clearer and more convincing? If so, what makes them so?

Write a list of the component parts of an organisation-wide metadata management framework (see Lesson 3) and briefly describe each one.

LESSON 3 WHERE AND HOW ARE DIGITAL RECORDS CREATED?

Introduction

This lesson illustrates how digital records are created, used and retained as the result of work processes. The examples have been chosen because they support common functions and processes that exist in nearly all organisations, regardless of the country or level of resources. The first two examples relate to work processes associated with the management of financial information, one of most important functions in any organisation. In many countries this function is supported by a Financial Management Information System (FMIS), sometimes called an Integrated Financial Management Information System (IFMIS). An FMIS provides a good example of processes generating various types of records and the metadata that is needed to protect and manage records; place them in the context of their creation; facilitate their access and retrieval; and maintain their integrity and trustworthiness through time. The third example illustrates the use of FMIS data and records for a different purpose, the production of statistics. All three of these examples illustrate work processes that are mostly well defined and highly structured. A fourth example illustrates a work process that is likely to be less well defined and less structured, the development of a policy. The consequences of less formal work processes for managing records and metadata are discussed.

Although the examples reflect real-world situations typically found in various types of organisations (private, public, academic), the overall objective is to enable records professionals to relate the examples and guidance provided in this lesson to their own realities.

The lesson begins with an explanation of the functions performed by an FMIS. The next section describes a typical generic workflow before and after data is entered in an FMIS. Two specific work processes are illustrated: purchase from a supplier and the addition of a new employee to the payroll. The steps in these two processes and the kinds of records created are described in detail. This serves as the basis for examining the nature and role of metadata. Two other processes (*producing statistics* and *developing policy*) are also examined to illustrate the nature and role of metadata in supporting accountability, open data and open government.

The example of an FMIS was selected not only because of it supports an important and easily recognised function but also because it underlines the principle that understanding metadata for digital records means understanding the work process. As explained in Lesson 1, digital records are created as a result of the transactions in a work process. The work process itself, and its context within the organisation, provide much of the information (metadata) that enables records to be understood and used. Metadata are the glue that relate records in a given process to one another, place them in the context of their creation and use, and ensure that records integrity can be proven. The effectiveness and integrity of

records depends on the effectiveness and integrity of the work process and the supporting metadata.

Although the lesson emphasises the importance of the work process, it also acknowledges the need to establish an organisation-wide framework for managing metadata as explained in Lesson 1. The last section of this lesson therefore explores this requirement by describing the components of such a framework. The goal of this section is to explain why metadata must be approached both horizontally (organisation-wide) and vertically (within individual work processes supporting the different functions and processes within the organisation).

Financial Management Information System (FMIS) as an Illustration

An increasing number of financial management processes are conducted in an electronic environment, using a Financial Management Information System (FMIS).

An FMIS is usually a central database containing all the data needed to manage the organisation's financial transactions, accounting and financial management functions. The modules that make up the FMIS can access the data as necessary, enabling the flow of information between sections and staff engaged in different functions. Details of a transaction are entered once and the information is shared throughout the system. Information relating to many transactions can be aggregated and expressed in various reporting formats, giving totals, summaries, etc

An FMIS encompasses a number of sub-systems and functions. These may include for example:

- budgeting
- accounting (expenditure, purchase, receipts)
- cash management
- debt management
- asset management
- procurement
- payroll
- personnel management.

The sub-systems themselves also manage processes, such as management of vendor accounts, payment approvals, printing of cheques and so on.

In a centralised FMIS, parts of the organisation may enter data locally via a network, extracting the data from records held locally. They also may submit the records manually or electronically to a central point for data entry.

Some organisations may use an FMIS to manage the payroll and also certain HR management functions, such as employee positions and appointments. Data will be held about individual employees and their employment status. Other organisations may have a separate HR management system. In both cases, the data held can range in detail from basic employment and personal details to virtual personnel files documenting the individual's employment history.

The FMIS collects information on different aspects of financial management usually in sub-systems: for example, purchases for materials and services; receipts from fees and charges; employee expenses that need to be reimbursed; expenditure that is mandated by laws and policies; information about vendors, organisations and individuals that need to be paid, and so on. Accounts are set up within the FMIS corresponding to the categories of items on which funds are spent or received and which must be tracked by the system.

This is called the chart of accounts. Each account in the chart of accounts is assigned a unique identifier or account number. Information about this account, such as the cost center and the department or unit responsible for transactions under that account is associated with unique identifiers or account numbers. The account number is attached to the data for the transactions using that account and serves accounting, management and reporting purposes. It also forms part of the data validation process relating to, for example, whether or not a vendor exists in the system, whether or not there is an authorised budget, and whether or not funds have been committed. In other words, the account number and information about that account are part of a transaction's metadata and are associated with each transaction record under that account.

At the operational core of the FMIS is the General Ledger. The General Ledger constitutes the central record of the FMIS. Transactions are posted to the General Ledger, starting with the allocation of budget funds, through to the commitments to payment for goods or services. Transactions are simultaneously posted to the General Ledger and to all appropriate sub-ledgers or modules following the rules imposed by the standardised chart of accounts.

The FMIS also generates reports, for example about individual invoices, payments and receipts, together with summary reports that aggregate information and are used by managers to monitor and track expenditure, receipts, performance and commitments. The chart of accounts helps organise the finances and categorises expenditure, revenue, assets and liabilities in order to give interested parties a better understanding of the financial health of the organisation across all its functions and activities.

The section that follows describes a generic workflow before data is entered in the FMIS and after data entry has taken place. This generic workflow is common to different activities, such as the purchase of materials, equipment or services, or recruiting a new

member of staff to fill a vacancy. It is being described here in order to provide an overview of the sequence of activities and records creation and to illustrate the point that the quality of data in an FMIS is dependent upon the quality of work processes, records and metadata from which the FMIS data is derived. It is a high level view of how work processes are commonly performed but it is not intended to reflect any particular FMIS application. Work processes may vary greatly in the extent to which they are automated. Some organisations will be heavily dependent on paper records. Others will use a hybrid of paper, electronic and digitised (scanned) records. Very few organisations are entirely paperless.

FMIS Processes: Workflow Illustrations for Payroll and Purchase

The first steps in the process, whether it is a purchase from a supplier or the addition of a new employee to the payroll, take place before any data is entered in the FMIS. These steps are critical to ensure that the expenditure or recruitment meets a genuine need, is within budget or staffing limits, is authorised and is being carried out according to the correct policies and procedures. This is not only to prevent fraud but also to be able to demonstrate that each step has been conducted properly and that there is the documentary evidence to prove it. Documentary evidence will be needed, for example, if there is a problem with the transaction, or auditors or other investigators need to see that the correct process was followed. The records themselves, created during the process, are the documentary evidence and the metadata (information about the records) prove that the records are authentic and trustworthy.

The steps in the workflow illustrations are show below to illustrate the creation of records and associated metadata:

- 1 There is a need for action:

Payroll: a vacancy arises when a staff member in the organisation retires

Purchase: the organisation needs to purchase materials or services to perform its functions

- 2 The reason for action is documented:

Payroll: by a notification of the pending retirement of a post-holder

Purchase: by documents confirming that expenditure is included in budget estimates or by a business case for expenditure

- 3 The case for action is made: this may be internal communications between officials at the local level seeking authorisation to start the process of recruitment or purchase. The internal communication could be, for example, an internal hard-copy memo, with the authorisation annotated on the memo, or an exchange of emails.

- 4 Approval is given to go ahead with the recruitment or purchase:

Payroll: the approval of the employing authority is obtained and documented; other

stakeholders are notified as necessary

Purchase: the budget controller's approval is obtained and documented; other stakeholders are notified as necessary

- 5 Appointment/ procurement procedures are followed (eg by open competition or competitive tender). The selection/ procurement process is documented:

Payroll: in response to the advertised post, candidates submit their application forms, CVs and supporting documents which are filed; interviews are conducted, documented and filed

Purchase: in response to the tender, suppliers' estimates/ proposals are received and filed; tenders are opened, evaluated and filed

- 6 A decision is made:

Payroll: the successful candidate is selected, a conditional appointment is made and steps are taken to appoint him/ her formally⁷

Purchase: the successful supplier is selected; steps are initiated to generate a purchase order for the supplier⁸

- 7 Data is entered in the FMIS (for example, using source documents); source documents may be received electronically or they may be received as a paper input document with supporting documents. The critical issue here is the metadata that link all source documents with the FMIS data; a key element will be a control number generated by the FMIS which is associated with other metadata such as name, description of transaction, date and authorisation.
- 8 Audit trails are created within the FMIS to document who entered or changed the data and when, and to hold any original data that has been changed.
- 9 Checking/ authorisation is done (either on line or through a paper-based process to capture signatures).
- 10 The new employee or expenditure is 'posted' in the FMIS (to the payroll or accounting system).
- 11 Output records are generated by the FMIS and/ or manual processes (appointment letter, salary details, cheque for supplier, etc).
- 12 Payment is made (salary is paid to employee, cheque is sent to supplier).

⁷ A *conditional offer* may be made, subject to reference checks and approval by the employing authority; the formal appointment letter constitutes a contract between the employer and the employee.

⁸ A *purchase order (PO)* is a document issued by a buyer to a seller, indicating types, quantities and agreed prices for products or services that the seller will provide to the buyer. Sending a PO to a supplier constitutes a legal offer to buy products or services. Acceptance of a PO by a seller usually forms a one-off contract between the buyer and seller, so no contract exists until the purchase order is accepted.

The following work processes go into more detail for each of the examples already provided, the purchase of materials, equipment or services; and the recruitment of a new member of staff to fill a vacancy.

FMIS Processes: Workflow Illustrations for Purchase of Materials, Equipment or Services from a Supplier

The essential requirements prior to data entry in the FMIS are:

- Expenditure complies with the organisation's Procurement Regulations (eg by competitive tender. approval by a Procurement Committee) and compliance is demonstrated by full documentation kept on file by the local office; examples of the documents include:

Example 1: The tender document, issued by the organisation to invite potential suppliers to submit a response; responses from potential suppliers.

Example 2: Minutes of the Procurement Committee about the selection of the supplier.

- All required standards forms and documents (paper or electronic) have been prepared to support the expenditure and are accessible for audit.

Example 1: A pro-forma invoice from a supplier.

Example 2: The supplier's business registration certificate.

Example 3: The organisation's standard *expenditure initiation* form.

- Expenditure is within the organisation's approved annual budget and current quarterly budget allocation.

Example: Budget report or a document confirming that expenditure is within budget.

- Financial policies and procedures (eg Financial Regulations) are followed.

Example 1: A standard *payment voucher* and supporting documents (eg tender document, pro-forma invoice) are prepared for submission.

Example 2: Financial Regulations require that 'a vote controller shall submit payment vouchers to the Treasury supported by a batch sheet which has been completed in triplicate, two copies being sent with the vouchers to the Treasury and one copy retained as the departmental record together with copies of the vouchers'.

A simplified business process after data entry is:

- A data entry clerk enters data relating to the expenditure in the FMIS Accounting Module using a standard input form; when all fields are completed, the data is saved as a temporary record in the FMIS database.
- The data is confirmed by a supervisor and permanently saved in the FMIS; the data can be audited against source documents (input forms, pro-forma invoices, estimates, etc); there is also an in-built check to ensure invoices match approved commitments.
- The FMIS generates a Purchase Order with a unique number; the Purchase Order includes data relating to the supplier and materials/ services, etc; the FMIS holds a virtual copy of the Purchase Order.
- The Vote Controller approves payment; this could be on-line or may still require a signature on critical documents that form part of the process; the FMIS is updated with the approval.
- The printed Purchase Order is sent to the supplier.
- The FMIS now holds data relating to the expenditure, the authorisation and the *contract* with the supplier to provide the materials/ services; a documented audit trail also exists in the form of paper documents, FMIS records or a mixture of both, all linked by their metadata.
- The expenditure is posted to the General Ledger; the amount of the expenditure is deducted from the funds available to the local office.
- A cheque is printed from the FMIS either locally or centrally for the local office.
- The FMIS is updated to track the issue of the cheque; this is likely to be an online process.
- The local office passes the cheque to the supplier.
- The FMIS is updated to show that the cheque has been sent to the supplier.
- The supplier provides the goods/ services.
- The organisation receives the goods/ services and confirms that they match the Purchase Order.

FMIS Work Processes: Addition of an Employee to the Payroll

The essential requirements prior to data entry are:

- The vacant position is within budget limits; this can be demonstrated by reference to documents relating to authorised staff complements and the budget for salary and employment costs.

- The recruitment has been approved by the appropriate authority (may be central or local, depending on recruitment policy):

Example: The approval requires a signature by a senior official (eg on a 'request to fill a vacancy' form).

- Recruitment has been carried out in accordance with approved policies and procedures and can be demonstrated by records kept on file by the employing authority. Examples of key records include:

Example 1: Advertisement of the vacancy issued in accordance with recruitment rules.

Example 2: A description of the qualifications and experience required for the position and the job content.

Example 3: Interview records' and minutes of decisions of the selection panel.

- All required standards forms and documents (paper or electronic) have been prepared to support the recruitment:

Example 1: A standard request to fill a vacancy form.

Example 2: All required documents have been received from the selected candidate (eg CV, references, completed application form, educational certificates) and are placed on a new personnel file; the personnel file is temporary until the employee payroll number is known and this becomes the file number.

Example 3: Necessary checks on the selected candidate (eg, criminal records, proof of identity) have been completed, documented and filed in the personnel file.

- The appointment of the selected candidate and his/ her grade and start date are approved by the relevant authority; additional approval may be required if, for example, the appointment must be approved by a central authority:

Example 1: Communications between the approving authority and the employer.

Example 2: Letter of appointment issued to the successful candidate.

