Digital Preservation in Lower Resource Environments: A Core Curriculum

Understanding Digital Records Preservation Initiatives

International Records Mangement Trust

May 2016

Copyright:

CONTENTS

Figures

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 the 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 metadata[1], and the rapid obsolescence of software and computer systems all place digital records at great risk if they are not managed professionally. 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 professionals[2], who should be the key agents for improving the management of digital records, often do not have the knowledge, tools or authority to ensure that organisations understand the issues and adopt practical strategies

[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.

to address them. Many records professionals lack a fundamental understanding of records *management* standards in relation to IT systems and metadata, making it difficult, if not 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. Records professionals have not yet been exposed to the skills needed to manage digital records. At the same time, digital records are being generated at a rapidly increasing rate.

Understanding Digital Records Preservation Initiatives 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 protect the integrity of digital records through time, as well as to discuss the issues involved with key stakeholders. The module is also designed to support records professionals in engaging with the 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 real requirements of the countries concerned and provide a practical pathway for moving forward toward implementation. It is hoped that ultimately the material will be useful to records professionals in a range of environments across the world.

Purpose and Scope

Understanding Digital Records Preservation Initiatives examines selected digital preservation initiatives underway around the world in order to assess the practical application of the findings in lower resource environments. The module aims to serve as an introduction to digital preservation for records professionals, providing them with an understanding of current digital preservation practices, issues and potential strategies and of the initial steps that they can take to apply these practices. It explains key concepts associated with digital records preservation; examines the relevance and applicability of current digital preservation research initiatives around the world; describes strategies and solutions based on examples; and advises on how digital preservation can be communicated to key stakeholders regardless of organisation type, including public, private, academic, etc.

In brief, the objectives of the module are to help records professionals to:

- recognise how significant international initiatives in digital preservation may be understood and applied in lower resource environments

- identify the issues and define potential strategies for addressing digital preservation in a range of digital environments, including those associated with Open Data, Open Government and Access to Information

- understand the challenges of digital preservation and take practical steps to introduce solutions

- communicate effectively with key stakeholders about digital preservation concepts, issues and strategies to secure their support in incorporating digital preservation in organisational work programmes and in obtaining the resources to fund this work.

Audience

Wealthier countries have been investing in digital preservation for some time; in lower resource countries[3] where the use of digital technology is more recent, digital systems are now being introduced rapidly but often without attention to preservation issues. This module is designed to support the requirements of records professionals working in records management programmes in these circumstances. It presents a basic understanding of digital records preservation concepts, issues and strategies issues and strategies in relation to digital records created and held in different IT environments, including office and business systems, databases, networks and desktops, as well as by digitising paper records. The issues involved 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.

To support these diverse uses, each lesson in the module includes a section suggesting assessment exercises for students.

[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 include governments of developing countries, organisations with low levels of funding, and non-profit or community organisations.

Content and Structure of the Module

The module contains four inter-related lessons:

Lesson 1: *Concepts and terminology:* What is digital preservation, what factors influence the preservation of the integrity of digital records over the long-term, and what are the implications for organisations of not preserving digital records properly?

Lesson 2: *Digital preservation initiatives:* What is their importance and relevance, and how can international initiatives contribute to national and regional initiatives?

Lesson 3: *What to do next?* Based on the contributions being made by international initiatives, what practical strategies can organisations employ to begin addressing the complex challenges of managing the integrity of digital records that need to be retained and preserved over the long term?

Lesson 4: *Communicating the message and securing support:* What should the messages to key stakeholders look like and how should they be delivered?

Additional Resources

The module includes a glossary of terms and a list of core references and sources that support and elaborate the guidance provided in the lessons.

LESSON 1: CONCEPTS AND TERMINOLOGY: WHAT IS DIGITAL PRESERVATION?

Digital records preservation is one of several activities that are carried out as part of the records management function. Digital preservation is not simply a process of capturing digital records and holding them in a digital repository. It must be carried out in relation to well-run records systems. Otherwise, the records and the connections between them cannot be preserved systematically, and much of the meaning will be lost, even within a short period of time. This lesson begins, therefore, with an illustrated overview of essential records concepts before moving on to describe digital records preservation concepts. It provides the background to a discussion of digital records preservation concepts including the factors that influence the integrity of records when they stored for the long-term.

General Records Concepts

Records[4] 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. It continues with the receipt and evaluation of submissions from construction companies, and it ends with awarding of the contract to the company selected to deliver the project.

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

- Records provide 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.

- 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.

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

- 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. Taking another example, records can be used to support tenants' claims that insufficient compensation has been paid when a building they have been living in has been demolished during a construction project.

- Records are the source of valuable data and information for monitoring, analysing and planning. For example, information from a contracting process is combined with information on all other contracts for construction projects in the same year; the combined information is 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, records created as part of a single contracting process are linked. The records also must be reliable, authentic and accessible for as long as they are required. In records management, integrity is the term often used to describe these qualities meaning the records are whole and without corruption.

Records typically comprise *content* (what the record says), *context* (where the record comes from, how it came to be created, when and by whom) and *structure* (the different parts of the record). 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. The records' content, context and structure must be preserved throughout their life span; otherwise their integrity will be affected, and they may no longer have the same meaning or be understandable at all. The quality of the information extracted from the records now and overtime will depend on preserving the records' integrity.

Records are the product of work processes, also called business processes. 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 carried out and how. 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, 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), which itself is derived from a mandate(s) and/ or an enabling law(s) or some other authority. In other words, the organisation's mandate defines 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 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 follow formal procurement rules reviewing the submissions from all the companies that have responded to the tender and either approve or reject them. An intermediate stage may include short listing 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 contract is issued there may be contract negotiations to ensure that the successful company and the ministry agree on 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, or should be, because rules are in place to control what happens at each step; as far as possible, standard procedures are applied to allow comparisons between the companies responding to the tender and 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 in 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 Ministry's mandate is derived from a law that 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 that meets Government's needs, fosters economic development, protects the environment, and respects the interests and concerns of citizens and all those 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. Records underpin all of this.

Work processes can be highly structured, for example, processing tenders leading to the award of a contract for a construction project, or less well structured, for instance 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. 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 and approvals. Some of the communications in the work process may be carried out via email messages, which are stored and managed according to the personal preferences of the

individual. In such a work process (communicating by email) there are few controls over the management of the records. However, the email messages may be just as important in documenting all the steps in the developing the policy.

How can formal and informal record-creating processes be controlled 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 with a high level of awareness and understanding of 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. This regulatory framework defines 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.

When the records are well managed, accountability is assigned across the organisation. 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.

Digital Records Preservation Concepts

What is digital records preservation?

Records preservation, including records in digital form, is one of several essential record-keeping activities undertaken as an effective records management system. Digital records preservation fits within and is supported by the records management framework described above. Together with the other record-keeping activities it supports the organisation's ability to:

- achieve strategic and operational goals and priorities
- achieve development goals
- operate efficiently and manage information as a key resource
- meet accountability obligations
- meet the requirements of emerging high-profile themes, such as freedom of information, open government and open data.

Specifically, and for the purposes of this module, digital records preservation is, 'the series of managed activities necessary to ensure continued access to digital records for as long as necessary.'[5]

In 2003, a standard was developed through the International Standards Organisation (*ISO-STD 14721: Open Archival Information System)* that explained *long-term* as:

> *A period of time which is long enough to be concerned about the impacts of changing technologies, including support for new media and data formats, and with a changing user community, on the information being held in a repository. This period extends into the indefinite future.*

In the (fictional) Public Works and Government Services Ministry contracting example in the previous section, the records documenting the processes of tendering the contract, bidding, processing submissions and awarding the contract to the successful bidder must be protected and preserved for 20 years from the time the contract ends. Bidding documents received from unsuccessful companies must be retained for seven years. The retention periods of 20 and seven years are derived from a Government policy issued by the Ministry of Public Works and Government Services as part of its mandate to deliver a public works function and construction projects sub-function. The policy was drawn up by Ministry officials and law officers and takes account of contract law and other key legislation such as the Limitations Act. The preservation periods are also based on the following:

[5] Derived from the definition provided in Digital Preservation Coalition (2008) *Introduction: Definitions and Concepts Digital Preservation Handbook*. York, UK

- The Ministry is able to demonstrate, through the evidence in the records, that it acted with due diligence and according to the law and its own procurement policies in awarding of the contract.

- The records can be accessed if companies participating in the tender dispute the process and decision.

- The Ministry is able to build a knowledge base of information (eg precedents) that can be used in subsequent tendering and contracting processes and in assessing trends that will guide policy in the area.

- Citizens, especially those impacted by the construction project, can defend and protect their rights by referencing government records if they want to challenge the decision or the impact of the project.

- The Government is able to support its Open Government policy by releasing, through its Open Government portal, non-sensitive information concerning the contracts it has awarded; citizens are able to access this information over the long-term.

- The Government is able to support its Open Data initiative by making the valuable statistical data accumulated by the public works function and construction projects sub-function to support economic development and research.

In the example, the records are not retained forever. A careful analysis of the factors described above concluded that '20 years from the end date of the contract' for the successful company and 'seven years after contract awarded' for unsuccessful companies were reasonable retention periods. Two additional factors were considered:

- Is there any possibility that the records will still be needed? If so what would be the consequences for the Government if the records were no longer available?

- Is the cost of retaining and preserving records through the long-term justified if there is very little likelihood that the records will ever again be needed?

The challenge for the Ministry is how to protect and preserve the integrity of the records over the entire retention period in spite of the changes that are expected to occur in the supporting computer technology.

Essential Records Issues for Long-Term Preservation

Records professionals need to understand what is involved in preserving the records over the long-term to protect the records' authenticity and integrity. In practical terms, institutions periodically change the hardware and software they use either on personal computers or for central IT systems, upgrading to newer components or versions. As newer

versions of hardware and software do not necessarily support all the media and file formats used in previous versions this 'technology migration' process always includes a risk of making records and data inaccessible. As a result, from a technology perspective, the key digital preservation requirement for records management and business systems is interoperability. That is, the ability to export and import records and their metadata in spite of changes to the technology.

The issues involved are illustrated below using the example of a record generated by the contracting process for a government construction project. In this fictional example, the record is an email message from the chairman of the Procurement Committee to the Ministry's senior management team, asking for authorisation to award the contract. The email has an attachment (the relevant minutes of the Procurement Committee) and a hyperlink[6] to the same minutes. The issues involved are illustrated below in relation to the examples:

- *Content:* This is the information conveyed in the digital record. The content of the email message is contained in the message portion of the email.