- Authorisation is given to add the new employee to the payroll:

Example 1: A payroll data input form prepared by the employing organisation and signed by authorised signatories.

Example 2: Authorised signatures on a standard appointment form completed as part of the appointment process.

- All source and input documents are retained according to retention rules; copies of all documents are placed on the employee's personnel file.

A simplified business process after data entry is as follows:

- The central Payroll Section creates a new entry for the employee in the Employee Module of the FMIS payroll system and enters the employee's name, date of birth, sex, marital status, date of first appointment, place of employment, grade, job title and other basic details (eg by direct entry from the appointment documents and/ or from a payroll data input form); the details are entered in specified fields, some of which are in the form of drop-down lists to limit the choices (eg sex: M/F; grade, job title, etc). Updates, for example, a change in marital status, address, position, etc will require a separate authorised process for payroll change.
- Grade and pay details are calculated/ entered. This may be an automated process with the calculation performed by the system and then authorised; or it may be from an input document where the grade and salary have been noted and authorised.
- The Position Module in the FMIS is updated to show that the position is no longer vacant. This is an automated process once the necessary authorisations have been given.
- The new employee' data is checked on line by the head of the Payroll Section and approved. The approval is captured by the system.
- A unique PIN is generated as the employee/ payroll number and also becomes the personnel file number.
- A formal letter of appointment with terms and conditions is issued by the central HR Management Office. A copy of the appointment letter is placed on the employee's personnel file; the file is numbered with the payroll number and becomes the critical metadata to link all the records. The key appointment documents may be held as digital images of paper records in the form of a virtual file that may be accessed from the FMIS; all subsequent employment records should display the employee's unique payroll/ employee number.

Because employment data is held in structured fields in the database, the payroll can be analysed and reports generated to support decision making and planning. The following are examples:

- gender: how many male and female employees
- grades: how many employees in particular grades
- job titles: how many employees in particular positions
- age: the age distribution of the work force

- retirement: the employees due for age retirement in three months, six months, one year
- vacancies: how many positions are unfilled
- distribution of employees by office/ place of employment.

Discussion

Activities and transactions undertaken in the FMIS are highly formalised. Many are automated and built into the system in the form of input screens and operations 'behind the scene' that are written in the software. For example, the input screen for a payment has structured fields so that the same type of information (name of vendor, date, amount, etc) must be entered in a particular box. The payment itself is assigned a unique control number that can never be used for any other transaction. The date of an invoice has to be entered in a precise format (for example, DD/MM/YYYY). Otherwise, it will be rejected and the data entry cannot be completed. There are also inbuilt rules throughout the system to ensure the integrity of the data (for example, the data can only be permanently saved if it is authorised by a supervising official); alternatively, the amount must be within a fixed range of values, otherwise different procedures and authorisations are required. The aim is to reduce errors in data entry. Training, procedures manuals and checking are essential to achieve an acceptable level of accuracy and also to maintain the security and integrity of the data.

In some fields the system itself will fill in the data (for example, the date the entry was made, or the unique control number). The name of the vendor may be represented by a code so that it is always in exactly the same form and not, for example, entered in different spellings (*J D Brown and Company, Brown and Company, Brown Company Ltd* etc). A new vendor who has not previously supplied the organisation will need to be entered in a separate input screen that assigns a unique vendor code and connects to an index of all vendors so that in future anyone entering this vendor can look up the code. There also will be rules about how to enter, for example, the name of a new employee who is being added to the payroll (surname first, then first and middle names in full with no abbreviations) and also a rule which requires that a unique payroll number assigned by the system can never be reused.

Though it might not be given this title, the rules for entering data constitute part of a *metadata schema*, which has been described in Lesson 1, the set of rules that enable metadata management. If, for example, all dates are in the form DD/MM/YYYY, the system can be programmed to search for a date or a date range, and the records themselves can be sorted and organised by date. A date search can then be used to generate a list of all the purchases made in a particular month or all the new employees added to the payroll between particular dates. If the metadata rules have not been well defined or are not followed, the effectiveness of the system will be greatly reduced. This point will be addressed in Lesson 4.

Some fields will have drop-down menus to limit the information that can be entered (for example, descriptions of materials and equipment and their codes or the grades or job titles of employees). Additions and changes to these menus will require their own rules and authorisations, capturing information (metadata) about who made the change and what was changed. In this way, the materials or job titles will always be described by the same term and will be properly categorised to allow accurate identification, aggregation and analysis. This will also ensure, for example, that when accounts are prepared, expenditure on particular items are correctly calculated and the accounts are accurate.

The data entered in the FMIS for a particular transaction constitute a record. Much of the data is, in fact, metadata, or data about the data (date entered, by whom, description, which input screen or function of the FMIS, etc). The transaction itself will have a unique control number, which is associated with all the processes connected with the transaction, including authorisations.

FMIS operations will be governed by technical and user procedures that define how the FMIS works and how data and metadata are managed. There also will be policies and rules with which FMIS operations have to comply (for example, Financial Instructions, office instructions, limits on expenditure above which higher authorisations are required, system security plans, records retention schedules, etc). Within the public sector there also will be laws in place that define the roles and responsibilities of the Ministry of Finance, Treasury, Budget Office, Audit Office and other agencies involved in managing state finances, as well as an overall framework for public financial management, including the use and reporting of resources (how much is spent, how much public services cost, etc). In many situations, all the necessary rules, procedures and framework will not yet be in place. For example, there may be no formalised retention schedule approved by the organisation or by the archives authority. These issues are discussed in more detail in Lesson Four.

Finally, there are likely to be many related records held outside the FMIS, often in the form of source documents or output records, linked to the FMIS by their metadata. Some may be held in filing systems (paper or electronic) such as decisions to go ahead with a purchase or a recruitment. Others will be records generated by the work process prior to data entry (such as payment vouchers or data input sheets, kept in batches or bundles by date). The entire record-keeping landscape (FMIS, filing systems, bundles of records, etc) will be subject to the archives legislation and/ or records policy, retention rules and monitoring by records professionals. The following list illustrates the location of related records:

- FMIS and its sub-systems: data held on FMIS server
- batched paper input and output transaction and supporting documents: held in Treasury or Finance Office records store
- electronic input and output transaction and supporting documents: separate database, Treasury or Finance Office networked office system; database of scanned documents, etc: held on various servers

- paper management reports: held in Treasury or Finance Office filing system or in officials' own offices
- paper correspondence with vendors, other agencies, finance staff, other stakeholders: held in Treasury or Finance Office filing systems
- electronic correspondence with vendors, other agencies, finance staff, other stakeholders: held in Treasury or Finance Office filing systems
- email communications, transmitting transaction and supporting documents; held on email server or saved to other systems; or printed and filed in other record-keeping systems.

The challenge for the records professional is to ensure that all these records can be related to each other so that together they support the organisation's functions and provide the necessary trusted information when it is needed. Metadata are the glue that enables records to be linked, as illustrated in the following examples of metadata.

Figure 4: Metadata as the Link

Category of Records	Example of Record(s)	Example of Metadata	Example of Role in the Work Process
Electronic correspondence with vendors	Pro-forma invoice for goods/ services, received by email	Supplier's name, contact details and company registration details	Enables tender conditions to be met and vendor to be considered for selection
Electronic input document	Minutes of agency' Procurement Committee, and scanned tender documents, received by email	List of people present at Procurement Committee meeting; signature of chairman; response to tender submitted by successful company	Confirms tender and selection of supplier have been performed correctly
Paper input and supporting documents for a payment	Payment voucher authorised by vote controller, prepared by agency for FMIS input	Unique payment voucher number; budget code and description	1. Ensures correct processes have been followed 2. Enables payment to be authenticated and authorised
Payment record in the FMIS	Transaction record for payment of invoice, entered in the FMIS (data about the transaction)	1. Unique transaction number 2. Chart of accounts unique account number and description	1. Identifies payment and can be used to link to other records 2. Ensures payment is made from the correct account
Electronic output transaction document	Purchase Order for supplier and acceptance by supplier	Unique purchase order number; supplier's acceptance	Provides legal commitment to supply good/ services
Paper correspondence with vendor	Supplier's dispatch note	Supplier's dispatch note number, purchase order number, date and description of goods/ services	Confirms goods/ services have been dispatched and receipt can be checked

Paper management reports generated by FMIS:	Printout of expenditure by budget lines, covering a three-month period	Account numbers and descriptions	Enables managers to monitor expenditure
---	--	----------------------------------	---

The following two work process examples are less detailed as the first two examples but they are intended to illustrate the nature and role of metadata in supporting two different themes: Open Data and Open Government (high profile international trends that have gained considerable attention among development partners and donors) and a less structured work process that presents additional challenges to managing records and metadata.

Work Process Illustration: Producing Statistics

This example is a fictional description of a work process leading to the production of statistics that are used for internal decision-making and for dissemination to the public through an open data initiative. The work process is based on the steps that are typically carried out in collecting, processing and making available statistics. It uses an FMIS as the source of the data so that this example can be seen in a single context of the first two examples already described. It is assumed that the FMIS has a module that manages the payroll and has data on basic employee details. Although the example uses a payroll for government employees it can be applied to any payroll.

In this example, using FMIS information, the work process is designed to produce statistics showing the number of employees in a given ministry by gender, region and district, occupational group, age and grade/ salary range.

The work process begins with the FMIS database and the extraction of the relevant data from the payroll. The gender data are contained in one field of the payroll database, *regional* and *district* data in another field, and so on, and a simple process of copying selected fields into another blank database can be employed though there are other ways of accomplishing the same result.

If necessary, the raw data set is processed to remove names of employees (*anonymised*) to protect the privacy of individuals. The raw data may also need to be cleaned to remove any anomalies that might affect the accuracy of the data. For example, employees who retired within the current month, but who have not yet been removed from the payroll need to be excluded; and any inconsistencies in the occupational group data, such as group names no longer in use, need to be standardised. The anonymised and cleaned data set is now ready to generate statistics. Pie charts, tables, graphs or other illustrations are prepared to present the data in summary form and reports are prepared to provide guidance to the data. The aim is to present the statistics in a variety of ways: for example, number of men and women in different occupational groups or regions; age profiles (number of employees in the age range 20-29, 30-39 etc) for occupational groups, grades, the whole workforce,

and so on.

Once the statistics and illustrative graphs are created, copies are made available for use internally in the Ministry (for instance, by HR staff to support future hiring strategies). Copies are also made available externally for use by citizens and academic, public and private sector organisations through the Ministry's Open Data initiative. In the case of the Open Data initiative a link to the data set is provided on the Ministry's web site.

The statistics are produced on a quarterly basis. A verification process is used at every stage to correct errors in the data, identify potential privacy issues (resulting from the combination of the fields inadvertently revealing the identity of an individual) and otherwise to ensure the integrity of the data. The work process, from the initial collection of the data from the FMIS to the dissemination of the statistics should be carried out within a defined period so that the statistics are current.

Using the payroll data, other reports can be produced on a regular basis by the Ministry for internal use. These may include, for example, number of vacancies, number of vacancies filled, vacancies by occupational group, changes in gender and age profiles, numbers due for retirement in the next year, in the next five years, etc. The data set made available through the Ministry's Open Data initiative may also be analysed in different ways. If the raw data is reliable, it is a relatively simple process for an expert to derive much useful information. This activity is sometimes called *data mining*.

Documents related to the production of the statistics such as the plans for the preparation of the statistics, the methodology, emails and related correspondence, and other documents generated as a result of the work process can be kept in both paper and electronic folders.

A copy of the raw data and its supporting documentation can be sent to the National Statistics Office, where statisticians can merge selected Government payroll data with a data set received from other sources, for instance the Ministry of Labour, which may hold employment information for the private sector. From this, more tables and reports can be developed to show the pattern of employment across the country, for instance by using geographical information derived from a separate Geographical Information System (GIS) to provide useful information to guide government planning and reporting and make information available through the Ministry's Open Data initiative.

The integrated data set containing the employee data, the labour force data and the geographical data is sometimes referred to as a *mash up*. Documents generated during the process of mashing up the three sets of data could be kept in electronic and paper folders, where the datasets could be kept in the Government's data library.

Discussion

Collectively, the raw data sets, the various other versions of the data sets, the outputs of analysis, and the documents generated as a result of creating the data sets and analysing

them, provide evidence of the entire work process that supports the production of statistics. The documentation will substantiate the findings and provide evidence of the integrity of the process. If, for example, a concerned citizens' group or a journalist asserts that the age profile of government employees is inaccurate, the Government has the means of explaining the methodology and defending its analysis. However, if the payroll data includes incorrect dates of birth or default data (an arbitrary date entered because the true date is not known or available), the statistical analysis will obviously be flawed.

Taking the age profile as an example, dates of birth in the payroll record are based on documentary evidence of each employee's date of birth (a birth certificate). When first appointed, all employees must provide evidence of their date of birth. In circumstances where compulsory birth registration is not enforced, a sworn affidavit can be produced to provide evidence of birth acceptable in a court of law. The birth certificate/ evidence of birth must be included in the documents provided by the new employee before he/ she can be added to the payroll. Data entry in the payroll database should not be entered until the 'date of birth' field is completed and entered in a standard form (DD/MM/YYYY) as defined by the metadata schema. The addition of the new employee to the payroll should not be authorised until the initial data entry is checked and 'permanently saved'. The date of birth is then unchangeable. If someone attempts to alter the date of birth, the FMIS will detect this and record the details of the attempt (username, time and date) in an audit trail. The age profile in terms of dates of birth can therefore be trusted. However, other metadata are needed to trust the age profile in relation to grades, regions, etc

Again, the glue that binds the records together logically, supports their integrity, and facilitates access to the information they contain is metadata. In the payroll data set, each employee has a unique payroll number associated with his/ her name and the other data about his/ her employment. Source documents should use this metadata (eg include the unique payroll number) to update the employee's data, for example, when the employee marries and changes her name, or when he/ she changes position or moves to a different place of employment. This control number ensures that data is entered for the correct employee who has been uniquely identified. A metadata rule should be that all source documents used to update payroll data should always quote the payroll number.

Each employee has a different number and the same number can never be used for more than one employee. With this rule in place, the statistics derived from the payroll cannot count the same employee twice or count an employee who does not exist. The integrity of the statistics in terms of employee numbers is therefore maintained.

Work Process Illustration: Developing Policy

This module is based on the fundamental principles that records are generated from transactions in a work process, and that metadata must account for the relationship between records and the work processes from which they are generated. In the modern office, however, some work processes are not clearly defined. This is particularly the case where 'office systems' are concerned (e-mail, word-processed documents, spreadsheets) and where work is done using a personal computer or other device from which work can be

accessed (laptop, notebook, tablet, mobile phone, etc). In this situation, the user has relative freedom over what information is created, sent and stored (eg as e-mail and attachments) and accountability for recordkeeping is unclear. Typically, it is user-driven and the user is not usually bound by structured work processes or rules and can usually choose what is created, how it is transmitted, how it is stored, managed and preserved. Centralised paper filing systems, imperfect though they often were, at least encouraged a single set of rules for record keeping. In modern offices, there is often less control.

The work process described in this final example (policy development) is designed to address less structured office systems, for instance, e-mail and other desktop created documents. Although the work process example is fictional, it reflects the typical process by which a policy is developed and illustrates the characteristics of the office environment within which records are generated.

The example relates to the security policy for the FMIS following several incidents in which unauthorised persons accessed personal information. The existing policy must be reviewed, changes made and a new policy approved. The steps in this process are as follows:

- The requirement for a policy review is identified. As the result of several privacy breaches, senior management decides that the policy on managing personal information in the FMIS must be reviewed.
- The organisation establishes a small working group chaired by the Director of the Department responsible for managing the FMIS, and including technical staff and FMIS user representatives.
- The working group's technical staff carry out research, consult with key individuals within the organisation and produce a first draft of the new policy.
- The technical staff report back to the working group and the first draft is reviewed. A second draft is prepared.
- The second draft of the policy is made available for consultation and review. Comments and recommendations are examined by the working group. A third draft is prepared.
- The third draft is passed to FMIS management for review and endorsement.
- The final draft of the policy, with a report on the consultation process and a communication and implementation plan, is submitted to senior management for approval.
- The approved policy is implemented according to the communication and implementation plan.
- Changes are made to the rules governing access and security in the FMIS.

During the policy development process, the following documents (the majority in electronic form) are generated or gathered (see box below). Notes in brackets give examples of the types of records created:

Following the first meeting of the working group, the Director of the Department responsible for the FMIS instructs his administrative officer to create an electronic folder on the Department's shared drive. As the records grow, sub-folders are created for minutes of the working group, drafts of the policy, comments by reviewers, etc. The approved policy and the communications and implementation plan are filed in the main FMIS folders and sub-folders. The titles of these folders are based on, and consistent with, the classification scheme for hard copy files kept by the Department. Key emails are saved in their native format in the folders.⁹

⁹ Email systems often support their own proprietary formats (eg .pst in the case of Outlook); while emails stored in these formats are accessible as long as the email system is in place, for preservation purposes, emails

Discussion

Developing a policy, consulting individuals, discussing requirements, preparing a draft, reviewing a draft are all tasks that have no well-structured work processes or well defined records formats to document them. Part of the process of developing a new policy may in fact be to define how it will be done and then design and assign the tasks. Those responsible for developing the policy know that records must be made of their activities, but there are no precise standards or procedures to tell them exactly what to create and keep. This presents challenges for record keeping and the capture of metadata. In the examples discussed earlier (purchase from a supplier and adding a new employee) most of the work processes are already defined and structured and the record-keeping and metadata requirements are known. This is not the case with the 'developing a policy' example, which can follow any number of work processes and involve a wide range of different activities.

How should metadata be defined and applied in the absence of defined steps in a work process and in an environment where individuals rather than the organisation or the system dictate how records are to be described and classified? How can email messages and their attachments, records of meetings and discussions, draft policies and reviews be placed in context and related to one another to tell the 'story'? Where should they be stored and how should they be organised and retained? What metadata are required to glue them together?

A key challenge for organisations and records professionals is to classify records generated in an office environment dominated by email and other electronic documents that are the product of ill-defined work processes. How can these records be related to the classification scheme (ie metadata schema) developed for more defined work processes where records can be identified clearly for each defined step in the process? In the FMIS example, metadata schema may be designed, developed and implemented for the defined work processes associated with purchasing goods from a supplier or adding a new employee to the payroll. In fact, without a metadata schema, whatever it might be called, the FMIS will not work. For records generated in the office environment (where policies are developed for example) the file classification approach is likely to be used. The metadata schema is based on a filing system.

In the policy development example, an electronic folder was created to hold records relating to the development of the new policy. The folder and sub-folders were given a title that is consistent with the Department's classification scheme which itself must be consistent with the organisation-wide classification scheme. The titles of the documents saved in the folders must also be consistent with the Department's guidelines for giving titles to documents. However, stating the ideal or what should be in place is the easy part.

can be converted to MBOX or EML formats (with EML being a preference because it can handle attachments); again, however, this step may only be necessary if the email system is to be discontinued and continued access to the emails could be placed at risk.

The challenge is to bring about change in the way that organisations work so that metadata standards are in place, are in use and there is compliance. Sometimes, this change will require employees to do more. There may be some resistance.

The first assumption is that there is an agreed classification scheme. The second assumption is that it works. The third assumption is that it is used properly. What is to stop the Director of the Department or his administrative assistant making up their own folder titles (eg 'security breach stuff') and giving documents titles that make sense to them (eg 'first meeting', 'Albert's comments', etc) but may not make sense to others.

It is easier to enforce compliance with metadata standards in the FMIS examples. The system can be designed so that users have to enter data in a certain way. The system itself may enter some of the metadata. Users will not be required to make any great effort to comply though they will have to follow rules correctly, for example, giving the right description to an item of expenditure. In fact, because the work processes are highly structured, users may not even be aware that anything is being enforced: what they must do is simply the way the system works; they have no choice. However, there are challenges even with the FMIS examples.

When building a strategy for creating and managing metadata across the organisation, it may be best to develop what seem like distinct metadata schemas for the work processes and the records generated in the office environment and then, over time, determine how the metadata schemas can be related more closely to the highly structured systems, such as an FMIS, and even standardised.

An organisation-wide approach requires all systems to be compliant. The easiest way to enforce compliance is to build in the work processes and metadata schema at the design and planning stage. This is likely not to be the case in many organisations. If, for example, the FMIS system, as implemented, has no standard for entering names of suppliers or names of employees, it will be possible to create more than one record for the same company or individual and it could be difficult to find them with a name search. Using another example, if it is possible to overwrite a payroll record, the 'unique' payroll number can be reused. There are real examples of payroll systems where this has happened and it has opened the way to fraud. There are examples of payrolls that are bloated with 'ghost workers' because work processes are not well defined and metadata standards are not in place or are not followed. Clearly, if payroll records can be overwritten, the system software will need to be changed and users retrained to comply with the metadata standard.

Organisation-Wide Management of Metadata

Any organisation framework and standard will need the full support of the most senior executives. As a starting point, it is essential to establish a policy that states the requirement for metadata standards and makes staff at senior levels accountable for ensuring that the standards are in place and used, even if this is at first a distant objective.

To implement the policy requires organisation-wide commitment and involvement. More practical steps are discussed in Lesson 4.

As discussed in Lesson 1 and emphasised in this lesson, metadata should always be viewed in association with the work process. However, if the organisation is to achieve consistency in the way metadata are generated and used and if it is to achieve the goal of interoperability where records and data can be shared across work processes, then the organisation-wide framework for managing metadata, described in Lesson 1, needs to be in place.

Using the FMIS example, if the metadata are to be shared among related applications such as HR management systems, other financial systems and with other organisations generating or using similar types of financial data, then an organisation-wide framework is needed, comprising:

- A policy that states the requirement for metadata standards and assigns accountability/ makes people responsible for ensuring that the standards are in place and respected. Example: A policy expressing the decision to use ISO 23081 (Metadata for Records) as the framework for the development of metadata schema in the organization will guide the development of metadata schema and standards in the HR and Finance systems; accountability for reviewing compliance with the policy includes the directors of HR and Finance in addition to the records manager.

A metadata standard complete with metadata schema that explains why a standard is required and sets out standards for the types of records, fields and values that must be used in systems established by the organisation, including the FMIS and related HR and financial systems. Example: The same fields such as name, age and payroll grade are used in both the FMIS and HR systems. This facilitates information exchange between the two systems (e.g. HR being able to query for the payroll information of a specific person).

- Formal arrangements for managing the standards and ensuring they are maintained and available as required to support the metadata requirements of systems such as the FMIS and other systems. Example: A steering committee has been established to oversee implementation of the metadata standards as part of the systems development/modification process for the HR system and the FMIS; adherence to the standards will be undertaken as part of the systems review and audit process and the quality control checks that are built into the design of the systems.
- Application profiles that apply the metadata standard to individual application systems (ie configure the metadata standard to support the specific metadata requirements of the individual system). Example: The employee profile (containing fields of information describing the employee's employment and payroll status) is adjusted to serve the needs of the HR and FMIS systems but in a way that enables employment and payroll information to be exchanged. The profile fits within the application profiles defined the HR and Finance systems and these in turn fit inside the generalised application profile for the organisation as a whole.

- Qualified people with the knowledge, skills and abilities to develop the standards, ensure their implementation and continuously monitor their use. Example: records management staff have been trained in the development of metadata standards and have worked with IT (data management) and audit specialists as well as the managers of the HR and FMIS systems to enhance their awareness of how to implement the standards and review their relevance and effectiveness through time.
- A programme of awareness setting and training to ensure that all of those who are involved in using the standards are equipped with the required knowledge and skills. Example: awareness setting and training programmes are in place for users of FMIS and HR systems to ensure that they understand the importance of the metadata standards being employed in the design of both systems and how to maximize the benefits of the standards in support of their work.
- A governance structure and management framework that oversees and directs the development and use of metadata standards, schema and systems; this would include a process for the development, review and approval of the standards. Example: The governance structure used to oversee the design, implementation, maintenance and ongoing review of the HR and FMIS systems is used to oversee the development and application of the metadata standards used in both systems. The process for developing and approving IT standards is used as the process for reviewing and approving metadata standards.
- An audit/evaluation process to monitor compliance and assess effectiveness of the standards. Example: records management has worked with audit specialists to incorporate in the systems review and audit processes the processes for complying with metadata standards and for reviewing their effectiveness.

Ideally, this metadata management framework should be situated within the context of a broader records management framework that includes legal and regulatory controls, internal responsibilities and accountability, records management policies, standards, guidelines and procedures, skills and training, and the physical infrastructure and resources for managing records.

Weakness in any one of these areas can undermine trust in the integrity of records. A weakness in the records management policy, in the availability of qualified people or in the design of the records repositories cannot be addressed on its own. All factors need to be addressed equally and to the same level of effectiveness and quality. If any one or all of the factors are weak or missing then trust in the records is eroded and if trust in the records is eroded, then trust in the organisation's ability to carry out its mandate will be at risk.

Assessing Student Understanding of the Lesson

At the end of this lesson, you should have developed a detailed understanding of the nature of structured and unstructured work processes. You should now be able to identify and analyse work processes within your own organisation or in organisations with which you have had contact. To test your understanding, do the following:

- 1 Identify a) a more highly structured and b) a less structured work process that takes place in your organisation or in an organisation with which you have previous experience.
- 2 Explain the function that these work processes support.
- 3 Analyse each of these work processes, breaking them down into the various stages in the workflow and describing each stage.

Then, for each of the stages that you have identified, describe:

- 1 The information needed (if any) before the stage can take place.
- 2 The information/ documentation that is created when the stage is carried out.
- 3 Whether or not it might be necessary to alter any of this information/ documentation later in later stages.
- 4 Whether or not it will be important for the staff carrying out this stage of the work process to prove that the work took place.

In considering these last four questions, you should begin to recognise the link between records, work processes and metadata. Decide what you think are the metadata and what are the records needed to document the work processes you have described. Be clear about your reasoning by writing it down or explaining it to another person.

Devise a plan for gathering an accurate understanding about a work process is carried out rather than just describing it in theory.

Finally, describe the organisation wide framework that will be needed to manage the metadata that has been created, including the policy, governance structure and standards that need to be in place.

Now, return to the questions asked in Lesson 1 and ask yourself:

- 1 Has my understanding of these ideas changed? If so how?
- 2 Are my explanations clearer and more convincing? If so, what makes them so?

LESSON 4 PRACTICAL STEPS

Introduction

This lesson offers suggestions for steps that can be taken to improve metadata management and protect the integrity of digital records through time. The lesson is divided into two parts.

The first part of the lesson describes practical strategies that can be adopted to address metadata management in an organisation. Based on the framework needed to manage metadata (laws, policies, standards, etc), the section uses the examples in Lesson Three to offer step-by-step practical advice. The section explains how the strategies are based on good practice, and it provides guidance on basic steps for establishing an organisation-wide framework for metadata management.

Building on the examples in Lesson Three, the second part of this lesson provides advice on how the concepts, issues and strategies associated with metadata management can be communicated to key stakeholders, such as senior business managers, IT and legal affairs specialists and development partners. These stakeholders must be persuaded that changes are needed in the way digital records are created, used and managed. The advice therefore includes:

- messages that can be used in presentations
- guidance on planning and organising briefing sessions and presentations
- advice on how to design and conduct interviews or hold formal and informal discussions with key stakeholders.