- *Context:* This Information enhances understanding of the work-processes to which the digital records relate and defines the provenance (creator and subsequent changes in custody and ownership) of the record, eg who, when, why. Contextual information includes the metadata about the content. In the example, information in the *To, From, Date,* and *Subject lines* of the message provide context. Other information on metadata may be added later, such as the information that relates the email message to the work process that generated it (ie the construction projects contracting process) and to the transaction (seeking authorisation for the award of the contract*).* This information can include, for example, the folder in which the email is filed. Metadata also establish how the record was managed through time (eg how it is protected, who accessed it and how it has been preserved through technology change).

- *Structure:* This is information about the arrangement of the component parts of the digital record and how they relate to each other. In the example, the structural components of the email message include, for example, the signature blocks and logos used in the email message, as well as the attachment and the hyper link to the same documents stored in a folder in a server; embedded images or media clips, and hyper links to other content would also be part of the structure.

- *Appearance:* This is information about how the record should be rendered or presented on a screen; how it should be displayed in a manner that establishes its authenticity (eg the type of font and font size, colour, spacing and layout). In the example, the email message may have been kept for some time and may have been subject to a technology change, but it still can be rendered on a computer screen

[6] Hyperlinks are found in nearly all Web pages but are also used to 'jump to' a new document or image from the current document. Text hyperlinks are often blue and underlined.

complete with its component parts, such as the signature lines and logos, hyperlinks and attachments.

- *Behaviour:* This is information about functionality intrinsic to a digital record, eg hyperlinks, updating calculations, active links, attachments, etc. In the example the hyperlink to the minutes of the Procurement Committee is active and capable of being linked to the minutes in spite of the record having been stored for some time. If the email message had an embedded audio clip, it should be possible to click on the icon and listen to the clip. In other words, the software not only renders the message (ie displays the message), but it can also enable the record to behave as it was meant to behave originally.

- *Performance:* This is the ability of the digital record or parts thereof to be manipulated for purposes beyond that of its creation. In the example, the email message may have been retained as a PDF file (to ensure that the record can be rendered as it is supposed to be rendered), but the attachment may have been left in its native format, for instance, so that the data stored in selected spreadsheets in the attachment can be extracted and manipulated to produce statistics for purposes beyond the original purpose of the spreadsheet. For instance, the statistics from the spreadsheet can be combined with statistics from other reports to provide a consolidated picture of the Government's construction projects.

Content, context, structure, appearance, behaviour and performance are all endangered by media and format obsolescence.

Challenges to the Preservation of Digital Records

In addition to risks from viruses, the following factors need to be considered when developing strategies for preserving digital records. These issues must be addressed together as part of a unified strategy if the records are to survive and have integrity.

Media Fragility

Digital records are stored on a variety of media including, for example, CDs, external hard disks, floppy disks and internal disk drives. They are stored on network servers, database servers and a variety of other digital media. The common factor is that the records are stored in a digital format. Whatever the storage medium, all digital records are at risk from loss or destruction for the following reasons:

- *fragility of the digital media:* The life span of floppy disks (no longer made but still kept in many organisations) is three to five years; the life span of hard disks is two to eight years; and the life span of magnetic tape is 10 to 30 years.

- *poor environmental storage conditions:* Storage media are sensitive to extremes and changes in temperature and humidity.

- *lack of available technology:* For example, 5 ¼ inch diskettes can only be read by obsolete equipment.

- *quality of the media:* Some brands of storage media are of lower quality than others and may be more at risk.

Software and Hardware Obsolescence

Continual changes to the original creating software and hardware, and the rapid obsolescence of digital technologies, have critical consequences for organisations. We can read paper documents that were written hundreds of years ago and, assuming they have been kept in reasonable storage conditions, we can see them exactly as they were when originally created. For digital records, we need completely different strategies if the records are to be read in future.

In exploring the issue of software and hardware obsolescence, it is important to understand that obsolescence can occur at different times for any one or all of the following reasons:

- *Computer hardware:* Computers ranging from so-called mainframes to personal computers to smart phones are obsolete after only a few years of use. Many vendors of computer hardware products have disappeared taking their technology with them (eg WANG, Atari, etc).

- *System software:* The operating systems supported by major vendors such as Apple and Microsoft can become obsolete as new versions are developed; for instance, Windows 95 is no longer supported; present-day software may not be able to run on Windows 95.

- *Application software*: Even if the hardware and operating systems are still available, records may be at risk if the application software (for example, word processing software, spreadsheet software, etc) normally supported by the hardware and operating system no longer exist (eg Multimate) or if so many versions have been developed that records created using earlier versions can no longer be read. There are many examples of old versions of business applications (eg for accounting or financial management systems) that are no longer supported by the vendor.

- *Recording formats:* The hardware, operating system and application software may be in place, but if the records are recorded in a format that is not recognised, they may not be retrievable unless they are converted to another format. Some digital photo formats can only be read by certain software, and those who use Apple computers will understand the challenges that are sometimes encountered in exchanging documents and images with Microsoft PCs and vice versa.

- *Storage media:* 5 ¼ and 3 ½ floppy disks are difficult to find today because they have been superseded by more sophisticated storage media capable of storing much larger volumes of data. With the introduction of new storage media, from flash drives to high density tapes and from disks to hard drives and servers, digital records stored on older media must be migrated to new media. Organisations are driven to upgrade their storage technologies to ensure that records continue to be accessible. However, copying from storage media to storage media has its own risks as the records may be in danger of being lost or corrupted during the process.

Complicating these issues is the fact that hardware and software standards are also rapidly evolving and changing. Although format standards such as jpeg and PDF offer some stability, there are cases where standards have been superseded by other standards thus threatening the continued accessibility and integrity of digital records.

All of these risks to digital records must be monitored. Strategies are needed to ensure that rapidly changing technologies do not affect the integrity of digital records through time.

Inadequate Metadata

The companion to the training module, *Managing Metadata to Protect the Integrity of Digital Records,* describes in detail the risks associated with inadequate metadata. The purpose of metadata is to describe records in the context of their creation in a manner that facilitates access and retrieval, enables records to be understood and maintains the integrity of records through time. The risks arising when metadata are insufficient, inaccurate or incomplete are summarised as follows:

- failure to locate information
- inability to render and read the information
- lack of meaning or value in the information
- inability to verify the authenticity of information.

Weak Accountability

The lack of assigned accountability (who is responsible to whom for ensuring the integrity of digital records) can be potentially a greater threat to digital records than media fragility, software and hardware obsolescence, and the lack of sufficient metadata. If officials in the organisation know that they are responsible for ensuring the integrity of the records that they create and use, there is a far greater chance that the records will survive than if responsibility is not defined. Staff responsibilities should be clearly stated in an accountability framework that identifies who reports to whom about what. An effective accountability framework enables the organisation to identify any failure to take action to

preserve digital records[7]; if someone is held accountable, failure to take action will be less likely to occur in future.

Unfortunately, in many organisations, the accountability framework for managing records is weaker than the management frameworks in place for the organisation's other resources (such as human resources and finances). For human resource and financial management, reporting lines usually lead directly to the head of the organisation. Authority for setting standards and procedures, conducting audits, and managing human resources and financial resources are strong. This is not the case for records management, where responsibility and accountability are often at a low level in the organisation. Records managers often have little interaction with senior management. Senior managers tend to be unaware of, or have little interest in, the need for policies, standards, tools and procedures to ensure the integrity of digital records across the organisation. This has a profound impact on records managers' ability to influence the direction the organisation needs to take to preserve digital records.

Weak Legislation and Policy

Few laws reflect specific references to the requirement to manage records effectively. Some, such as freedom of information laws, imply that records should be managed effectively if the laws are to be respected but rarely are there specific requirements to do so. This is unlike the laws established for the management of financial and human resources where requirements are both implicit and explicit that such valued resources must be managed effectively. This is based on the recognition that failure to establish management frameworks for human and financial resources will undermine the ability of organizations to achieve their goals and priorities. Often the establishment of management frameworks is governed by policies (e.g. human and financial management policies). In the case of records, however, these are either weak or non-existent. If they exist they are often ignored because there are few sanction in place for non-compliance.

Awareness

If officials were aware that failure to manage digital records threatens the organisation's ability to carry out its mandate, they would be motivated to take action. In many organisations this awareness is lacking. Records professionals, who should have a high level of awareness, are often themselves unfamiliar and uncomfortable with digital records preservation concepts. IT staff and managers of programmes are also unaware of the concepts and the issues. Quite simply, the mindset required to see the implications of introducing new technologies for the preservation of digital records is non-existent across the entire organization. The result is that digital preservation is not part of the organisation's planning processes and the strategies and tools needed to manage the integrity of records through time are not well understood.

[7] The difference between accountability and responsibility can best be illustrated in the phrase, 'you are responsible *for* something; you are accountable *to* someone (for carrying out the responsibility)'.

Consequence of the Failure to Address the Risks Strategically

Weakness in any one of the factors described above can undermine trust in the integrity of records. This is important, because it cannot be assumed that fixing one weakness, for instance in decisions on recording format standards, will reduce the risks in other areas. All areas 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, trust in the digital records is eroded; if trust in the records is eroded, trust in the organisation's ability to carry out its responsibilities is at risk.

An organisation's digital records, when well managed, are a strategic asset that supports accountability, legal and policy compliance, resource management, service delivery, audit, access to information, information security and privacy. When poorly managed, digital records are incomplete, difficult to locate or cannot be authenticated, they can be easily manipulated, deleted, fragmented or lost. The familiar saying, 'garbage in, garbage out' accurately describes digital records that have been poorly managed and yet are needed. The result is that the organisation cannot carry out its mandate, make decisions, manage the systems that support its business processes, and hold itself accountable pursuant to laws, policies and audits. The outcome is also the inability to support emerging themes and priorities such as Open Government and Open data.

Open Government initiatives will fail if the records are not complete, accurate, understandable and accessible. They will fail if the records are not preserved for as long as they are needed to support the objectives of openness, transparency, and the public's right to access information about the conduct of Government programmes and decisions. If records are not managed adequately open government initiatives are at risk of being eroded and collapsing. Citizens realise that the Government is unable to manage the evidence it needs to demonstrate accountability, delivery its programmes and services, and manage the nation's affairs. If citizen engagement is to be meaningful, on-going access to trustworthy, reliable and accurate records is essential.

Similarly, Open Data initiatives will fail if records and the data sets are poorly managed. Poorly kept records result in inaccurate, incomplete or unverifiable data, which in turn can lead to misunderstanding and misuse of information, cover-up of fraud, skewed findings and statistics, misguided policy recommendations and misplaced funding, all with serious consequences for citizens' lives. Data sets may appear to be robust and comprehensive, but in reality they may not be traceable to an evidentiary source, usually a record. At best, organisations using these data sets 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 initiatives are based on the idea that citizens can trust and use the information that the government provides. Publishing inaccurate, incomplete or erroneous data can damage that trust relationship.

The accumulation of data over time can enable organisations to analyse trends and patterns which in turn inform policy development and decision-making. This powerful opportunity

will be lost if the records and data sets are not properly retained or if they are rendered inaccessible because of changes in the technology.

Records are the lifeblood of the organisation. They make it possible to achieve organisational goals and priorities, protect individual rights, and, on a broader scale provide economic and social development, and preserve cultural heritage. Their value, however, depends entirely on the steps taken to preserve them and on the quality and integrity of the records management framework that ensures they are managed throughout their life cycle.

In the contracting example, if the Ministry cannot preserve the integrity of the records of its contracting process for the required period there could be damaging consequences:

- The Government is challenged about the award of the contract to a particular company. Complete records documenting the selection process are not available and the Government is unable to defend itself in a court of law.

- A government building collapses eight years after it was built because of faulty construction materials. Records documenting the contracting process and the specifications for the building cannot be found. The Government is unable to take action against the company.

- The Government is unable to establish trends, identify precedents or carry out detailed monitoring, evaluation and planning because records are incomplete and inconsistent.

- The objectives of the Open Government initiative are undermined because the records relating to the building contract that were originally accessed through links provided on the open government portal are no longer available.

- The objectives of the Open Data initiative are undermined because the records from which statistical data about construction projects were extracted no longer exist. The statistics cannot be supported or trusted because the source records can no longer be accessed.

In summary, the failure to preserve digital records can have serious consequences for organisations and, more broadly, for society. Lesson 2 reviews the initiatives being undertaken around the world to address the preservation of digital records preservation. It describes the ways that records professionals in lower resource countries can benefit from understanding these issues, which can help them move forward in establishing digital preservation strategies.

Assessing Student Understanding of the Lesson

At the end of this lesson, you should be able to start to explain the following issues:

1 How do the content and context of records work together to support accountability?

2 What role does the records management framework play in making accountability possible?

3 How does digital records preservation support organisational effectiveness?

4 What factors influence the length of time for which a record needs to be preserved?

5 In addition to content, context and structure, what are three other aspects of a digital record that need to be preserved through time and why is this important?

6 Explain why the following are problems for those trying to preserve digital records: a) media fragility, b) software and hardware obsolescence, and c) weak accountability.

7 What are the potential consequences of these risks if they are not addressed?

8 If you are working with a large group, you may wish to have a debate. The issue could be: 'Digital records are harder to preserve than paper records'. Split the group into two to argue for and against this statement. Alternatively, this exercise could be undertaken individually by writing an essay to answer the questions: 'Are digital records harder to preserve than paper records?' If so, why?'

LESSON 2: DIGITAL RECORDS PRESERVATION INITIATIVES

Overview of the Focus of the Digital Records Preservation Initiatives

This lesson looks at digital records preservation initiatives that have resulted in standards and practices that can be useful to records professionals working in lower resource organisations. There have been a vast number of digital preservation initiatives over the past decade or more, and this module does not seek to describe all of them. The intention is to support records professionals in understanding the context in which the initiatives were established and the direction they are taking, so that they can make best use of the lessons learned and the tools that have been developed.

Most of the initiatives underway around the world are focused on research, and on developing standards and guides. They encourage and support networking and the exchange of information. Although more attention than ever before is being paid to issues associated with preserving digital records, the field is relatively new and highly complex. The research is multi-faceted, from analysing the requirements for digital records longevity, to exploring the role of metadata, to identifying effective approaches for migrating digital records through changing technologies. Largely as a result of the standards that have been developed and the close cooperation among the network of professionals engaged in the theoretical and practical aspects of digital records preservation, certain principles and practices have emerged and been accepted. Some of these relate to establishing plans for digital records preservation or applying tools and techniques. Others focus on the framework of laws and policies, standards and practices, systems and technologies, people and management that needs to be in place to apply the tools and techniques effectively. This framework is covered in Lesson 3.

Many digital preservation initiatives are not restricted to a single discipline, such as records management, archives or library science. Multi-disciplinary approaches are a feature of many of the initiatives described in this module. In several cases, the records professional's knowledge of authenticity, of preserving relationships among digital records and of the work processes that generate records, is being combined with the librarian's knowledge of accessing large collections of digital objects[8] (sometimes referred to as content discovery). This inter-disciplinary approach has led to the development of standards such as the *Open Archival Information System Standard* (OAIS - *ISO 14721:203*); and tools and techniques such as those generated by the *Digital Curation Centre* (DCC), the *Digital Preservation*

[8] 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.

Coalition (DPC), the *Open Planets Foundation* (OPF) and other organisations and collaborations.

It is important to understand that tools and solutions for digital records preservation are often either integrated with or embedded in tools and solutions addressing the management of digital information in general. Not all initiatives are inter-disciplinary. While collaboration across professional disciplines is becoming more common, some of the initiatives underway focus exclusively on the long-term preservation of current and archival records. The national archives of several countries are examples of organisations that have been leading the way in addressing the specific issues associated with the long-term digital records preservation. While they draw on other disciplines (for instance information access and retrieval from librarians and technical aspects from IT) their focus is on preserving digital records integrity through time.

When considering how to plan and implement strategies for digital records preservation, it is important to understand that good practice is continually evolving. Recognition is growing that there is no single solution for all digital records management situations. Digital records are being generated as the result of almost every human endeavour and they are being generated in multiple types and in multiple technology environments that are not only changing rapidly but are also growing rapidly in complexity. Nearly every sector now must deal with the complexity involved in managing and preserving these various types of records, and must do so in a way that meets the expectations and requirements of the sector itself and its stakeholders. Society expects information technology to improve our lives and solve many of our problems.

In spite of the emergence of common frameworks (eg OAIS) and methods (eg emulation and migration) as well as standards (eg XML[9]), no single implementation strategy is expected to emerge, nor should it be expected to emerge. Digital records preservation and strategies must account for the complexities that have been described, while at the same time drawing upon the experience of an ever-changing range of initiatives and implementations.

Finally, preserving digital records integrity and accessibility must be considered in relation to the organisation's broader information management frameworks. The business context must be understood and taken into account. Strategies for digital records preservation must be aligned with the organisation's overall approach to managing its information assets and, most importantly, with its approach to managing the organisation's business. The digital records preservation plan must be integrated into or linked with the broader strategic directions and priorities of the organisation.

In summary, the world of digital records preservation is still in its infancy. Most of the initiatives underway emphasise research and development. Major implementations (especially standards-based) are only just beginning. The field of digital records preservation is evolving. It is important to understand this when considering the methods, tools and plans for preserving digital records in the organisation. The strategy can aim to

[9] This markup standard has become an important tool for those involved in digital preservation. Students should familiarise themselves with this standard as they explore the role of digital preservation standards generally.

jump to the next stage of the evolutionary path or it can aim for a more steady progression. Whatever the strategy, it should be based on a clear understanding of the current state of development of tools and guides and the direction they are moving.

International Preservation Initiatives

Standards-Related Initiatives

The Consultative Committee on Space Data Systems (CCSDS) is an important initiative. This work led to an international standard, the Open Archival Information System (OAIS) model *(ISO 14721* (2002)[10], which has been used as a framework for digital preservation plans, strategies and initiatives around the world. According to the Standard, an archival information system is 'an organisation of people and systems that has accepted the responsibility to preserve information and make it available for a Designated Community.'

The OAIS model represents a management framework for receiving, managing and making available digital assets (including digital records) that need to be retained for the long-term. The model makes it clear that preserving digital records involves much more than simply storing the digital records in safe, environmentally controlled environments. It requires continual oversight and active management through time. The model represents a comprehensive and logical description of the functions of a digital records repository without addressing specific technologies or archiving techniques. It is generic in that it is applicable to any digital resources but it can be easily applied to records management.

The OAIS model is the current *de facto* standard in digital preservation and has a high profile around the world. In many digital preservation initiatives, from Australia to Norway, it is a common point of reference that is used to build understanding and consensus and to advance the objectives of digital preservation and interoperability.

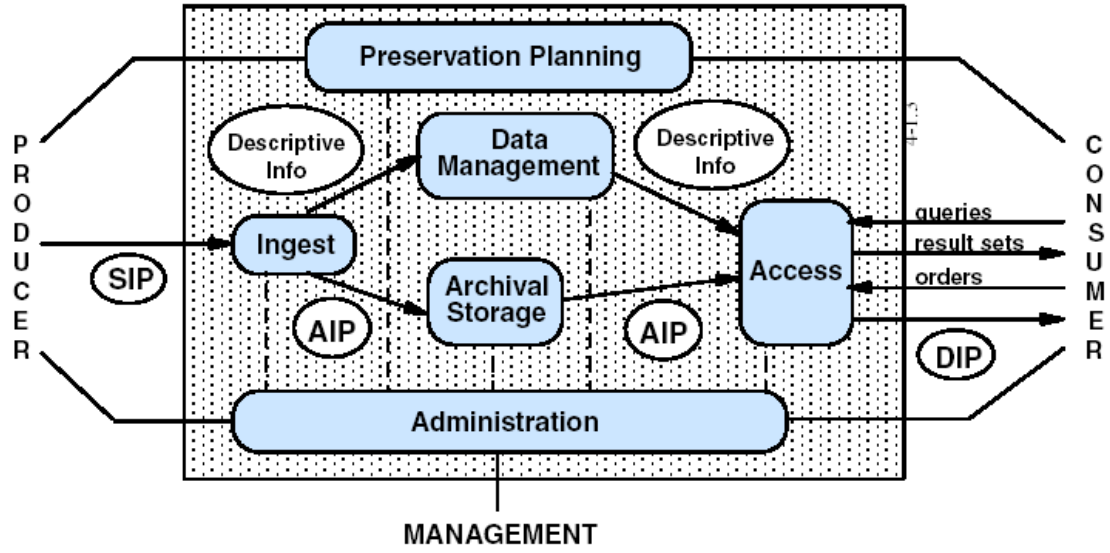
A key component of the OAIS model is the concept of a *package*, the unit of information to be archived. This generic term is used because the OAIS standard can account for a wide range of information *objects* including, for example, records, published materials and data in systems. A digital records package can be, for instance, a series of records documenting the contracts awarded by a ministry records relating to the tender and responses, selection processes and communications with the successful companies such as forms, emails and other electronic documents. Packages must be fully self-descriptive. That is, all of the metadata must be associated with the package itself and must be self-validating: the metadata must place the records in the context of their creation (as evidence of decisions, actions and communications); and the metadata must clarify how the records in the package can be accessed and rendered.