The goal is to enable records professionals to engage with stakeholders to gain the support they need to improve the management of metadata.

Practical Strategies

Two broad strategies will be needed and they can be pursued at the same time. These strategies are summarized below and then described in more detail.

- A *bottom-up* approach can focus on two or three smaller work processes where metadata for managing records is not being captured. By following this path, the experience gained can help to extend the strategy to more complex work processes.

- A *top-down* approach can be followed in parallel with or as a result of the first path. It will use the experience gained through addressing the work process metadata issues to develop, over time, the establishment of an organisation-wide framework for metadata management. The framework will include a policy, based on a set of accepted principles and a comprehensive set of standards (including a metadata standard) and practices, supported by qualified people that include skilled records professionals.

Bottom-up Approach

The following is a generic process that can be followed to address metadata issues associated with specific work processes.

Step One: What Are the Records?

Identify work processes that are generating high-risk records. For example, senior managers keep critical digital records (emails, office documents) on computers that are not accessible to the organisation and not covered by any records management controls. Taking another example, critical records that provide source data for a business system are poorly managed and difficult to access (eg supporting documents for payroll changes, payment vouchers and supporting documents for the accounting system).

High-risk records require more detailed documentation and more rigorous management controls and metadata. The following questions should help to clarify the nature and value of the records generated by a given work process:

- What is the value of the records to the organisation?
- What are the types of records that will be created in the work process and what is their format?
- How will they be identified, described, organised and classified?
- What is the level of sensitivity of the records (eg security, personal information, etc) and how and where will that be documented?
- How will they remain readable and useable into the future?
- What is the archival value of the records? Will they need to be retained as archives?

Step Two: What Are the Metadata?

The answers to these questions should help to clarify the characteristics and role of

metadata:

- What is the overall design of the work process (ie the steps in the process and the records they generate)?
- What types of records are being generated at each step in the process?
- What kinds of metadata are being used to access, retrieve, exchange, transmit, share and disseminate the records?
- What kinds of metadata are being used to identify, organise, protect, secure, retain, preserve and dispose of the records?
- Why are metadata needed?
- What purposes do they serve?
- What is the format of the digital records being described by the metadata?
- How will the metadata be captured?
- How will the metadata and digital records be stored, accessed and delivered?
- When will metadata be added/ captured in the life cycle of the digital records?
- Do metadata standards already exist (whether or not this is what they are called)?
- How are records and supporting metadata being retained - where, by whom, for how long?

Step Three: What are the Issues?

It is important to identify the issues that poor metadata management causes for the organisation and why they need to be addressed. If key stakeholders, especially managers of business units, are to engage in initiatives designed to improve metadata management they must see the benefits. The information acquired from the previous steps (finding out about records and metadata) will help to identify and analyse the issues. The kinds of issues experienced by organisations as a result of poorly managed metadata often can be divided into two categories. The first category concerns the use of metadata in managing the records. Examples include:

- Finding records (records can't be found because they weren't classified or indexed properly; there is no thesaurus or other tools to facilitate access and retrieval).
- Relating records (records documenting a given work process can't be related to one another so the full 'story' of what occurred cannot be understood).

- Authenticating records (tools such as audit trails, digital signatures and digital stamps, together with their supporting metadata, are not available, thus bringing into question the authenticity, validity and integrity of certain records).
- Controlling access and use (the security of records is placed at risk if metadata documenting access permissions, the security status of records and the related security provisions are inadequate or missing).
- Managing records through time (records needed for longer periods are unsupported and not migrated as technology changes; metadata that would trigger preservation action, including migration, are missing).

The second category concerns the impact of poorly-managed metadata on the performance of the organisation. Examples include:

- Business and operational issues: staff cannot find and understand the records and information they need to achieve their operational goals; poor metadata means that staff cannot do their job efficiently.
- Accountability (management and legal): metadata needed to support the organisation's ability to account for decisions and actions cannot be found; this undermines compliance with laws, policies and management accountability requirements.
- Development goals and priorities: metadata required to justify the need for development funds, account for the expenditure of the funds, and report on the achievement of development goals is not available.
- Global themes such as accountability, transparency, Open Government, Open Data, Big Data, Cloud Computing, etc: metadata are not available to enable citizens and other stakeholders to access and use information contained in records; in open data and big data initiatives, the absence of metadata can inhibit the ability to prove the integrity of statistics that were derived from source records.

Step Four: What are the Metadata Requirements?

Next it is important to understand what is in place and what is missing in terms of the metadata needed to manage the integrity of the records. What is missing with respect to the standards and procedures required to manage the integrity and trustworthiness of the metadata themselves through time. The analysis needs to consider for the three important sources of metadata:

- the records management framework
- the work process

- the records.

What needs to be done to close the gaps? This module can be used, along with the standards, guides and other references cited at the end of the module, to understand the requirements.

Requirements for Managing Metadata

Based on the ISO Metadata Standard (*ISO 23081-1:2006*) organisations should ensure that they can meet the following requirements:

- the ability to manage metadata at the point of records capture
- the ability to manage metadata after the record has been captured and is being accessed, used, retained, preserved and ultimately disposed of.

Within the context of these two higher-level requirements, organisations should ensure that policies, systems and procedures (separate or integrated in business systems or record-keeping systems) are in place to support the following:

- create and maintain metadata
- create and maintain structures for managing metadata
- determine when and how metadata should be captured
- document and enforce metadata standards
- store metadata
- describe metadata at various levels including systems, processes, functions, agents and organisations
- access metadata
- maintain metadata including management of metadata accrued through time as a result of actions performed on records (eg access and retrieval actions, preservation actions such as migration, etc)

Metadata Elements

Metadata elements are used to describe a given series of records. Many organisations around the world have developed metadata standards for use within all or parts of their

organisations. Several governments (such as Norway, Australia and Canada at the national level) and governments at the state level (New South Wales and Queensland in Australia) have established metadata standards to ensure consistency and the potential for sharing and exchanging records across systems and organisations. These standards should be consulted for examples of the types of metadata typically associated with records, how they are defined, and how they should be applied. References to these and related sources can be found in the section at the end of this module.

Step Five: Developing and Implementing the Strategy

Recommendations need to be developed to address the metadata issues associated with the work process. The strategy should be implemented by configuring systems and developing relevant policies, standards and procedures. This is discussed in more detail below.

Step Six: Evaluating the Results

Perform ongoing quality assurance. Assess the project in terms of moving towards the longer-term goal of establishing an organisation-wide framework for managing records management metadata.

Work Process Environment: Structured and Unstructured

The generic steps that have been defined need to be tailored to the nature of the work processes being examined. Typical organisations support work processes ranging from the highly structured (for example an FMIS) to those where the work processes are less well structured (for example word-processed documents, emails, spreadsheets, etc created by an individual employee). Some work processes involve a mixture of structured and unstructured (for example, preparing documentation and authorisations for a change to the payroll). The work process environment will have an impact on the nature of the metadata. Understanding the work process is fundamental to understanding how metadata are created and used, how well they are managed, and how their mismanagement can have implications for the business of the organisation. The work process environments are as follows:

The *structured environment* is characterised by application systems¹⁰ that support highly structured business processes such as those associated with licensing, financial management, tax collection, banking, air travel ticketing, etc. This is an environment where

¹⁰ An application system normally consists an automated business function or collection of functions, a user interface and a database of some sort to perform a specified set of tasks.

considerable care is normally taken in the planning, design, implementation and maintenance of the systems, where accountability for the integrity of the systems has been assigned, and where policies, standards and practices are well developed to ensure the ongoing integrity of the systems. In this environment where key stages of the records life cycle (eg creation, capture, and organisation) may already have been accounted for in the design of systems. However, rules for records' retention, long-term preservation and records' authenticity are often poorly addressed or not taken into account.

In well-designed systems, metadata will already be in place, and many of the records management metadata may already have been built into the metadata schema used to support the system (unique reference numbers, date formats, descriptions, identification of user, audit trails, etc). However, even well-designed systems may lack sufficient metadata to manage the retention, preservation and disposition of records. Records professionals have an opportunity to make a contribution by helping IT specialists and business managers fill this important metadata gap. More specifically, records professionals, with the help of IT specialists, can help ensure that records management metadata issues identified in Step 5 are integrated at each stage of systems development.

Figure 5: The Systems Development Life Cycle

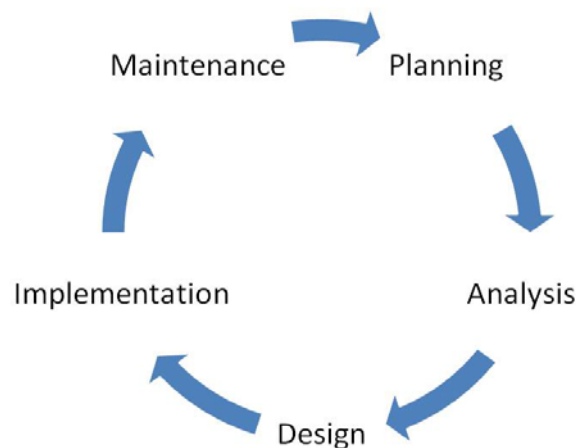


Figure 5 shows the stages in the systems development life cycle. The records and metadata issues for each of these stages are considered below:

➤ **Planning:**

Records management metadata issues, including missing retention rules; insufficient metadata to ensure the completeness of the record as a record, such as its creator; missing or inadequate links to related paper records should be identified and plans for addressing these issues should be integrated with the plans and subsequent steps of the system development.

➤ Analysing and defining requirements:

The requirements for records management metadata (eg retention information; links to paper records, etc) should be identified and integrated with the overall metadata requirements for the system.

➤ Integrating into a metadata schema:

The records management metadata should be integrated with the other metadata into a metadata schema supported by standards and rules. These should be translated into specifications that can be integrated into the overall design specifications for the system and into the standards and procedures for how the system will be used and maintained. Responsibility for certain aspects of the system, including the management of records, needs to be assigned.

➤ Testing:

The technical, procedural and other design specifications should be tested for their quality and integrity and the extent to which they meet the original requirements including those for security and records management. This step often includes pilot projects with selected users and user groups.

Training and implementing:

The system is implemented, often in stages. Training sessions, briefings and demonstrations are delivered to acquaint users with the new system¹¹; records management metadata trigger certain actions such as retention, preservation and disposition; users trust the records because metadata are complete and accurate; although records management metadata is captured automatically as much as possible, users respect their responsibility to contribute metadata as required (for example, naming conventions or the selection of a description from a drop-down list).

➤ Maintaining:

The metadata schema, standards and procedures should be reviewed on a regular basis and changes made as required.

➤ Reviewing and Evaluating:

Formal reviews and evaluations of the effectiveness and continued relevance of the metadata schema and standards should be conducted and modifications should be

¹¹ Training and awareness sessions are often the most important part of a systems development process, especially when it involved managers and staff who are to be the prime beneficiaries of the system. At times, it may become clear that records managers and IT staff may require training in order to enhance the knowledge and abilities they require to design, implement and maintain the system effectively.

made to the design of the system (including its supporting metadata schema) through a formal system modification process.

The strategy is not restricted to new systems being planned. Based on ongoing monitoring and formal evaluations, systems may need to be modified to account for factors such as the introduction of new technologies, changing business requirements, new policies, new workflows and other factors including those relating to records management (eg significant changes to retention requirements, introduction of a digital preservation process, etc). As in new systems, metadata requirements should be built into the formal steps that guide the modification of the system.

Using the FMIS (purchase of goods or services) as an example, the following points illustrate the kinds of issues to be discussed between the records manager, IT specialists, business managers and other stakeholders involved in the planning of a new or modified system:

- When the data entry clerk creates a new entry for the expenditure, how will the input form be linked to the supporting documents? For example, what is the unique control number recorded on the batch of input documents so that, when stored, they can be located easily?
- What are the standards for entering names in the FMIS? For instance, there must be standards for entering company names and contact details (eg no abbreviations, telephone numbers with country and area codes, etc)
- What is the audit trail record? The complete audit trail should include the time, user and any change made, each time the entry is accessed and each time a separate task is performed or data is added or changed (for example, an authorisation or approval, the addition of a Purchase Order number or a correction to the entry).
- How long will data need to be kept on the system? Accounting records may be destroyed after six years (from the end of the financial year in which the data was created) assuming audit is complete. Records that must be retained beyond six years must be identified (for example, management reports, contracts) and different rules applied. What are these records? Where are they stored?

In an *unstructured environment* processes are less well defined than the work processes in the structured environment. It is an environment dominated by email traffic, and individual workers having substantial autonomy over the way they create, transmit and store information. Some organisations may still be operating without an internal network that enables folder sharing, and this adds to the risk of disjointed and inaccessible records.

The documents generated and communicated in this environment (emails and other electronic documents) tend not to be managed by standards and procedures. In this kind of environment, work processes are difficult to define because the way information is created and communicated is dependent on the often-informal practices of individual users.

In many cases, digital records are stored in personal hard drives or in shared directories¹² (or folders) that are poorly managed. There are often few rules to guide users and accountability for the integrity of the records is weak or non-existent. In an office of 50 desktop users, there may be 50 different record-keeping systems. This situation is made more difficult if there is no shared drive where at least some common rules and standards can be applied. The issues associated with the unstructured environment cover every stage of the life cycle from creation to final disposition. Users may see the imposition of any rules or standards as an intrusion into their work or an unnecessary addition to their work load.