In order to submit data to the 'archive' (or repository), OAIS requires that the producer create a *Submission Information Package* (SIP) (eg a series of digital records with all

[10] OAIS reference model http://public.ccsds.org/publications/archive/650x0m2.pdf

appropriate metadata) that is submitted to the archive. The archive processes the SIP into one or more *Archival Information Packages* (AIPs) that are stored in the archive. Once a SIP is processed, checked and certified it becomes an AIP. SIPs are destroyed after the AIP is generated. The archive produces *Dissemination Information Packages* (DIPs) to enable users to locate information about the AIP. DIPs can be anything from a simple list of search results to a copy of the digital records themselves. Figure 1 is an illustration of the OAIS model.

Figure 1: The OAIS Reference Model



According to OAIS, three versions of the digital records are created and managed:

- The *SIP* is the version that is validated and tested to ensure that it is what it purports to be and that it is complete.

- The *AIP* is the version that is stored in the vault. The reference in the model to data management is for the metadata associated with the records that are managed as a distinct entity: this is both the metadata at the point that the records are ingested[11] and the new metadata created as the records are managed in the archive (eg when they are migrated to new formats).

- The *DIP* is the version that is made available to defined audiences or users.

The OAIS reference model has a number of clear benefits. It:

- is a well known and well understood model for long-term preservation

- provides both an information and functional reference model that can be used as a

[11] 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. (OAIS Reference model).

guide when developing digital preservation systems and/or functionality within other systems

- provides the discipline necessary to maintain the accessibility of packages and interprets the information they contain, even across changes in technology and changes in representation standards

- clearly defines the roles of the stakeholders (creators, users and managers of records) who interact with the archive

- identifies the necessary controls needed to maintain reliable archive management

- identifies the documentation required to communicate the archive's purpose and interactions to interested parties

- carefully documents the chain of custody of archived packages to ensure that documents are not inappropriately tampered with.

Digital preservation is as much about addressing the management factors as it is about the technical factors. The OAIS Standard needs to be placed in a broader records management context that addresses the management of records throughout their life cycle, from creation and capture, to organisation and use, to retention, preservation (the focus of the OAIS standard) and disposition. This broader records management context has been defined at the international level by two other important ISO initiatives.

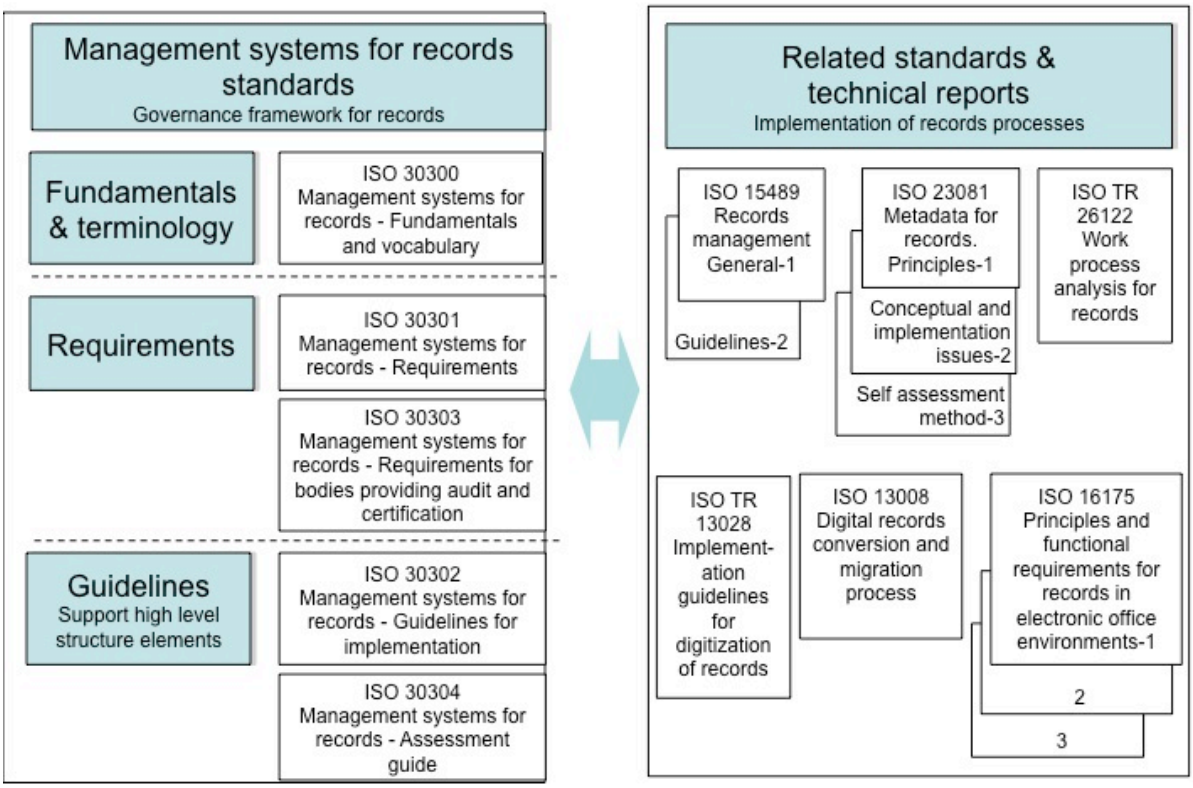
The first led to the, *ISO 15489 Standard: Information and Documentation -- Records Management,* which was released in 2003. This has been an important foundational standard for many years and has been adopted by many organisations around the world. It is highly influential, and to date it has been adopted 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 establishing the records management policies, programmes and systems needed to meet accountability requirements, support government operations, and achieve strategic priorities, including e-Government, open data and open government. The standard is in two parts. Part 1 of *ISO 15489* describes the components of a records management system while Part 2 sets out detailed guidelines on how Part 1 can be implemented.

The second important ISO initiative, which was developed and issued by the ISO's Technical Committee 46/Sub-Committee 11, is the *ISO 30300* series of records management standards. The committee comprises representatives from 27 countries (national member bodies) from around the world, many of whom were involved in developing of the first ISO standard on records management (*ISO 15489*). While *ISO 15489* was directed to records professionals in organisations, the audience for this new series of standards is business 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 series is comparable to the well-known *ISO 9000* series of standards that have had a significant influence on the manufacturing industry world-wide. The goal of the *ISO 30300* series is a similar series of internationally-recognised quality standards for managing of records, especially those in electronic form. The *ISO 30300* standards are intended for all types of organisations including governments. Over time, and similar to the experience with *ISO 9000* standards, the objective is to establish an agreed benchmark for international good practice in the management of records. Two standards now available in this series 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 shown in Figure 2.

Figure 2: ISO Records Management Standards and Supporting Documents



The ISO initiatives are complemented by initiatives sponsored by other organisations around the world. The examples that follow have been selected based on the extent to which their products can be useful in developing digital records preservation plans and initiatives in lower resource environments.

Relevant Digital Preservation Initiatives and Projects

A number of organisations around the world have been very active in developing tools and

techniques for preserving digital records. Several have emerged as highly recognised and respected centres of expertise that have had an impact on and contributed to digital preservation initiatives around the world. In a number of cases these organisations have adopted an inter-disciplinary approach. Some of the more notable initiatives and their implications for records professionals are described in this section.

Open Planets Foundation

http://www.openplanetsfoundation.org/about
The Open Planets Foundation (OPF) was founded in March 2010 to provide practical tools, solutions and expertise in digital preservation, to help assure long-term access to digital content. It builds upon a €15 million investment made by the European Union and the Planets consortium, which brought together sixteen major research and national libraries, national archives, leading technology companies and research universities to address core digital preservation challenges. The OPF web site contains the products of the Planets initiative plus a wide range of guides, reports, case studies and tools related to digital preservation.

Two of these are:

- *Plato*
  http://www.planets-project.eu/events/plato/
  Preservation planning seeks to ensure authentic future access for a specific set of objects and designated communities. Plato is a decision support tool that implements a reliable preservation planning process.

- *FIDO: Format Identification for Digital Objects*
  http://www.openplanetsfoundation.org/software/fido
  FIDO is a tool used to identify the file formats of digital objects[12]. It is designed for simple integration into automated work-flows.

Electronic Resource Preservation and Access Network (ERPANET)

http://www.erpanet.org/
(ERPANET) was a successful initiative that served as a knowledge-base for preserving cultural heritage and scientific digital objects. The dominant feature of ERPANET, which concluded in 2005, was the exchange of knowledge on state-of-the-art developments in digital preservation and the transfer of expertise among individuals and institutions. While the project concluded a number of years ago, the sources, including guides and reports, are still considered valuable to those concerned about preserving digital records. Some useful guidance covers:

[12] Digital Object: An object composed of a set of bit sequences.
http://www.alliancepermanentaccess.org/index.php/membership/member-resources/digital-preservation-glossary

- ingest strategies
- costing orientation
- selecting technologies
- digital preservation policy
- risk management.

Digital Curation Centre (DCC)

http://www.dcc.ac.uk
The Digital Curation Centre (DCC) is a world-leading centre of expertise in digital information curation[13] with a focus on building capacity and skills for research data management across the UK's higher education research community. The Digital Curation Centre provides expert advice and practical help to anyone in UK higher education and research wanting to store, manage, protect and share digital research data. Although the orientation of the DCC is on research data, it has developed a number of products that are relevant to the preservation of digital records. These include:

- Introduction to Curation
- Curation Lifecycle Model
- Digital Repository Audit Method Based on Risk Assessment (DRAMBORA)
- Registry/ Repository of Representation Information (RRORI).