Identifying metadata requirements for the management of records in this environment can be challenging. Organisations typically face the following problems:

- There is confusion over which email messages and other electronic documents should be kept, which should be deleted and when.
- Deletion of records is left to the individual's choice.
- There are difficulties in accessing documents that are not saved on a shared drive.
- There are difficulties in finding information on shared drives because of the absence of commonly shared naming conventions for folders and ad hoc approaches to establishing directory structures.
- There is no version control or version control rules.
- There is no systematic approach to retention and off-loading or deletion of files and folders, and this creates difficulties in identifying those that are most significant in a given context.
- There are difficulties in bringing together the complete story behind a decision or event because email messages, their attachments and other related electronic documents may be stored in different locations and described in a variety of ways.
- There is no one with the authority to set standards and guidelines for good record-keeping practices on desktops.
- There is no one to set the business rules and maintain the shared drives for the benefit of those participating in a given work group or organisational unit.

In this kind of environment metadata schema do not exist or they exist in a very rudimentary form as a user-designed schema. As often is the case in developing

¹² Many people use the terms *directory* and *folder* interchangeably as a location on a disk for storing information about files. Directory is the older 'systems' term while folder is a term which sounds more familiar as it is like the paper file-folder found in offices. There is a difference: a folder is a logical concept that does not necessarily map to a physical directory on a disk; in other words, the contents of the folder may be physically stored as digital information in different locations.

classification schemes for paper records, an important step is to build a user-friendly standardised classification scheme that will benefit individual users in a given work group, while ensuring that basic records management metadata are in place.

Next Steps

For organisations in countries with limited resources, acquiring an EDRMS may be extremely challenging given the costs and the lack of available expertise to guide its design and implementation. For this reason, this module focuses on the initial practical and cost-effective steps that can be taken to enhance digital records management. The key is to develop a metadata schema for a shared directory that can be migrated easily to the schema developed for the EDRMS whenever such technology can be acquired.

Based on this approach, records professionals should take the following specific steps in developing metadata standards and schema (ie a classification scheme). This approach is recommended for shared drives but can also be used for stand-alone computers that are not networked. The approach is based on enhancing the ability of users to share information. The objective is to meet the needs of a given business unit by developing a metadata schema and a set of procedures that support the way individuals in the business unit carry out their activities. Rather than impose what may be perceived as a foreign, corporate-driven approach that would make the staff dramatically alter their work habits, this approach is designed to encourage users to move toward a new organisation-wide, information-sharing environment with minimal disruption to the way they work. At the same time, by introducing a standardised classification scheme and procedures, the approach represents a stepping-stone to an organisation-wide record-keeping system and records management framework.

An important point to be communicated to senior management is that the approach is cost-effective. Generally, directory/ folder management and classification can be improved using the existing hardware (eg shared drive) and software (network and directory management software, email systems, etc).

Finally, it is also important to note that if there is no shared drive, or the shared drive is not available to all users, the stop-gap practice of printing and filing in the paper filing system may be the only practical option for sharing and making the information available. However, the practice of using a standardised classification scheme for desk top and paper-based filing systems should still be undertaken and encouraged. The steps that follow refer to a shared drive, but they can be broadly applied to stand-alone computers.

Step 1: Preparation

- Where the shared drive is poorly managed and there are business-related issues such as difficulties in finding information and responding to formal requests for records, obtain the support of the senior manager responsible in addressing the issue. Keep in

mind that many managers faced with this situation will be more supportive when they realise that the solution will be user-driven and cost-effective.

- Through the manager, brief the IT contact for the unit on the initiative.
- Confirm the support of the IT unit in carrying out its role.
- With the support of the manager, ensure that all staff are aware of the initiative and understand the benefits. Staff must see that the manager owns and supports the initiative.

Step 2: Designing the Directory

- Review the current folder structure on the shared drive. Find out how many folders are managed on the shared drive (eg who creates them or changes them), if there are any existing rules for folder titles, how folders and documents stored in the folders are named, and, most important, how many folders are actually being used. In many cases a substantial number of folders are 'orphaned', or not used, because staff have left, the issues are old or initiatives have been completed and the documents are never used. Typically, many users only use anywhere from 12 to 20 folders to support their day-to-day activities. Some folders may need further investigation because they have been given poor or misleading titles (eg 'Meetings', 'Misc', 'Mary's folder').
- Review the relevant file titles from the part of the paper filing system covering the unit in question. If the paper filing system is well-designed and managed, parts of the structure can be used, eg the titles of file series or higher-level categories relevant to the functions performed by the business unit. Assess whether or not they can be used for the high-level folder titles for the new directory. If they cannot, new titles will need to be developed.
- The goal is to establish a reasonable number of high-level folder titles (eg between 8 and 15) reflecting the main functions of the business unit. Distinguish between folders for 'operational functions' (what the organisation does to fulfil its mandate) and folders for 'administrative' functions that are common to most units (Finance, Personnel, etc). Depending on the circumstances, such as the complexity of the functions, it may be useful to create three or four sub-folders (representing sub-functions or activities) under each main functions-based folder.
- With the help of the IT contact, create a new folder at the top of the directory; label it '000 new drive' so that it will always come to the top when the directory is accessed. The purpose of this step is to establish the root for an entirely new directory structure. Below the root folder ('000 new drive') create folders and sub-folders based on the folder structure developed in the previous step. When the time comes, staff will be advised that this higher level folder structure can only be changed with the approval of the relevant manager (supported by the records professional). However, when the staff folders are migrated to the new structure the (see below)

staff should be permitted to add and change file titles that are within the structure, based on standards and guidelines provided during the implementation phase.

- Consider whether to create three other types of folder. This will depend on the needs of the unit:
 - ◇ The first type, labeled 'personal', will contain sub folders for each of the staff in the unit. This will promote the idea that the same directory structure can be used to accommodate personal, non-work related documents, in addition to the records generated to support the operational and administrative functions of the organisation. This will demonstrate to staff that using the new directory will be as easy as using a personal directory, and it should encourage greater acceptance.
 - ◇ The second type acknowledges that a senior manager in the business unit may wish to have his/ her own private space in the directory structure. This goes against good records management practices but it helps to avoid managers creating their own folders outside of the new directory structure. If a senior manager says he/ she must have a private space, create a folder with a title such as 'Office of the Director'. The senior manager may insist on restricted access to the folder, but try to discourage this.
 - ◇ The third type of folder deals with the situation where important business-related documents in a folder become 'buried' in a large amount of reference material and cannot be identified quickly. In this case, advise users to create a special sub-folder under the main folder for this activity called 'Reference Material'. This can be used to store the large volumes of material that are not part of the 'corporate memory', while still linking the sub-folder (through the metadata) to the folder containing the documentary record.
- Based on the steps outlined above, develop simple guides and handouts for the staff in the business unit on: what are records, how are records filed in the new directory and what are the basic procedures for using the new directory. The guides should also contain naming conventions for labeling of file folders and digital records. Examples are available in references materials listed at the end of this module.
- Use the handouts and guides to brief the staff on how they will migrate to the new directory, how they will use the directory and what this role will be in managing its integrity. It will be very important to brief administrative staff on their role in supporting the management and integrity of the new directory. For instance, an administrative officer can offer advice on naming folder titles and documents. He/ she could also coordinate any changes to the higher-level folder structure on behalf of the manager of the business unit.

Step 3: Migrating Users to the New Directory on the Shared Drive

- With the support of the manager of the unit and the IT contact, organise a folder migration day and ask users to move the folders they are currently using to the appropriate sub-function or activity folder in the new directory. This should not be difficult because, as mentioned previously, typically most users have about 15 active folders that they use on a regular basis. They need not change their folder titles immediately. Be on hand to provide advice during this exercise. The migrated folders can be renamed over time in accordance with the naming conventions described in the guidance.
- By moving their folders to the new structure, staff in the unit will be functioning within the context of a corporate-driven metadata schema which, over time, can evolve to provide a framework for identifying, organising and describing records. However, the approach suggested here begins with the user, rather than an organisation-wide set of rules that are imposed, this is more likely to be seen as helpful.
- It is likely that a large number of folders will no longer be used. Some of these may have been created and used by former staff and their contents may not be immediately clear. 'Corporate records' that are easily identified and still have potential value may be moved to the appropriate folder in the new directory. All other documents may be moved to a specially created folder called 'Archive'. The folders can be reviewed over time to determine which should be moved into the directory structure and which should remain in the 'Archive'. This step ensures that the focus of attention is on moving forward with the new directory rather than getting held up trying to understand the titles and contents of folders that people never use. Over time, retention and disposition rules can be developed and applied.

Step 4: Using the New Directory

- Create a *site map* for the new shared directory. This will help users understand the directory. It will also facilitate access and retrieval by enabling users to search the site map and, through reviewing the folders, understand the context of the records being accessed. Guidance on creating site maps is freely available on the internet.
- Develop enhanced procedures on using the shared directory and organise and deliver briefing sessions on an ongoing basis, especially as the directory evolves in structure, scope and use. The procedures should cover: handling email (store with the attachments and other related digital records, not separately) security, retention, and other document handling and records management activities. Further guidance is available from the sources listed at the end of this module.

An enhanced shared drive directory has many benefits beyond facilitating information

exchange and retrieval. Based on a careful assessment of its use through time and the effectiveness of the metadata schema, it can serve as a stepping-stone for migrating of the organisational unit to an electronic document and records management system (EDRMS). An EDRMS is a software application that manages digital information such as email, word-processed documents, spreadsheets, images and scanned documents. An EDRMS can also control paper records and physical objects by capturing metadata about the paper records. An EDRMS enables desktop access to information across an organisation and provides the security, access, version control and audit functionality required for improved information management. An EDRMS can also deliver automated business processes, such as workflows and approvals.

While an enhanced shared directory and its classification scheme is a cost-effective user-driven way of managing digital records, it is not a records management system because it does not have all of the controls that would ensure the integrity and trustworthiness of the records through time. Above all, while the design and implementation of an improved shared directory is often facilitated by records professionals, they may not oversee its use. This is often left to the staff supported by an administrative assistant.

On the other hand, the design and implementation of an EDRMS, led by records professionals and based on the rigorous development of metadata schema, can help to control the creation and management of records throughout their life. An EDRMS can be expensive and highly complex to implement. However, if it is well designed and staff comply with its use and rules, an EDRMS can provide an effective corporate-driven (as opposed to user-driven) solution to the management of all forms of records including those in digital form.

Using the FMIS example (purchase of goods or services) how would the organisation file the documents generated in tendering and selecting a supplier and preparing the necessary documents before data entry in the FMIS. The following folder structure provides an illustration.

Top Level Folder	Sub-folder	Documents
Boards and Committees	Procurement Committee	Minutes and documents for meetings
Equipment and Services	Procurement	Records relating to the selected supplier and goods or services supplied, including documents prepared for FMIS
Equipment and Services	Contracts	Purchase order and/or contract
Finance and Accounting	Accounts Payable	Reports

Top-Down Approach

Developing a Metadata Strategy at the Organisation Level

Establishing an organisation-wide framework for managing records management metadata can be undertaken either in parallel with or subsequent to the work process initiatives introduced through the bottom up approach. Whether it is 'in parallel' or 'subsequent', it should build upon the relationships established with business managers, IT specialists and others as a result of involvement in the work process initiatives.

Introducing an organisation-wide framework for the management of metadata, there are a number of fundamental points that need to be understood.

- Records management metadata, including metadata for managing digital records, are most effective when situated in a comprehensive organisation-wide framework of policies, standards and practices, systems and technologies and people, supported by effective management structures and assigned accountability. Such a framework should be integrated in the overall framework overseeing the records management function of the organisation.
- In many organisations, records management is not recognised as a critical business function. There may be no unifying management structure for data, information and records, and there may be separate initiatives and responsibilities that fragment the management of the organisation's paper and digital records. Clearly, the records management and metadata management functions need to be positioned so that they are 'on the agenda' of senior management and treated as an essential component of the organisation's programmes and administration. Different approaches are possible, depending on the nature of the organisation. The essential point is that the design of the metadata framework and the overall records management framework should be aligned with, and have the same level of authority as the frameworks established for other valued resources such as human and financial resources.
- An organisation-wide metadata framework normally does not exist on its own. The objective is to enhance access to information residing in multiple sources across the organisation. To use the payroll example, while IT specialists and senior managers may not use the term 'records management metadata', they will know that the integrity of payroll records must be maintained. To do this, the payroll system must capture payroll records' metadata, as explained in earlier lessons. If records professionals are aware that other initiatives are underway (for example, to introduce or upgrade a major business application such as HR management or financial management) they should join the effort and ensure that records management considerations are taken into account.
- For most organisations, establishing a comprehensive metadata framework is a long-term goal. In spite of the absence of such a framework, records professionals should aim to work towards it.
- In moving forward, it is essential to identify a senior level champion who can communicate the benefits of such a framework to other senior colleagues. The objective is to enhance access to information in all forms across the organisation. The

metadata framework is the means of achieving this, and the senior level champion should communicate it.

- Securing the support of a senior official will require the development of a proposal document, such as a *concept note*, to argue why such a framework is required and to outline the strategy for its development. A full business case with costs should be prepared later after securing the necessary support
- Developing a policy, as described in the concept note, is essential. The policy should include the following points (as described elsewhere in this module):
 - ◇ basic principles relating to the creation and management of records management metadata (as described in Lesson One); this should embrace all physical forms of records, not just digital.
 - ◇ roles and responsibilities, including responsibilities for the policy and quality assurance of metadata
 - ◇ high level metadata requirements
 - ◇ a high level metadata standard for the organisation
 - ◇ how the policy will be evaluated.
- Developing the policy and its supporting standard will require considerable consultation. Users across the organisation need to understand how the policy will impact them and benefit their work.
- Given the organisation-wide scope of the policy, a steering committee comprising representatives from all the functions and areas that it will affect will be required. The manager (preferably a records professional) should be named to oversee the development and implementation of the policy and the standard.
- The policy will need to be kept current, for example to account for changes in the organisation's functions and operations and the impact these changes will have on the metadata requirements and the standard.
- The policy and the standard should be tested in one or two business areas to assess the impact of its implementation.
- The policy and the standard should be disseminated and guidance provided on their implementation.
- The policy and standard should be monitored and evaluated and adjustments made as required.

The records professional's ongoing roles and responsibilities for implementing the policy,

which should be carried out in partnership with other stakeholders, are described below. These roles and responsibilities should be seen as long-term objectives:

- analysing the needs of the organisation for records management metadata based upon business requirements
- monitoring and analysing developments within the organisation relating to metadata, particularly requirements for managing and maintaining trustworthy records
- ensuring that metadata schemas for managing records are developed in accordance with best practice and applicable industry standards
- developing the metadata framework for managing records, including the metadata schema, and related organisational standards and the rules for using them
- identifying or developing appropriate metadata encoding schemes (eg rules for classification)
- keeping the metadata schema up-to-date and in line with business needs
- managing the metadata schema as a record in its own right
- maintaining the overall quality of both machine-generated and human-generated metadata, particularly its accuracy, integrity, authenticity, usability and reliability
- coordinating implementation issues between records and IT staff
- coordinating with business system owners to ensure integration of metadata for managing records into business systems as appropriate
- coordinating with archival authorities to ensure interoperability between records application software and archival environments for those records that have archival value
- setting up a training programme and subsequent training of staff on the use and application of the metadata schema
- communicating about the metadata schema within the organisation.

As explained and illustrated in the work-process initiatives (see Part One above), the nature of records-generating work processes is far ranging, from highly structured (eg an FMIS to mostly unstructured (eg office systems). Establishing a *detailed* organisation-wide metadata schema that incorporates the metadata schema for all work processes is not only impossible (it would conflict with existing work process specific metadata schema) but also counter-productive. On the other hand, if the organisation is to achieve its objectives of enabling information interoperability (information access and discovery across work process boundaries) some form of high-level metadata model and standard is required.

International good practice suggests that an organisation-wide records management metadata model should be based on describing the functions and activities of the organisation. This function-based classification scheme should document the purpose for which the records were created. It captures details about the functions, activities, transactions and related records created, used and managed across the organisation. A function-based classification scheme differs from a subject-based classification scheme in that it:

- classifies records to identify their location within the organisation’s functions and their links to other related records
- maintains the links between the records and the context within which they are created (a requirement critical for digital recordkeeping)
- maintains details about the records and the activities they support over time
- identifies ownership of the records
- assists with the development of disposition authorities/ retention schedules
- helps determine the appropriate security protection for the records at the activity level, rather than at the folder level in the subject-based system.

Although subject-based schemes have been in use for many decades in many organizations, they are not advocated for the management of records in a digital environment. Figure 6 provides a comparative assessment of the subject-based and function-based classification schemes.

Figure 6: Subject-based vs Function-based Classification

Subject-based	Function-based
Context: What the record is about.	Context: What the department does and why the record was created.
Owner: Organisational name at the top of the scheme. Purpose for creating the records is not clear and there is little information about the evidence the records can provide.	Owner: the top level provides a descriptive ‘label’ for the business function or process that is supported. The top-level functions are represented at the top level of the classification scheme.
Events/ actions are at the bottom of the classification scheme, after the subject.	Functions and activities are described at the top and middle of the system; therefore the purpose of the records is much more clearly defined.

Subject-based	Function-based
Titles: The creator or the registry staff chooses the subject terms from the scheme to define the record context.	Titles: the terms are derived from the business functions and activities in consultation with business owners and RM staff. Subjects are defined at the lower folder level.
General files: General files are accommodated in the system. Retrieval is difficult because records related to a variety of topics can be found in the same file.	General files: there are no general files in the scheme because all records are related to a particular function and activity.
Retrieval: Searching to find the relevant document requires a review of more information because activities, events or actions are spread throughout multiple file 'volumes' (ie continuations of the same file).	Retrieval: Searching to find the relevant documents/records require a review of less material because the activity has been separated out into specific files.
Disposition: Because records are linked by subject, files mix together records of short-term value and long-term value. Disposition rules are difficult to apply and often files have to be reviewed document by document to determine whether they have on-going value.	Disposition: It is easier to group records of similar on-going value because they are organised by function and activity. Disposition rules are more easily applied.

Comparing the two schemes, the function-based classification scheme is more focused on business activities and transactions. It maintains the relationships between the records and the business activities more closely than the subject-based scheme and it means that disposition rules are more easily applied. For these reasons that organisations around the world are shifting to functions-based classification schemes.

The identification of functions should be based on an analysis the mandate of the organisation and a review of documents such as strategic plans, financial accounting reports and reports to central government, parliament or other equivalent organisations. These documents are often structured according to the main functions of the organisation, not by organisational structure, though the two may be related. The labels given to the functions can often serve as the labels for the high-level classification scheme. These can be used to establish a hierarchy of sub-functions and activities (ie programmes, services and work processes) at the lower levels. It is important to remember that functions are 'what' the organisation does (eg human resources management, mining, banking, education and schools, etc) and activities and work processes are 'how' the organisation carries out its functions (appointments, extracting resources, personal banking, setting standards in schools, etc).

It is also important to remember that the highest level of the scheme will be generic across the organisation while lower levels will use terms and hierarchies that are in line with the nature of the work processes. It is at these lower levels that links will be established to the metadata schema established for each of the work processes. If the links are effective and the metadata schema is complete, the outcome is a comprehensive classification scheme (or metadata scheme) that covers the entire organisation.

Function	Sub-function/work process/ folder	Activity/ Documents	Metadata examples
Boards and Committees (organisation management)	Procurement Committee (oversight of procurement)	Meeting of the Procurement Committee: minutes and documents needed to evaluate tenders	<ul style="list-style-type: none"> • Unique tender number • Signature of Committee chairman • List of people present
Equipment and Services (acquiring, using and managing the material resources and services needed to run the organisation)	Procurement (acquiring new equipment or services that are needed)	Selecting the supplier which best meets the requirement in terms of quality and cost: records relating to the selected supplier and goods or services supplied, including documents prepared for FMIS	<ul style="list-style-type: none"> • Unique tender number • Suppliers' names, contact details and company registration number
Equipment and Services	Contracts (entering a legal agreement with the supplier to provide the goods or services)	Purchase order and/or contract: issuing the legally binding agreement	<ul style="list-style-type: none"> • Unique tender number • Unique purchase order • Contract number • Suppliers' names, contact details and company registration number.

Using the purchase of goods or services as an example, how are these principles applied? The following table sets out a simplified version of a function-based classification scheme that reflects activities and work processes.

Establishing a Target Vision

In moving forward, it is important to establish a vision of what should in place to manage and use metadata, both within individual work processes and across the organisation. Short and medium-term initiatives are needed to enhance the management of metadata, but there should also be a longer-range vision that can serve as the overall goal to guide the various initiatives.

Norway's Example

The Government of Norway has developed such a vision and turned much of it into reality, as described below. The Government of Norway has established a comprehensive framework supported by the NOARK standard (Norwegian Archive Standard). Norway's vision is being achieved through a powerful combination of inter-connected laws, standards, well-defined metadata architectures and technology systems that make it possible for citizens to access authoritative and trustworthy government information. Among the most striking aspects of Norway's approach are the emphasis on protecting the security, content and context of the information and reducing the time between creating records and public access. The Government is committed to meeting increasing citizen expectations for rapid, almost 'real time' access to information.

The components of the framework, which are the same components of the records management framework described in Lesson 1, are as follows:

Laws and Policies

- The Constitution, the Freedom of Information Act and the National Archives Act and its national record-keeping standard, have all been made to work together to provide a comprehensive legislative umbrella.
- The right to follow the proceedings of government and to the protection of privacy are enshrined in the Constitution, which gives the government the 'responsibility to create conditions that facilitate open and enlightened public discourse'¹³.
- The principle is accepted that 'archives' means the whole life cycle of records and that archives have a role in facilitating proper management.
- The legislation is used to establish a government-wide approach to managing the integrity of records and in positioning archives.

Standards Framework

- There is a standardised approach to records registration. A records registry system is

¹³ Constitution of the Kingdom of Norway, Article 100.

in place; this is used as the platform for standardised metadata to control incoming and outgoing documents/correspondence.

- There is a standard for records identification, labels and structure, as well as format standards for records transmission.
- Standards enable records to be rendered according to their original structure, showing relationships and original context to protect authenticity and accuracy.
- Metadata document the records' creation and any subsequent alterations, thus creating an audit trail of context: this establishes a governance audit trail, which enables 'traceability'. Traceability refers to the completeness of the information about every step in a process.

Systems and Technology

- Noark is based on functional requirements that must be complied with by vendors.
- While the Noark standard was for documents originally, it is now being applied to all systems where records are generated. Eventually it is likely to be extended to support open data initiatives where the ability to account for records traceability will be key.
- Noark stipulates minimal requirements that must be respected; the focus is on records integrity and authenticity.
- Noark contains requirements for system functionality throughout the record lifecycle (capture, maintenance, retrieval, disposition); metadata templates and integrity requirements for locking metadata and records; standardised processes for electronic document exchanges and for securing authoritative digital signatures; guidance on producing statistics and reports; rules for transferring records to repository control; and rules for identifying and authorising system users, allocating and administering access rights, and establishing log and audit trails.
- Under FOI law and supported by Noark, every ministry is required to produce a register of metadata for an online portal (the OEP). The portal provides central access to all records. The register records the date the document was drafted; the date it was registered; document number; sender; recipient; a meaningful description of the content; filing code; and date and manner of closure. A document, including email, is available for access as soon as it is produced, received or transmitted by a central government agency unless the law restricts it.
- The work process makes everything work together. There is always a work process involved which is why Noark is applicable across all systems.
- A trusted digital repository (TDR) is under development to provide reliable, long-term access to all managed digital resources.

- Records are transferred to the archives within five to ten years to protect the integrity of records even if they are to be retained for 25 years within the ministry.
- The TDR will be a technology-neutral means of preserving the records using standardised digital preservation models, compliance with international IT security standards as well as appropriate elements of the Open Archival Information System (OAIS) and the Trusted Repository Audit and Certification checklist.
- Metadata standards and transfer format standards will facilitate transfer to the TDR; certification processes will verify integrity of the TDR and the records.

People

- Relevant staff in the ministries are trained in Noark and in complying with the work process governing the identification, indexing and protection of records documenting government actions and decisions.
- Archives staff are qualified to assume a leadership role in developing and maintaining Noark and ensuring its effective application and use across the Government. They have the expertise (in partnership with others) to build the remaining components of the vision such as the TDR. IT expertise is available within the archives.

Governance and Management

- Oversight and direction are provided by a high level senior steering committee comprising senior officials in lead ministries including the Archives.
- A relevant and effective governance structure exists for the approval of standards.
- An accountability framework, reflected in policy, assigns responsibility to officials at all levels across the government.

Achieving a vision reflecting the qualities of the Government of Norway's Noark initiative is a substantial task; it will take time to develop. Nevertheless it is essential to establish a vision of what could be achieved, if only to guide short and medium term initiatives and ensure that they are heading in the right direction.

As in Norway's case, it is essential that the vision can be understood by senior managers and staff in the organisation. If they do not understand the vision or, worse, cannot see any value in it for themselves, the effort will be useless. The ideal is for senior managers to own the vision and be prepared to support the short and medium term initiatives established to move towards it.

Developing a vision of the future can be as basic as identifying and researching innovative and 'visionary' initiatives such as Noark, reviewing the literature for ideas and, most of all, discussing with business managers and others (IT specialists) what they see as an ideal state for the future.

Communicating the vision and gaining support must be part of a broader approach to engage with key stakeholders in the organisation. Suggestions for doing this are given in the next section.

Communicating Concepts, Issues, Significance and Strategies to Stakeholders

This section provides guidance on how records professionals can communicate metadata concepts, issues and strategies to key stakeholders to secure their support in incorporating metadata management in organisational systems and work programme, and obtaining the resources to fund this work.

Sometimes the most challenging step is to begin the discussion with senior colleagues and IT specialists. Will they ask difficult questions? Will they say it is not a priority? Will they say it is not a matter that should concern a records manager? Gaining the support of colleagues is a crucial because records professionals cannot address the issue of metadata management on their own (or any records management issue involving the management of digital records). Partnerships, especially with senior managements and IT specialists are essential. Unfortunately, few records professionals feel they have the knowledge and expertise to engage in a meaningful conversation with their stakeholders. As a result, discussions are not held, partnerships are not formed, and the failure to tackle records management metadata issues continues to put the organisation at risk.

The information in this module is intended to build the knowledge needed to have these discussions and to encourage constructive communication between records professionals and key stakeholders.

Before beginning the conversation, records professionals should prepare themselves by taking the following steps:

- Review the material covered in this module and ensure that you are comfortable with the concepts, the examples and the suggestions being made.
- Research the organisation where metadata requirements are to be introduced:
 - ◇ Know its business functions and work processes; where are records being generated, how are they being managed and who is responsible for maintaining their integrity?