Digital Preservation Coalition (DPC)

http://www.dpconline.org
The Digital Preservation Coalition (DPC) is a not-for-profit organisation that supports its members through knowledge exchange, capacity building, assurance, advocacy and partnership. The DPC raises awareness of the importance of preserving digital material and of addressing related strategic, cultural and technological issues. It adopts a multi-disciplinary approach, which is why its guides and tools address the preservation of digital objects generally. They are still applicable to digital records but some interpretation may be required. Examples of products of DPC initiatives are:

- Preservation Handbook

[13] *Curation* is the management activities required to maintain data long-term so that it is preserved and available for reuse.

- Technology Watch Reports
- What's New in Digital Preservation?

The Joint Information Systems Committee (Jisc)

http://www.jisc.ac.uk/
Jisc supports UK colleges and universities in using digital technologies innovatively to help maintain the UK's position as a global leader in education. Jisc provides:

- a world-class network – JANET
- access to electronic resources
- new environments for learning, teaching and research
- guidance on institutional change
- advisory and consultancy services
- regional support.

Although many of its research papers and guides focus on the library science community, there are several on the management of digital records. An example is:

- Records Management
  http://www.jiscinfonet.ac.uk/infokits/records-management/

Collaboration to Clarify Costs For Curation (4c)

http://4cproject.net
4C helps organisations across Europe invest effectively in digital curation and preservation. Research on digital preservation and curation has tended to emphasise costs and complexity. 4C research encompasses concepts such as 'risk', 'value', 'quality' and 'sustainability'. Organisations that understand this will be able to control and manage their digital assets over time, and they may also be able to create new cost-effective solutions and services for others. The project was launched in February 2013.

Scalable Preservation Environments (SCAPE)

http://www.scape-project.eu
The SCAPE project is developing scalable services for planning and executing institutional

preservation strategies on an open source platform that enables semi-automated workflows for large-scale collections of digital objects. SCAPE aims to enhance digital preservation in three ways: by developing infrastructure and tools to support preservation actions; by providing a framework for automated, quality-assured preservation workflows; and by integrating these components with a policy-based preservation planning system.

Sustainable Preservation Using Community Engagement (SPRUCE)

http://wiki.opf-labs.org/display/SPR/Digital+Preservation+Tools
SPRUCE aims to foster a self-supporting community of digital preservation practitioners and developers through a mixture of online interaction and face-to-face events based on the successful AQuA Project mashups (see AQuA Wiki for more information). The events are intended to provide support and technical expertise to address specific digital preservation challenges. The best work from attendees at events will secure funding awards to further develop the activity and embed it within business processes at the home institution. These awards will be allocated during the 2 year life of the SPRUCE project. An example of a SPRUCE initiative that is relevant for records professionals is the Digital Preservation Business Case Toolkit.
http://wiki.dpconline.org/index.php?title=Digital_Preservation_Business_Case_Toolkit

E-ARK

http://eark-project.eu

E-ARK is a 3-year multinational research project co-funded by the European Commission under its ICT Policy Support Programme (PSP) within its Competitiveness and Innovation Framework Programme (CIP). Competitiveness and Innovation Framework Programme (CIP). The objective of E-ARK is to create and pilot a pan-European methodology for electronic document archiving, synthesising existing national and international best practices, that will keep records and databases authentic and usable over time. The methodology will be implemented in an open pilot in various national contexts, using existing, near-to-market tools, and services developed by the partners. The project partner is the DLM Forum supported by numerous and diverse organizations ranging from national archives to institutes to universities. The project results will be generic and scalable in order to build an archival infrastructure across the EU and in environments where different legal systems and records management traditions apply. E-ARK will run from 1st February 2014 to 31st January 2017.

Online Computer Library Center (OCLC)

http://www.oclc.org/research/publications.html

OCLC connects libraries in a global network, "to manage and share the world's knowledge and to form a community dedicated to the values of librarianship: cooperation, resource sharing and universal access. The network links members to a cloud-based infrastructure that provides the system wide intelligence and cooperative platform needed to collectively innovate and drive operational efficiencies in metadata creation, interlibrary loan, digitization, discovery and delivery." Although directed to the library community, many of the OCLC publications can be of value to records professionals involved in digital records preservation. Some are conceptual but others focus on technical and practical aspects that can be adapted to the management of records. An example is "Demystifying Born Digital" (http://www.oclc.org/en-europe/publications/nextspace/articles/issue22/demystifyingborndigital.html).

Standard for Preservation Information Documentation of Electronic Records

http://www.futuregov.asia/articles/2014/jan/17/india-develops-standards-digital-preservation-reco/

In a move to standardise the preservation of digital records across government, India's Ministry of Communications and IT announced an initiative to develop a Standard for Preservation Information Documentation of Electronic Records. Developed by the Research and Development team at the Centre of Excellence for Digital Preservation, the guidelines and standards will ensure that electronic records are produced in a preservable manner. They will be applicable to all e-government initiatives at the Centre and State level in India.

The Role of National and State Archives

National and state archives in several countries have been active in developing the tools and techniques that serve as the foundation for developing and implementing digital records preservation. In addition to providing the ministries in their jurisdictions with much useful advice on managing and protecting their digital records holdings (based on the premise that to achieve digital records preservation, the records must have been well organised and managed), the archives' efforts to preserve their own archival digital records can serve as a useful model both for records-creating organisations and in other archives. Examples of archives that have assumed a leadership role and have made products available to be used by other organisations are described below.

National Archives of Australia

http://www.naa.gov.au/records-management/agency/digital/index.aspx

The National Archives has developed a preservation approach for archival digital records (ie those retained as national archives) based on converting or normalising[14] digital records into archival data formats for long-term storage and access. The basic conceptual approach of the project is described in the 2002 National Archives Green Paper, 'An Approach to the Preservation of Digital Records'. The Archives' approach to the long-term preservation of digital records is also expected to be useful for preserving digital records that are the custody of the creating agency. In 2004, in order to guide departments and agencies, the National Archives released, *'Digital Record-keeping: Guidelines for Creating, Managing and Preserving Digital Records'*.

State Records Authority of New South Wales

http://www.records.nsw.gov.au/

The State Records Authority is concerned with all aspects of record-keeping, ranging from measures to ensure that public officials create records in the course of their duties, managing records in agencies, to preserving and making records of continuing value accessible as State archives.

Queensland State Archives

http://www.archives.qld.gov.au/

In addition to its cultural role, and as the lead agency for record-keeping, the Queensland State Archives is responsible for developing and implementing a whole-of-government record-keeping policy framework. This framework ensures a consistent approach to creating, managing, disposing, storing, preserving and retrieving government information. The sections of its web site on *Record-Keeping and Digital Continuity* contain valuable guidance on a range of records management and digital preservation issues.

Public Records Office Victoria: Victorian Electronic Records Strategy

http://prov.vic.gov.au/government/vers

The Victorian Electronic Records Strategy (VERS) provides leadership and direction in managing digital records. VERS is a framework of standards, guidance, training and consultancy and implementation projects, centered on the goal of archiving reliable and authentic electronic records. The VERS Standard, *PROS 99/007*, was developed in 2000, and the most current version was released in July 2002. The VERS Centre of Excellence was established in May 2002. Located at the Public Records Office of Victoria (PROV), the Centre of Excellence is responsible for overseeing the development of a strategy for rolling out VERS across the Victorian government. The Centre provides resources, advice and guidance to Victorian government agencies as well as conducting research into the long-term

[14] Normalisation is the process of creating and/ or sharing digital documents or other digital objects in a limited number of often standardised digital data on file formats.

preservation of electronic records and overseeing the construction of an electronic records repository at PROV.

Archives New Zealand: Continuum – Create and Maintain

http://www.archives.govt.nz/continuum
Archives New Zealand has developed a strategy called 'Continuum' that has been designed to provide tools and services to government agencies to enable them to meet good practice record-keeping standards. It assists agencies in developing their own records management programmes to fulfill business and accountability requirements, and it promotes good records management so that the most significant records of government are preserved for current and future generations. Continuum also is designed to promote strong, cooperative and mutually beneficial partnerships between Archives New Zealand and government agencies.

The National Archives (UK): Information and Records Management

http://www.nationalarchives.gov.uk/information-management/projects-and-work/information-records-management.htm
PRONOM is the UK National Archives' online source for information about file formats and software products. It provides impartial and definitive technical software products that are needed to create, render or migrate these formats.

The *UK Central Government Web Archive* is a selective collection of UK Government websites, archived from August 2003, which has been developed by The National Archives (TNA) using the services of the US-based Internet Archive.

US National Archives And Records Administration (NARA) Electronic Records Archives (ERA)

http://www.archives.gov/era/rms/index.html
The Electronic Records Archives (ERA) is NARA's system for allowing Federal agencies to perform online records management transactions with NARA. Agency records management staff can use ERA to draft new records retention schedules for records in any format, submit these schedules for approval by NARA, request the transfer of records in any format to the National Archives for accessioning or pre-accessioning, and submit electronic records for storage in the ERA electronic records repository. The system went operational in 2011 and is being implemented systematically across the government. It is highly controversial, and it is worth reading audit reports in conjunction with accessing the ERA web site.

Information on NARA's guidance to records managers on the management of electronic records can be found at:
http://www.archives.gov/records-mgmt/initiatives/erm-guidance.html

The Challenges to Digital Preservation in Lower Resource Countries

As the Nigerian librarian Osarome Ogbebor[15] has pointed out,

> *An African perspective on preservation ought not to be different from other perspectives. However, digital preservation is often discussed in terms of technology, infrastructure and practices. Africa is largely composed of developing nations and thus has peculiar problems.*

He identifies a number of additional challenges that may arise in lower resource countries, including:

- lack of relevant standards and information policies
- lack of technological infrastructure and access to appropriate hardware and software
- lack of money for ongoing digital preservation work
- lack of technical knowledge about digital preservation
- irregular electricity supplies, which interrupt business operations and put organisations at risk of information loss
- low internet bandwidth, which limits the ability to transfer digital information.

A 2011 study[16] by the International Records Management Trust articulated the elements of a 'Regulatory Framework for the Management of Records'. The elements of the regulatory framework provide a baseline that should be in place before governments can address digital records preservation effectively.