- ◇ Know the key officials who are managing the work processes; who are they and what are they like? Are they potential allies or will they inhibit progress? Be careful in identifying IT specialists. Many are technical specialists who will have little interest in metadata issues and only maintain existing systems. However, there will be some (perhaps not working full time in the organisation) such as business systems analysts, data managers or information architecture specialists, who will be familiar with metadata concepts and who will be interested.
- Based on this research, identify metadata issues for individual work processes and at the organisation-wide level. This does not have to be an exhaustive analysis (more details will come from the conversation with business managers and IT staff). It is simply a way of 'jump-starting' a discussion, especially if a stakeholder says he/ she is not experiencing any issues. Ideally, the work process(es) selected to start the discussion will be highly visible and important to the organisation.
- Identify an individual (preferably a business manager but it could also be an IT specialist) who would be most receptive to a discussion about records management metadata.
- When you feel that you are well-prepared, arrange a meeting with the individual. The objectives of the meeting should be to:
 - ◇ establish a sound and productive working relationship based on respect and trust
 - ◇ explore records management metadata issues within key work process(es) supported in the individual's area of responsibility; examples should be relevant to the key work processes, for instance, issues relating to: data/ records accuracy and completeness; finding data/ records; understanding information contained in the records; security and protection of records; access issues; audit trails; records retention and disposition
 - ◇ identify practical steps to address the issues; this could involve further meetings, perhaps with the individual's work group, with more senior staff and other stakeholders, where you would both present the results of your initial discussions; practical steps could include, for example, integrating records management considerations in existing initiatives or establishing an entirely new initiative (eg setting up an enhanced shared directory).
- Use the concepts, issues and suggested approaches described in this module to shape the nature of the conversation.
- The issues you raise should always be related to the business of the organisation (ie delivering programmes and core functions, making decisions and responding to strategic priorities including open government and access to information); they should also be of special relevance to the business-related interests and needs of the

individual.

- A test of the effectiveness of the initial conversation(s) is to evaluate the following:
 - ◇ Comprehension: did the individual get the message, the main idea, the point? Was it easy to get your message across?
 - ◇ Connection: if the individual 'got it', did he/ she want to do something about it?
 - ◇ Credibility: The individual needs to believe *who* is giving the message, *what* is being said, and *how* it is being said; otherwise the connection begins to break down.
 - ◇ Contagiousness: The individual should not only understand the importance of message but should want to 'run with it' and to spread the message among other stakeholders. You have raised important issues that need to be addressed. To be contagious, a message has to be new, different and memorable. It should offer a new insight that has relevance to the individual's own situation and to the organisation as a whole. It should motivate the individual to do something.
- Confirm the next steps with the individual. This could include a number of actions. For instance, you might agree to brief the individual's team to explore options for dealing with the issue, based on suggestions raised during the meeting, alternatively there could be a briefing with the individual's manager and/or with a group of key stakeholders to enhance their awareness of the issues and propose an overall strategy. The key is to use the initial meeting(s) as a stepping stone to inserting the records management metadata issues inside the organisation's thinking and to insert the records managers in the processes for building or modifying systems where records management metadata issues will need to be addressed.

The objective is to enhance awareness of the importance of records and records management metadata, and to have key stakeholders act on this awareness. It will be difficult to proceed any further if this awareness is not in place and stakeholders are not prepared to act.

Engaging with a senior manager or group of senior managers has to be handled with care. They do not have a lot of time and their attention to any single issue will be limited, especially if it is not already on their 'agenda'. In this case it may be more productive to integrate briefings on records management metadata in briefings on wider issues. These could be, for instance, progress being made on new systems or significant modifications to existing systems. That is why it is so important to establish a sound working relationship with business managers and IT specialists. It is often through them that records management considerations such as records management metadata will be heard.

In certain circumstances, it may be possible to meet with a senior official or a group of officials to brief them on records management and, within that context, the role and

importance of metadata and the issues and risks faced by the organisation. Rather than simply providing a briefing for information, it would be preferable if the session could propose initiatives to address the issues. The following steps are suggested for handling such a meeting. They can also be used to guide any meetings with managers or senior officials about records management metadata:

- Explain what you want out of the meeting in the first two or three minutes of the session. Make a list before the meeting of the points you want to raise. Keep the list to three points.
- Do not ask a long series of questions:
 - ◇ Explain the purpose of the meeting (eg to understand metadata issues; to obtain support for an upcoming meeting where records management metadata will be discussed; to request that they serve as a 'champion' for advancing the issue).
 - ◇ Ask the senior manager or official to state how he/ she sees his/ her official responsibilities in relation to records and metadata issues and the wider issues of access to reliable and meaningful information; this will give you an idea of how the points you are making will be important to them.
 - ◇ Provide a general understanding of metadata concepts; this should be accomplished quickly to set the context for the points that follow; do not over communicate.
 - ◇ Ask about their concerns for the management of digital records and metadata generally from three perspectives: themselves as senior managers, the functions and activities for which they are responsible; and the organisation.
 - ◇ Ask for any suggestions they might have for addressing the issues; here is where you can offer some ideas, though in doing so they should be presented in a way that the senior management can see, understand and own them.
 - ◇ Bring the session to a close by returning the original objectives for the meeting: providing information to enhance awareness; asking them to serve as a champion; or asking them to support the metadata initiative (eg securing cooperation of the managers and staff in their business area; seeking the support of peers at the senior executive management table; etc).
- Keep the session to between half an hour and one hour.
- Take notes during the meeting but do not dominate the meeting with note taking; you need to be as engaged as the senior manager.
- Afterwards, send an email or other communication expressing thanks for the meeting and giving a brief summary of the main points covered.

Collectively, the initial meeting with a potential partner, the briefings delivered to key stakeholders and the enhanced awareness session with senior officials will set the stage for a cooperative approach to be taken to address the records management metadata issues that have been addressed. Equipped with the knowledge presented in this module and from additional resources identified at the end, the records professional should be seen as a valued member of the team. Only the record professional knows about records and what is required to ensure that they are properly managed, including how they are identified, described, organised and classified. The key is taking the right steps to make IT specialists and senior managers understand that this knowledge and your expertise are needed. The guidance presented in this lesson together with the material covered in the module as a whole will help records professionals to achieve this goal.

Assessing Student Understanding of the Lesson

With the guidance in this lesson, you should now be in a position to start to plan the practical strategies and actions needed to introduce metadata control within your organisation within an organisation with which you have had experience. This will involve communicating effectively with stakeholders and defining the steps needed to introduce a relevant policy, metadata standards and schema and a classification scheme. Develop an action plan for achieving this.

There are several activities that will help you define these strategies and actions.

Practising Your Case

Have a friend or colleague time you and give yourself one minute to make the case for proper metadata management in a given context (this could be your organisation, or you could imagine another one). You could also do this in a group and give everyone a chance to make their case before voting for the one that is the best.

You could also practise making the case to a variety of different audiences. For example, pretend you are talking to a member of the public or a senior manager or your own manager, and think about how you have to change what you say.

Start Doing Background Research and Plan Your Next Steps

If you are working in an organisation, start to undertake some of the research suggested in this lesson and plan the actions you will take next in developing both top-down and bottom-up approaches.

Additional Resources

Glossary of Terms

Unless indicated otherwise, the definitions described below are from the Glossary developed as a result of the InterPARES 3 Project, University of British Columbia, Vancouver, BC.

Activity: A series of acts or actions aimed to one purpose.

Archival description: The creation of an accurate representation of a unit of description and its component parts, if any, by capturing, analysing, organising and recording information that serves to identify, manage, locate and explain archival materials and the context and records systems which produced it.

Attribute: A characteristic that uniquely identifies a record or a record element.

Authenticity: The trustworthiness of a record as a record; ie the quality of a record that is what it purports to be and that is free from tampering or corruption.

Classification: The systematic organisation of records in groups or categories according to methods, procedures, or conventions represented in a plan or scheme.

Classification code: A series of alphabetical, numerical, or alphanumerical symbols used to identify the record in its documentary context.

Classification scheme: A plan for the systematic identification and arrangement of business activities and records into categories according to logically structured conventions, methods and procedural rules.

Complete record: A record that contains all the elements required by the creator and the juridical system for it to be capable of generating consequences.

Context: The framework in which a record is created, used, and maintained.

Data set: A collection of sets of information that is composed of separate elements but can be manipulated by a computer. (Oxford Dictionary)

Describe records: To record information about the nature and make-up of records acquired for permanent preservation and about their juridical-administrative, provenancial, procedural, documentary and technological contexts, as well as information about any changes they have undergone since they were first created.

Digital Object: An object composed of a set of bit sequences (Alliance for Permanent Access glossary) Digital objects include, for instance, digital records, digital photographs, audio and

video files, e-mails, spreadsheets, digital surrogates (images created by scanning or digitally photographing paper records), etc.

Digital record: A digital document that is treated and managed as a record.

Emulation: The reproduction of the behaviour and results of obsolete software or systems through the development of new hardware and/or software to allow execution of the old software or systems on future computers.

Encoding: The representation of symbols in some alphabet by symbols or strings of symbols in some other alphabet. See also: analogue encoding; binary encoding; byte-serialised encoding; cipher-text; digital encoding; durable encoding; encryption; metadata encoding scheme.

Function: All of the activities aimed to accomplish one purpose.

Ingest: To accept one or many submission information packages (SIPs) into an Open Archival Information System (OAIS). The ingestion process prepares archival information packages (AIPs) for storage and ensures that they and their supporting descriptive information become established within the OAIS. (International Organisation for Standardisation).

Integrity: The quality of being complete and unaltered in all essential respects.

Metadata:

- Information that characterises another information resource, especially for purposes of documenting, describing, preserving or managing that resource. (*Interpares 2*)
- A characterisation or description documenting the identification, management, nature, use, or location of information resources (data). (*SAA*)
- Structured information that describes and/or allows users to find, manage, control, understand or preserve other information over time. Metadata is attached to records when they are created and added to as a result of different processes such as sentencing and disposal. (*National Archives of Australia*).

Metadata application profile: A declaration of the metadata terms that an organisation, information resource, application, or user community uses in its metadata. In a broader sense, it includes the set of metadata elements, policies, and guidelines defined for a particular application or implementation. The elements may be from one or more element sets, thus allowing a given application to meet its functional requirements by using metadata elements from several element sets including locally defined sets. An application profile is not considered complete without documentation that defines the policies and best practices appropriate to the application.

Record: A document made or received in the course of a practical activity as an instrument

or a by-product of such activity, and set aside for action or reference.

Record characteristic: A quality that belongs to all records, such as a fixed documentary form, a stable content, an archival bond with other records either inside or outside the system, and an identifiable context.

Record element: A constituent part of a record's documentary form; an element is a formal expression visible on the face of the record (eg a signature).

Guide to Relevant Metadata Standards and Guides

Metadata standards are essential to the effective management and use of metadata, especially in an organisational context. The lists below draw on existing tools to present an overview of the key international metadata standards with which records professionals should be familiar. The goal is not to provide an exhaustive list of standards but to explain how key standards provide the framework required to enable metadata to be created, structured and applied to help support the integrity of digital records.

In approaching and using metadata standards it is important to become familiar with metadata concepts through the information provided in this module and various guides that have been made available by leading organisations around the world. An example of one such guide that provides a good general overview of metadata can be found in the *Understanding Metadata* guide, produced by the National Information Standards Organisation (2004). While it is primarily directed to the library community, this short guide defines metadata, the main types and functions of metadata, and offers a practical approach to structuring and sharing metadata schemas.

With respect to records management metadata, the key standard that should be referenced is *ISO 23081---2:2009 Information and Documentation – Records Management Processes – Metadata for Records*. *Part 1* of the standard covers the principles governing records and their metadata, the processes that affect them, the systems in which they are created and maintained, and organisations responsible for their management. *Part 2* establishes the framework for defining metadata elements in order to enable the standardised description of records, and to support interoperability of records and metadata over time, across space and across applications. It identifies issues arising in the implementation of metadata for managing records and the options for addressing these issues.

The international standard is important to understand and acknowledge for three reasons:

- it is an international standard approved at the highest level of the global standards process; as an ISO standard, it is recognised and respected world-wide
- it is based on exhaustive consultation and input from experts around the world; it has credibility

- given its status and its applicability in any records management environment, it can be used as a talking point in conversations with various stakeholders including business managers and IT specialists.

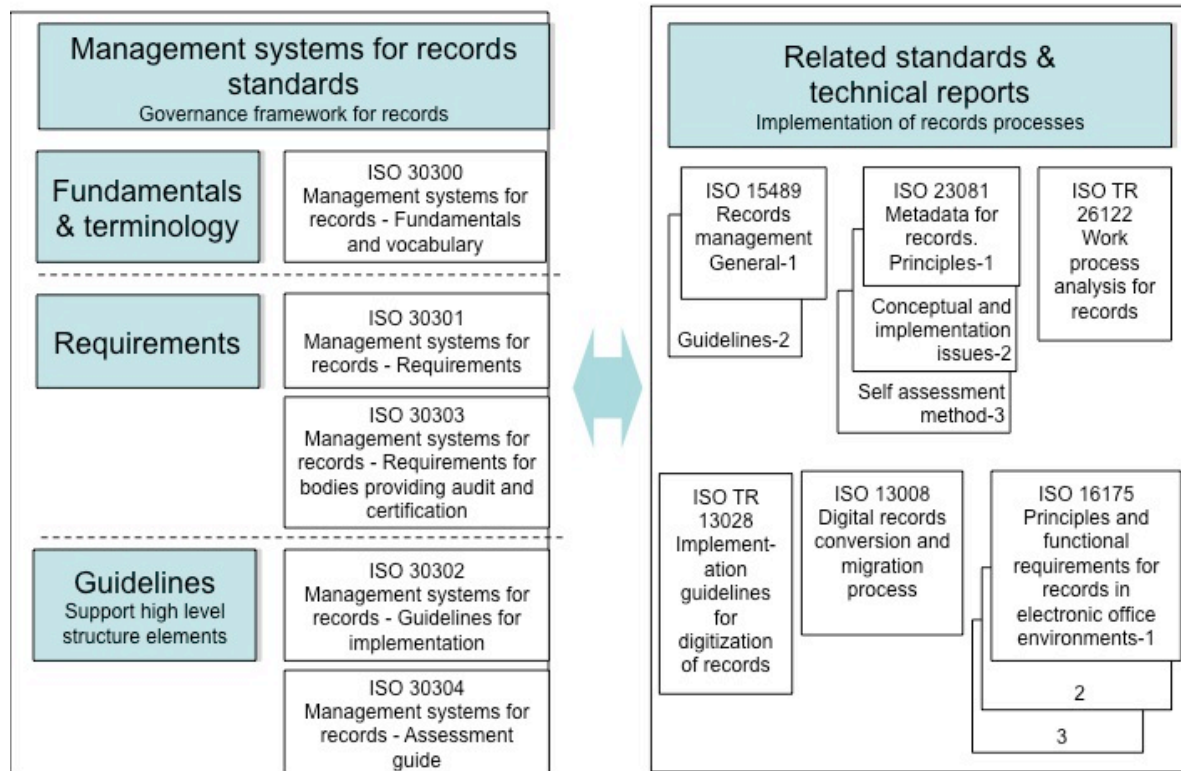
The standard does not stand by itself. As mentioned in the module, an effective framework for the management of records, regardless of their physical form needs to be in place as an important pre-condition. Several other ISO standards address the establishment of a framework and should be reviewed with *ISO 23081*.