ICT/ e-Government
Planning for ICT/ e-Government systems ensures that the records needed for the proper functioning of the system are complete, accurate and accessible.
Planning for ICT/ e-Government systems addresses functionality for the management of records from creation to disposition.
The national records and archives authority is included in consultations on ICT/ e-Government initiatives.
Freedom of Information

[15] http://osarome.blogspot.com/2011/10/challenges-of-digital-preservation-in.html
[16] http://irmt.org/portfolio/managing-records-reliable-evidence-ict-e-government-freedom-information-east-africa-2010–-2011

An FOI law has been enacted.
The FOI legislation is aligned with existing legislation, particularly the national records and archives legislation and other legislation relating to the release of information.
The FOI legislation specifically over-rides the 30 year access law if there is one.
The FOI law stipulates mandatory response times.
A plan for FOI implementation has been adopted by the Government.
The plan for FOI implementation considers the completeness, accuracy and accessibility of government records in all formats.
The plan for FOI implementation makes all government staff aware of their responsibilities for managing records.
Records Management
Legislation
The records and archives legislation establishes a single authority on the management of government records, from creation to disposition.
The records and archives legislation positions the national records and archives authority centrally within government so that it can fulfil its crosscutting function.
Policy
A government-wide records management policy has been adopted to define responsibilities for records management and relationships with ICT/ e-Government and FOI bodies.
Standards
The national records and archives authority has adopted a records management standard (ie ISO 15489).
A standard for records management functionality in ICT systems has been adopted.
A standard for archival management and digital preservation has been adopted.
Procedures
The national records and archives authority has issued or approved procedures for every phase of the management of records, from creation to disposition.
A national retention and disposal schedule exists and is applied to all hard copy and electronic records.
The national records and archives authority is mandated to enforce compliance with the retention and disposal schedule.
Staffing
A cadre of records management staff exists.
A scheme of service exists for staff responsible for managing records in electronic or paper form, from creation to disposition. The scheme of service spans government and ranges from clerical to management positions.
Infrastructure and Facilities
The national records and archives authority is allocated sufficient funds to fulfil its mandate
MDAs have sufficient space and equipment to manage active records securely, in electronic and paper formats.
Purpose built records centres have been provided for the storage of semi-active records.
Purpose built archival repositories have been provided for the storage of inactive records.
A digital repository has been created to preserve electronic records over time.
Capacity Building

Training in records management is available to staff at all levels and includes practical training in electronic records.
University programmes offer in-depth education for records management with practical training in electronic records management.

The study, conducted in the five countries of the East African Community, found that the majority of the elements of the regulatory framework were not in place in the five countries, which undermined their ability to manage records according to international good practice. Digital preservation strategies for governments and organisations in developing countries will need to take account of the broader regulatory framework in which the digital preservation issues are being addressed, and seek to address missing elements.

Research and Education Initiatives in Academic Institutions

Several academic institutions around the world are undertaking research into various topics related to preserving digital records. While much of the research is theoretical, the results help tend to shape the conceptual frameworks that records professionals can use as they develop and implement strategies and solutions at the practical level. These academic institutions also support education programmes that focus on enhancing knowledge of digital records preservation. The programmes and their associated courses can offer a useful reference for those who are interested in developing graduate programmes on digital records preservation initiatives. It is important to recognise, however, that many of the graduate level courses are based on theoretical approaches. Those developing course programmes at the practical level may have to look elsewhere, for example, practical workshops. Examples of leading academic institutions that feature digital records preservation as a key feature of their research and education progammes are described below.

University of British Columbia (UBC)

School of Library, Archival and Information Studies
InterPARES Trust

http://www.InterPAREStrust.org
iTrust (InterPARES Trust), otherwise known as 'Trust and Digital Records in an Increasingly Networked Society', aims to produce frameworks that will support the development of integrated and consistent local, national and international networks of policies, procedures, regulations, standards and legislation concerning digital records entrusted to the Internet, to ensure public trust grounded on evidence of good governance, and to provide a digital memory over time.

iTrust is the fourth 'generation' of the InterPARES initiative, which has addressed a range of digital records preservation issues over a nearly 20 year period. The products of InterPARES 1, 2, and 3 continue to be important because they focus on fundamental digital records preservation concepts and, through the numerous case studies associated with InterPARES 3, because they provide useful examples of how organisations of various types and sizes have approached digital records preservation. The reports of case studies in small organisations with limited resources may be especially helpful. iTrust is a recent initiative, and it will be important to monitor its progress, particularly because of its focus on the implications of preserving digital records in an online environment and on the impact of global initiatives such as open government and open data.

Information on the education programmes supported by the School of Library, Archival and Information Studies at UBC can be found at:
http://www.slais.ubc.ca/programmes/mas.htm.

School of Information and Library Science, Archives and Records Management
DigCCurr: Preserving Access to Our Digital Future: Building an International Digital Curation Curriculum

This three-year, collaborative project seeks to develop an openly accessible, graduate-level curriculum, course modules and examples to prepare students to work in the 21st century environment of trusted digital and data repositories. DigCCurr II seeks to develop an international, doctoral-level curriculum and educational network on the management and preservation of digital materials across their life cycle. This project will prepare future faculty to perform research and teach in this area, as well as providing summer institutes for 'cultural heritage' information professionals. Information on the education programmes supported by the School of Library and Information Science can be found at:
http://sils.unc.edu/programmes/arm

University of Michigan (UBM)

School of Information
PAVEL: Preservation and Access Virtual Education Lab

http://www.virtualarchiveslab.org
The University of Michigan's School of Information (SI) has obtained two years of funding from the National Endowment for the Humanities' Preservation and Access Education and Training Programme to develop and implement a virtual education laboratory featuring digital access and preservation tools.

Information on the education programmes supported by the School of information can be found at:
https://www.si.umich.edu/academics/msi/archives-and-records-management-arm

Other Useful Sources of Education Materials

Massachusetts Institute of Technology (MIT)

Digital preservation workshops
http://www.dpworkshop.org/workshops/fiveday.html
The Digital Preservation Management Workshops, a series presented since 2003, incorporate community standards and examples of good practice to provide practical guidance for developing effective digital preservation programmes. The workshops, partially funded by grants from the National Endowment for the Humanities, were initially developed at Cornell University beginning in 2003. They were further developed at the Inter-University Consortium for Political and Social Research (ICPSR) from 2008 to 2011, and at Curation and Preservation Services, MIT Libraries since 2012.

International Council of Archives (ICA)

http://www.ica.org/sites/default/files/Study16ENG_5_2.pdf
In 2005 the International Council of Archives 'Committee on Current Records in an Electronic Environment published *Electronic Records: A Workbook for Archivists.* This publication was aimed at 'everybody who has an interest in the management and preservation of electronic records with a view to their accessibility over the long-term'. The document is available online as a PDF in English and French. It presents a practical approach to digital records management from the perspective that archivists should be involved throughout the entire life cycle. Its governing principles and aims come from ICA's *Guide for Managing Electronic Records from an Archival Perspective.* Terminology and definitions are from *ISO 15489-1* (Records Management). This workbook covers terminology, influencing strategies in records management, implementing record-keeping requirements, preservation and access.

Digital Records Pathways: Topics in Digital Preservation is an educational initiative developed jointly by the ICA's Section for Archival Education and the InterPARES Project. It contributes to the education and training of archivists and records professionals responsible for carrying out the preservation of authentic, reliable and usable digital records. It is based on the research findings of InterPARES.
http://www.ica-sae.org

The International Records Management Trust (IRMT)

http://www.irmt.org/educationTrainMaterials.php
The International Records Management Trust is a non-profit, UK-based organisation dedicated to making information about managing records available at no cost to lower-resource countries. For over 20 years it has been carrying out practical records management improvement projects internationally and also conducting its own research

programmes. Its free Training in Electronic Records Management Programme provides five modules (Understanding the Context of Electronic Records Management; Planning and Managing an Electronic Records Management Programme; Managing the Creation, Use and Disposal of Electronic Records; Preserving Electronic Records; and Managing Personnel Records in an Electronic Environment), a resource list, a glossary of terms, good practice indicators for integrating records management with ICT systems, and route maps. The documents are available on the IRMT Website as PDF and Word documents.

Initiatives with a Strategic Vision for Digital Records Preservation

Three initiatives serve as useful examples of what is possible over the long-term. While specific to the situation in the countries concerned, they provide a target vision that any organisation should consider when establishing a strategy for preserving digital records.

National Archives of Norway

http://www.arkivverket.no/eng/Public-Sector/Noark/Noark-5-English
http://www.arkivverket.no/eng/Preservation/Electronic-Archival-Material
The National Archives Central Office in Oslo is responsible for the records created by the government's central administration, (ie ministries and directorates, etc) as well as the archives of the Supreme Court. Noark is a Norwegian abbreviation for Norsk arkivstandard, or Norwegian Archive Standard. Noark was developed as a specification of requirements for electronic record-keeping systems used in public administration in 1984 and quickly became established as a national standard. The latest version, Noark 5, sets out requirements on record structure, metadata and functionality. It does not describe how these should actually be met for any given departmental system. It is an excellent example of the relationship that can be established between an archives and the records-creating organisations.

National Archives of Portugal

Repository of Authentic Digital Records (RODA)
http://www.duraspace.org/keeping-it-real-the%C2%A0roda-platform-repositories-authentic-digital-records
RODA (http://www.roda-community.org) has evolved from a digital repository project created in conjunction with the Portuguese National Archives (http://antt.dgarq.gov.pt) into an advanced open source digital repository platform that provides long-term preservation and authenticity of digital objects. RODA is a complete digital repository that delivers functionality for all the main units of the OAIS reference model. It is capable of ingesting, managing and providing access to various types of digital content produced by large corporations or public bodies. RODA is based on open-source technologies and is supported by existing standards, such as the OAIS, METS, EAD and PREMIS. The Fedora application

framework supports RODA. Although it addresses the management of all types of digital objects, rather than just digital records, RODA provides a useful illustration of an OAIS implementation.

National Archives of Australia

Xena
http://naa.gov.au/records-management/agency/preserve/e-preservation/at-naa/software/xena.aspx
Xena (*Xml Electronic Normalising for Archives)* is free and open source software developed by the National Archives of Australia to support the long-term preservation of digital records. Xena software aids digital preservation by performing two important tasks: detecting the file formats of digital objects and converting digital objects into open formats for preservation. Xena preserves digital records in a three-step process:

- Xena determines the file format of the digital record.
- Based on the file format, Xena either converts the digital record to a preservation file format or, if the record is already in a preservation file format, preserves it as it is.
- Xena then stores the digital record, with its preservation metadata, as a Xena file.

Xena handles a range of formats, including office documents, email, images and audio files. This example is useful because it is compliant with international standards and the software is freely available. Those who are interested in establishing an OAIS-compliant digital records preservation process should consider Xena.

Other Sources

Blogs, wikis and listservs can also be important sources of information on digital records preservation as though these sources may address digital objects in general, they provide useful information to complement the information found in the guides and tools described elsewhere in this lesson.