One of these is *ISO 15489: Information and Documentation -- Records Management*. This has been an important foundation standard for many years and has been adopted by many organisations around the world. It is highly influential and to date has been adopted in over 50 countries and translated into 22 languages. Entire governments, at the national and local levels, have adopted the standard either in whole or in part. It is especially important for governments because it provides a framework for the establishment of the records management policies, programmes and systems that are required to meet accountability requirements, support government operations and achieve strategic priorities including e-Government, open data and open government. The *ISO 15489 Standard* is in two parts. *Part 1* describes the components of a records management system. *Part 2* sets out detailed guidelines on how *Part 1* can be implemented. Together the two parts complement the ISO metadata standard.

The most important development in recent years has been the issuance of the *ISO 30300* series of records management standards. These standards were developed by the ISO's Technical Committee 46/Sub-Committee 11. The committee comprises 27 experts from around the world, many of who were involved in the development of the first ISO standard on records management (*ISO 15489*). While *ISO 15489* was directed to records managers in organisations, the audience for this new series of standards is managers. The *ISO 30300* series of International Standards, 'focuses on the implementation and operation of an effective management system for records to ensure that authoritative and reliable information about, and evidence of business decisions and actions are created, managed and made accessible to those who need it, for as long as required.'

The *ISO 30300* series is comparable to the well-known *ISO 9000* series of standards that have had a significant influence on the world-wide manufacturing industry. The goal is to develop a similar series of internationally recognised quality standards for the management of records, especially those generated in electronic form. However, rather than being directed to the manufacturing sector, the standards are intended for all types of organisations including governments. Over time, and similar to the experience with *ISO 9000* standards, the goal is to establish an agreed upon benchmark for international best practice in the management of records. Two standards that have been made available are *ISO 30300:2011, Management Systems for Records – Fundamentals and Vocabulary*, and *ISO 30301:2011, Management Systems for Records – Requirements*. The full suite of existing and planned standards in the *ISO 30300* series is described in Figure 7. The figure describes where the metadata standard is positioned relative to the *ISO 300* series of standards and other standards and ISO technical reports that, collectively, form the suite of ISO records management standards.

Figure 7: Relevant ISO Records Management Standards



A number of national archives around the world, especially in Australia, have used the standard to produce their own standards as well as guides to how records management metadata should be created and managed (see the annotated list that follows this section).

An excellent standard as well as a guide is, *Queensland Recordkeeping Metadata Standard and Guideline*, produced by the Queensland State Archives (2012). It identifies metadata elements required to manage records in accordance with best practice and provides guidance on implementation. It contains both a guideline on understanding and applying record-keeping metadata and a technical standard that identifies and defines metadata elements and specifies whether they are mandatory or optional. It is clearly written and the guidance it provides can be easily applied and/or adopted. It also provides guidance on implementing a metadata strategy, a topic that will be of particular interest to records professionals seeking a step-by-step approach to enhancing metadata management in their organisation.

Annotated List of Standards and Guides

Primers on Metadata

JISC (2010)

An Introduction to Metadata

<http://www.jiscdigitalmedia.ac.uk/guide/an-introduction-to-metadata>

This is the first in a series about metadata, and is aimed at those developing managed and sharable digital collections. This document defines metadata and introduces basic concepts.

ARMA

Why Metadata Matters

<http://www.arma.org/bookstore/files/Franks-Kunde1.pdf>

ERPANET

Getting what you want, knowing what you have and keeping what you need.

Metadata in digital preservation

<http://www.erpanet.org/events/2003/marburg/finalMarburg%20report.pdf>

Other Standards and Guides

Among the many standards and guides that have been developed in countries around the world, several are relevant to records professionals working in low resource environments.

National Archives of Australia

Australian Government Recordkeeping Metadata Standard (2008)

http://www.naa.gov.au/Images/AGRkMS_Final%20Edit_16%2007%2008_Revised_tcm16-47131.pdf

The standard describes information about records and the contexts in which they are captured and used. This is information that the National Archives recommends is captured in business systems used by Australian Government agencies to create and capture records. It is based on a multiple-entity model, allowing for the description of five separate entities: Record, Agent, Business, Mandate and Relationship. It defines a basic set of 26 metadata properties and an additional 44 sub-properties that may be used to describe these entities.

The State Records Authority of New South Wales

Introducing Recordkeeping Metadata

<http://www.records.nsw.gov.au/recordkeeping/government-recordkeeping-manual/guidance/recordkeeping-in-brief/recordkeeping-in-brief-18#mandatory-recordkeeping-metadata>

The guidance begins with an overview of metadata concepts, continues by describing mandatory metadata requirements and concludes with links to guidance on implementing metadata strategies in an organisation.

Archives New Zealand

Electronic Recordkeeping Metadata Standard

<http://archives.govt.nz/s8-electronic-recordkeeping-metadata-standard>

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

Technical Guide: Implementing Recordkeeping Metadata

<http://archives.govt.nz/g14-technical-guide-implementing-recordkeeping-metadata-edrms-tailoring-technical-specifications-ele>

The advice in this Technical Document extends beyond the minimum mandatory requirements contained in the Electronic Recordkeeping Metadata Standard. EDRMS can easily exceed the minimum mandatory requirements of the Electronic Recordkeeping Metadata Standard and achieve much higher degrees of conformance with the metadata established in the Technical Specifications for the Electronic Recordkeeping Metadata Standard. This Technical Document is intended to provide explanations of the options available to implementers of new EDRMS.

United Kingdom

Requirements for Electronic Records Management Systems: Metadata Standard (2002)

<http://www.nationalarchives.gov.uk/documents/metadafinal.pdf>

This publication is the second in a series on *Requirements for Electronic Records Management Systems*. It is designed to complement the first volume in the series, *Functional Requirements*. The standard describes the records management metadata elements that UK ministries should attach to their records to ensure that they are complying with the functional requirements.

Minnesota State Archives

Minnesota Recordkeeping Metadata Standard

<http://www.mnhs.org/preserve/records/metadatastandard.html>

The Standard was developed to facilitate records management by government entities at any level of government. It was designed to achieve the following benefits:

- facilitate data sharing where authorized
- enhance efficiency with respect to location, evaluation and retrieval of records
- provide guidance for consultants, vendors and system designers.

The standard is comprised of twenty elements, ten of which are mandatory. It is referenced as a 'current standard' in the *Minnesota Enterprise Technical Architecture*.

Sources Used to Develop This Module

ARMA International

Why Metadata Matters

<http://www.arma.org/pdf/articles/franks-kunde.pdf>

Archives New Zealand

Electronic Recordkeeping Metadata Standard

<http://archives.govt.nz/s8-electronic-recordkeeping-metadata-standard>

Technical Guide: Implementing Recordkeeping Metadata in EDRMS: Tailoring the specifications for the Electronic recordkeeping Metadata Standard

<http://archives.govt.nz/g14-technical-guide-implementing-recordkeeping-metadata-edrms-tailoring-technical-specifications-ele>

Digital Curation Centre (DCC)

What are Metadata Standards?

<http://www.dcc.ac.uk/resources/briefing-papers/standards-watch-papers/what-are-metadata-standards>

Using Metadata Standards

<http://www.dcc.ac.uk/resources/briefing-papers/standards-watch-papers/using-metadata-standards>

ERPANET

Getting what you want, knowing what you have and keeping what you need.

Metadata in digital preservation

<http://www.erpanet.org/events/2003/marburg/finalMarburg%20report.pdf>

Metadata: Reports and commentaries

<http://www.erpanet.org/topic/metadata/index.php>

Joint Information Systems Committee (2010)

An Introduction to Metadata

<http://www.jiscdigitalmedia.ac.uk/guide/an-introduction-to-metadata>

International Council on Archives

Digital Records Pathways: Module 4: Metadata

<http://www.ica-sae.org>

International Records Management Trust

Training in Electronic Records Management: Module 3 - Managing the Creation, Use and Disposal of Electronic Records (Chapter 1: Developing Classification Schemes)

http://www.irmt.org/documents/educ_training/term%20modules/IRMT%20TERM%20Module%203.pdf

International Standards Organisation

ISO 15489: Records Management

ISO 30300: Management Systems for Records – Fundamentals and Vocabulary

ISO 30301: Management Systems for Records – Requirements

ISO 23081: Metadata for Records

Minnesota State Archives

Minnesota Recordkeeping Metadata Standard

<http://www.mnhs.org/preserve/records/metadatastandard.html>

National Archives of Australia

Australian Government Recordkeeping Metadata Standard (2008)

http://www.naa.gov.au/Images/AGRkMS_Final%20Edit_16%2007%2008_Revised_tcm16-47131.pdf

Australian Government Recordkeeping Metadata Standard Implementation Guidelines

http://www.naa.gov.au/Images/AGRkMS%20Implementation%20Guidelines_tcm16-50156.pdf

Using Metadata to Describe Information and Records

<http://www.naa.gov.au/records-management/agency/create-capture-describe/describe/index.aspx>

Recordkeeping Metadata

<http://www.naa.gov.au/records-management/agency/create-capture-describe/describe/recordkeeping-metadata.aspx>

National Archives of Norway

Noark

<http://www.arkivverket.no/eng/Public-Sector/Noark>

Queensland State Archives

Queensland Recordkeeping Metadata Standard and Guideline

<http://www.archives.qld.gov.au/Recordkeeping/GRKDownloads/Documents/QRKMS.pdf>

Metadata for Digital Continuity: A companion guideline to the Queensland Recordkeeping Metadata Standard

<http://www.archives.qld.gov.au/Recordkeeping/GRKDownloads/Documents/MetadataDigitalContinuity.pdf>

State Records Authority of New South Wales

Introducing Recordkeeping Metadata

<http://www.records.nsw.gov.au/recordkeeping/government-recordkeeping-manual/guidance/recordkeeping-in-brief/recordkeeping-in-brief-18#mandatory-recordkeeping-metadata>

Managing Digital Records: 3. Using Recordkeeping Metadata for Digital Recordkeeping
<https://www.records.nsw.gov.au/recordkeeping/government-recordkeeping-manual/guidance/documents/recordkeeping-guidelines/3%20Use%20recordkeeping%20metadata%20for%20digital%20recordkeeping.pdf>

NSW Recordkeeping Metadata Standard - Technical Specifications
<http://www.records.nsw.gov.au/recordkeeping/government-recordkeeping-manual/documents/recordkeeping-standards/Technical%20specification%202007.doc>

The National Archives (UK) – Information and Records Management

Managing digital records without an electronic record management system
<http://www.nationalarchives.gov.uk/documents/information-management/managing-electronic-records-without-an-erms-publication-edition.pdf>

Requirements for Electronic Records Management Systems: Metadata Standard (2002)
<http://www.nationalarchives.gov.uk/documents/metadatafinal.pdf>

US National Archives and Records Administration

Recommended Practice: Analysis of Lessons Learned for Enterprise-wide ERM Projects
<http://www.archives.gov/records-mgmt/policy/lessons-learned.html>

Literature

Atkinson, E, 'Much Ado About Metadata,' in *Records Management Journal* 12, 1 (2002): 21

Baca, Murtha (ed), "Introduction to Metadata: Pathways to Digital Information" (Los Angeles: Getty Information Institute, 1998).

Bearman, D, Capturing Records Metadata: Unresolved Questions and Proposals for Research. In *Archives and Museum Informatics* 11, 3-4 (1997): 271-76.

Cumming, Kate, "Purposeful Data: The Roles and Purposes of Recordkeeping Metadata" (Ph.D. dissertation, Monash University, 2005).

Gilliland, Anne J, Nadav Rouche, Joanne Evans and Lori Lindberg (2005), "Towards a Twenty-First Century Metadata Infrastructure Supporting the Creation, Preservation and Use of Trustworthy Records: Developing the InterPARES 2 Metadata Schema Registry," *Archival Science* 4(1): 43–78.

Hofman, H, Metadata and the Management of Current Records in Digital Form, July 2000. [<http://www.ica.org/biblio/com/cer/metadata.htm>]

Horsman, P, Electronic Record Keeping. The Record Keeping System as Framework for the Management of Electronic Records, Amsterdam, 2001

Joanne Evans, Barbara Reed and Sue McKemmish, 'Interoperable Data: Sustainable Frameworks for Creating and Managing Recordkeeping Metadata', *Records Management Journal*, vol. 18, no. 2, 2008, pp. 115-129.

Monash University, Records Continuum Research Group (1998), *Create Once, Use Many Times - The Clever Use of Metadata in eGovernment and eBusiness Processes in Networked Environments: Final Report*
<http://www.infotech.monash.edu.au/research/groups/rcrg/crkm/docs/rpt-final.doc>