Over the past few years a number of blogs have emerged that focus on digital preservation. Among the more notable are the following:

- Open Planets Foundation http://www.openplanetsfoundation.org/blog
- Digital Curation Centre http://www.dcc.ac.uk/blog
- Library of Congress: The Signal: Preservation
  http://blogs.loc.gov/digitalpreservation/

Individual digital preservation experts have established blogs that provide discussions on digital preservation topics. Four examples are:

- David Rosenthall's blog: http://blog.dshr.org
- Barbara Sierman's blog: http://digitalpreservation.nl/seeds/
- Kate Theimer's blog: http://www.archivesnext.com/
- Osarome Ogbebor's blog: http://osarome.blogspot.com/2011/10/challenges-of-digital-preservation-in.html

The Digital Preservation Daily is an active and very useful reference to current topics and events related to digital preservation. It is available at:
http://paper.li/z_gharbi/1306434752

Wikis also can be useful sources of information. The best known wiki, Wikipedia has a segment on digital preservation at: http://en.wikipedia.org/wiki/Digital_preservation

SPRUCE supports a wiki on digital preservation at:
http://wiki.opf-labs.org/display/SPR/Digital+Preservation+Tools

Other wikis include:

- Digital Preservation Coalition:
  http://wiki.dpconline.org/index.php?title=Main_Page
- Digital Preservation Network
  https://wiki.duraspace.org/display/DPNC/Digital+Preservation+Network
- Open Planets Foundation http://wiki.opf-labs.org/display/KB/Home

Listservs also can be useful tools for obtaining information about digital records preservation. Several focus exclusively on the topic of digital preservation; though in some cases the discussions may address much broader issues. Two examples are:

- Joint Information Systems Committee listserv: https://www.jiscmail.ac.uk/cgi-bin/webadmin?A0=digital-preservation
- Library of Congress, Digital Preservation listserv:
  http://www.digitalpreservation.gov/news/2010/20101202news_article_10years_jisc.html

Other sources addressing specific aspects of digital records preservation are described in Lesson 3. Collectively, the initiatives described in Lessons 2 and 3 are the basis for the strategies described in Lesson 3. They illustrate the means for communicating the message covered in Lesson 4. In the past, records professionals and others were simply trying to

understand the concepts associated with digital records. Today records professionals are able to make use of a wide range of tools and methods that cover nearly all of the components of the records management framework. These are global issues. Digital records preservation is an issue shared by organisations around the world. This has led to tools and methods that are independent of national boundaries, organisation type, and, at a broad level, technological environment. The next lesson harnesses the products of the national and international initiatives described in this lesson to present practical strategies that are based on these products, but adjusted to those that are relevant to lower resource environments.

Assessing Student Understanding of the Lesson

At the end of this lesson, you should have a sense of the wide range of initiatives that form the field of digital records preservation. In particular you should have an understanding of the OAIS concept of a package and be able to explain the difference between a SIP, AIP and DIP. Consider carefully the research initiatives, the initiatives pursued by national archives and the initiatives aimed at implementing a strategic vision.

Digital records preservation is a rapidly evolving, interdisciplinary and complex field, and it is vital to keep up to date with new initiatives and thinking. To practise the necessary research skills and to gain an understanding of the nature of the initiatives, investigate at least three of the initiatives or tools described here. Write a page on each one, and describe briefly whether or how you believe it is relevant to your own situation. If you are in a large group, divide up the initiatives and tools between you and then present your findings back to the whole group. Alternatively, try to plot (individually or as a group) all these initiatives onto a timeline to see the development over time of activity in this area.

If possible, follow the blogs and join the listservs mentioned and see how useful they are to you. Again, if you are in a group, you could each take one and write a summary of the activity on it over a month to share with each other.

Following all this activity, write a plan for yourself to help you to keep up to date. List the sources of information that you think are most helpful, and schedule time in the future to look at them.

LESSON 3: PRACTICAL STEPS

This lesson presents practical strategies that records professionals in lower resource environments can use to address digital records preservation issues. The concepts described in Lesson 1, and the digital records preservation initiatives described in Lesson 2, form the basis for the step-by-step practical advice in this lesson. The lesson offers advice on establishing digital records preservation initiatives in relation to specific work processes and systems and also on basic steps for establishing an organisation-wide framework for preserving the integrity of digital records. Finally it presents the example of the National Archives of Norway's approach to establishing a comprehensive digital records preservation programme within an effective government-wide framework for managing of records throughout their life cycle. The example establishes a target vision to which records professionals may aspire as they develop digital records preservation strategies. It also illustrates the importance of positioning digital records preservation within the larger context of the records management framework.

Principles and Strategies for Digital Preservation

Strategies described in this section are based on the findings and lessons learned from the initiatives described in Lesson 2. The strategies have emerged from practical experience gained internationally, in developing and applying digital records preservation tools and techniques.

Digital Preservation In Brief

Basic digital preservation requires:

- sufficient backup solutions for disaster recovery
- the ability to monitor changes in the hardware and software environment
- a generic framework for addressing hardware/ software changes affecting the records
- a metadata structure that allows users to understand and contextualise the records throughout their retention periods

- a digital preservation policy as part of the records management policy with appropriate review and awareness in place to ensure the sustainability of digital preservation actions.

General Principles

Any digital records preservation strategy must be:

- *feasible*: It must be based on the availability of hardware and software capable of supporting the implementation of the strategy.

- *sustainable*: It must be capable of being applied indefinitely into the future.

- *practical*: Its implementation must be within reasonable limits of difficulty and expense.

- *appropriate:* It must be relevant to the types of records and metadata to be preserved.

It must also be supported by a records management framework that comprises a combination of laws and policies, standards and practices, systems and technologies, and qualified people which in turn is supported by a management and accountability structure maintained by people who are aware of and understand the importance of records to the business of the organization.

In line with these principles, it is important to remember that digital records preservation initiatives, as well as overall digital records preservation programme for an organisation, should be:

- *multi-disciplinary:* Digital preservation cannot be undertaken by one individual or profession. There has to be widespread involvement across various departments within an organisation and with employees from a number of professional backgrounds. In addition to records professionals, the staff involved in implementing digital preservation strategies, can include information technology specialists, security officials, auditors and legal affairs specialists, as well as the business managers responsible for managing and directing the business units generating digital records.

- *flexible:* Business units generate a number of digital records formats that require different preservation strategies. Preservation strategies need to be flexible enough to support the ongoing care of different records formats.

- *streamlined:* Digital preservation requirements should be integrated into the system's development life cycle (plan, design, test, implement, maintain, review/ evaluate) whenever possible. The systems development life cycle is described in more detail in the companion module '*Managing Metadata to Protect the Integrity of Digital*

Records', Lesson 4.

- *integrated:* If digital preservation initiatives are to be effective, they must be integrated in an overall record-keeping framework that controls and manages the authenticity and reliability of records throughout their life cycle (ie creation, capture, organisation, use, retention and disposition). Similarly functional requirements, should include specifications and procedures for preserving digital records, guaranteeing the entire life cycle management of the records.

Steps in a Digital Records Preservation Survey and Plan

Regardless of the level of the strategy, and if a baseline is to be established, it is important to understand where records requiring preservation are being generated. This is why an important step in developing any digital records preservation strategy is to undertake a survey. Rather than survey the entire organization, however, the focus should be on those business processes and activities where there is a clear requirement to retain records over the long term. The results of the survey will enable the limited resources that might be available to be brought to bear on those processes and activities where the long term accessibility of critical records is at greatest risk.

The key steps involved in conducting a survey and establishing a digital records preservation plan are:

- Identify work processes and/ or systems generating records requiring long-term retention (following the initial meetings with business unit managers and IT specialists).

- Undertake a survey of the target work processes and systems (active and inactive) and identify file formats.

- Determine which file formats are specific to individual work processes and systems and which are common to some or all.

- Determine the quality of the metadata associated with the digital records where the metadata is poor or missing, determine whether its integrity can be reconstructed.

- Create a strategic plan to address digital preservation in the target work processes and systems and, if the survey is organisation-wide, for work processes and systems where records are being generated and need to be retained for the long-term. Identify digital records that are at risk and need immediate intervention to ensure their continued accessibility.

Support will be needed from business unit managers and IT specialists, particularly if there is any staff resistance to the survey, for instance if some people see it as an intrusion. The best way to remove suspicion is to build an open and friendly relationship with staff involved in the target work processes and systems. Records professionals should make it

clear that they are not concerned with the contents of the records, rather, with the function of the records within the organisation, the types of record formats generated and the types of systems used.

If funds are limited, the records survey will help to prioritise groups of digital records according to their importance to organisational operations and those at greatest risk of loss because of technological obsolescence or corruption.

Finally, it is critical that an assessment be conducted of the capacity of the records professionals and other specialists (e.g. IT specialists) to implement the strategy. There is no point in developing an ambitious strategy if the knowledge and abilities are not available to implement it. Or, if the intent is to develop such a strategy in an environment where the human capacity is weak then part of the strategy will need to account for the development of existing human resources (ie through education and training) and/or the recruitment of new staff. See "Identifying Technical and Staff Capacity" below.

Developing a Digital Preservation Strategy

A digital preservation strategy is likely to be developed through two interrelated approaches. The first path is a bottom-up application-specific approach; the second is a top-down organisation-wide approach. These paths are connected through a bridging step that involves developing a business case. The whole approach is based on good practice used internationally to develop digital records preservation strategies. In broad terms this involves: identifying requirements; assessing capability; designing; testing and systematically implementing solutions; evaluating results and developing a business case.

Bottom-Up Approach

The bottom-up approach involves analysing several small and simply structured work processes or systems generating records that need to be kept for the long-term. Long-term retention here means long enough for there to be concern about the impact of changing technologies on the records continued accessibility and trustworthiness as authentic and reliable records. This bottom-up approach should be based on the standards and practices discussed in Lesson 2, recognising that they may need to be adapted for use in lower resource environments. By focusing initially on several small and simply structured work processes or systems, the bottom-up approach will enable records professionals to gain valuable experience in building partnerships and applying what they have learned about digital records preservation. It will enable records professionals to decide how the standards and practices (and the experiences of others) can be configured and applied to address the needs of the organisation concerned. In a small organisation it may be sensible to combine the two approaches.

As described in the previous section, the first practical step is to undertake a survey of organisational units that are creating digital records likely to require long-term retention.

This survey can be as basic as reviewing the functions and activities of the organisation and finding out where records that need to be retained for the long-term are generated and held.

The next step is to identify the key individuals responsible for the records. As a minimum this will include the manager of the business unit in which the records are generated and the IT specialists responsible for the IT infrastructure supporting the business unit. Others, such as the security officer and systems audit specialists, may also have an interest.

It is important to approach the IT specialist or the business unit manager, or both, to discuss the long-term preservation of records generated in the business unit. The goal is to sensitise them to digital preservation issues and reach agreement on the need to conduct an assessment.

In some cases it may be best to approach a business unit manager who has shown an interest in the on-going quality and integrity of digital records. For instance, the Director of a unit responsible for contracting large government projects should be concerned about how long records documenting the contracting process need to be retained and how they should be preserved. Based on this interest, he/ she may ask the relevant IT specialist also to be involved. In other cases it may be more appropriate to approach the IT specialist first, especially if he/ she is sensitive to the issue. Then the IT specialist may help to approach the business unit manager. Having the IT specialist as a partner is fundamental if the business unit manager is reluctant to be involved.

In emphasising the involvement of IT specialists, however, it is important to remember that they do not use the same terminology as record specialists when they talk about digital records management and preservation. Nor do they share the same conceptual frameworks. An 'archive' to an IT specialist may mean a backup tape, and 'preservation' may simply mean storing records on high quality tapes in a secure, environmentally controlled room. Standards like OAIS can be helpful in creating a shared vocabulary to discuss digital preservation issues. However, in any case, records professionals need to explain concepts in understandable language. A good way to gain IT support is to find information management issues of common concern (for example, difficulties in accessing information, reducing email volumes) and then begin a discussion. This will help build goodwill, while identifying problems that can be solved mutually.

The key action during this partnership building stage is to highlight the issues that potential partners and stakeholders may be facing so they recognise the need to act.

As will be discussed further in Lesson 4, the initial meetings with business unit managers and IT specialists should be based on the following approach:

- Meet potential partners informally and discuss the purpose of the digital records programme. Treat the meeting as an informal event between and among professionals.

- Identify problems related to digital records preservation that partners or stakeholders

have encountered.

- Use words business unit managers and IT specialists can understand. Make sure all parties understand the meaning of any records management terms such as 'archiving' and 'retention and disposition'.

- Explain the implications of failing to address the issues. Use cost-benefit potentials or risk that may impact departmental functions and activities. This is especially helpful when working with business unit managers.

- Suggest pilot projects for work processes or systems that are generating digital records that need to be retained long-term.

The results of these initial meetings will prepare the way for developing a business plan for addressing specific digital record-keeping problems identified in the selected work processes and systems using the bottom-up approach. Engaging early on with business unit managers and IT specialists early on will also generate support for the longer term goal of establishing a digital records preservation programme for the organisation (the top-down approach). Ideally, the business unit manager and IT specialists, rather than the records professionals, will drive the organisation-wide digital records preservation programme forward.

Once the support of the business unit manager and the IT specialist is confirmed, the next step is to conduct a survey of the target work processes or systems. The survey will identify the types of records formats being created by each of the work processes and systems and help the records professional to identify the records that will require long-term preservation. It also will identify digital records that need immediate attention. Finally, it will help to determine the nature of the digital preservation strategies that will ensure the on-going access to records. Although the survey will tend to focus on active digital records and systems, records professionals should also survey legacy systems, as they could contain important digital records that need to be recovered and preserved. By conducting the survey, records professionals will gain understanding of how records are generated in the work processes and systems being studied. They also should gain an understanding of the nature of the metadata needed to support the on-going accessibility of the records.

Building a Business Case

Once records professionals have an understanding of the digital preservation challenges and issues, they need to present a business case to senior management. The business case is a document that demonstrates the need for a digital preservation programme. It describes short, medium and long-term goals for moving the programme forward. It should provide a situation analysis, based on practical information, findings and observations that will enable senior managers to discuss the issues and take decisions. It then is time to develop the second part of the business plan using a top-down approach.

The findings from the bottom-up approach are brought together to form the business, which demonstrates the need for action to address the issues through a digital preservation programme across the whole organisation (the top-down approach). It should identify the preservation issues and requirements for addressing them, the strategy for doing so, and the resources needed.

The business case for the bottom-up approach (targeted work processes and systems) should already have the support of IT specialists and business unit managers. The business case for an organisation-wide digital preservation programme (the top-down approach) normally must be presented to the organisation's senior management committee for approval. In many organisations, both types of business case will need approval at the senior management level. However, the business case for an organisation-wide programme should be represented by a senior champion from within senior management who has already agreed to bring the digital preservation issue to the senior management and has already briefed his/ her senior management colleagues on the business case.

It is helpful to use both the OAIS Standard and the Digital Repository Audit Method Based On Risk Assessment (DRAMBORA) as guides to building a strong argument in the business case. The OAIS model will provide terminology that can be used when working with partners and stakeholders involved to develop the business case and the proposed digital preservation initiatives. Both sources are helpful in planning an infrastructure that accounts for all aspects of the digital records preservation process. DRAMBORA was originally developed as a Trusted Digital Repository (TDR) audit and certification standard, using risk management methodology for identifying and addressing potential digital repository issues. However, it can be adapted to identify capacity gaps and the digital preservation risks that can threaten organisational operations. Using DRAMBORA will help provide a strong case for establishing digital preservation initiatives for the specific work process and systems, as well as for developing of a digital preservation programme for the organisation as a whole. DRAMBORA is especially useful as an internationally endorsed tool that can be used to demonstrate to senior managing the serious implications of failing to create, manage and preserve digital records.

In preparing the business case, records professionals also need to assess the current regulatory framework and whether or not it can support digital preservation initiatives at the local level (ie specific work processes or systems) or at the level of the organisation as a whole. Regulatory frameworks are the policies, procedures and guidelines in an organisation that guide staff on managing the organisation's records. In the public sector, the regulatory framework normally includes national archives legislation empowering the archives to guide the management of records. This legislation is often supported by a records management policy that assigns responsibility for managing the records across all levels of the organisation. In the private sector, which is not subject to archives legislation, the organisation-wide records management policy is a necessary component of the regulatory framework.

A regulatory framework is not essential in a small introductory initiative involving targeted systems, so long as records professional can work with IT specialists and business unit managers informally to support work processes and systems that have been selected in the

first stage of the digital preservation initiative. However, the framework is essential if digital records preservation is to succeed at the organisation-wide level. Assessment tools, such as ISO16363 (Audit and Certification of Trustworthy Digital Repositories) can help records professionals identify gaps in the regulatory framework. It is important not only to determine the gaps but to describe the impact that the gaps will have on digital records preservation and the extent they will place the organisation at risk.

Justifying a digital preservation initiative (targeted systems or organisation-wide) should be based on an assessment of risk, which is why DRAMBORA is such a useful tool. It is, therefore, important to have as much support as possible from IT specialists (who will be concerned about the risk for IT operations), business managers (who will be concerned about the risk to business operations), legal affairs specialists (who will be concerned about the risk from liability and legal accountability) and others who should be concerned about the impact of the gaps in digital preservation. Obtaining inputs from multiple stakeholders will help to strengthen the business case and gain the support of senior management.

In addition to outlining the problems and risks, a business case should also offer practical and affordable solutions. Standards like DRAMBORA, TRAC and RAC, as well as being useful in conducting assessments and building the business case, can also help records professionals map a way forward, while at the same time demonstrating to decision makers that the proposed solutions are strongly rooted in international good practice.

Finally, costs are an important part of the business case. Digital records preservation initiatives can be expensive. It is important to recognise that addressing digital preservation issues is not a one-time cost. As well as the start-up costs, it must involve on-going investment requiring the allocation of resources on a continuous basis over time. Implementing digital preservation initiative in stages is one way of reducing the impact of costs. Employing outside consultants can be expensive, but they are an option if internal capacity is weak. Qualified local consultants should be used if possible. The cost of the technology can be reduced by acquiring free open source software that can be easily accessed and downloaded. Local IT experts can be used to configure the system if the capacity does not exist within the organisation.

If the business case is approved, records professionals should continue to keep the relevant managers and digital records preservation champions informed about the progress being made.

Top-Down Approach

The top-down approach concentrates on developing an organisation-wide digital records management and preservation framework, based on lessons learned in the bottom-up analysis and on the proposed strategy presented in the business case. This involves developing the framework of policies, standards, practices, systems, technologies and skills needed to manage and preserve digital records effectively.

The key to achieving the aims of a digital records preservation programme is to position the

programme within an organisation-wide records management framework. Standards such as OAIS and DRAMBORA require digital records to be properly managed by records-creating business units. In other words, the quality of the digital records ingested into a digital records repository depends on the quality of the records management framework that controls the way they are created, identified, organised, described, used and retained. The records management framework is comprised of laws and policies, standards and practices, systems and enabling technologies, and qualified/ trained personnel. This framework is also supported by an effective governance and management structure (usually stated in the Records Management Policy) where accountability is clearly assigned for managing records through their life cycle.

If the records management framework is weak or non-existent (for example, if there are no standards and practices for capturing and managing the organisation's records) the records ingested into the repository will lack the essential characteristics and attributes to demonstrate their integrity. These essential characteristics and attributes cannot be entirely re-built, even if the repository is supported by the highest quality digital records preservation processes.

As digital records preservation issues are being addressed, parallel steps need to be taken to establish the records management framework or enhance an existing framework. This will take time, but adopting a prioritised and phased approach will make it possible to integrate the results of digital preservation initiatives effectively.

The first step is to obtain management approval for a policy that expresses the principles and objectives of a records management framework, defines the framework and its role in supporting the business of the organisation, and documents the roles and responsibilities of those responsible for implementing and maintaining its various components (standards, procedures, technologies etc). Crucially the policy must assign accountability for managing records.

In most organisations, accountability for managing records is weak when compared with the accountability assigned for the management of other resources such as financial and human resources. In most organisations, everyone is responsible for some aspect of records management, whether it is records creation, capture, use or disposition. Responsibilities (who is responsible for what) and accountabilities (who is accountable to whom for carrying out the responsibility) should be documented in the policy. Ideally, responsibility and accountability for preserving digital records should be integrated within the accountability framework for records management as a whole. Establishing a records management framework that has at its core a records management policy documenting the assignment of accountability for records management will form the umbrella under which a host of initiatives can be established, including those related to digital records preservation.

Key Issues for the Strategy

Metadata

In assessing the selected systems, records professionals will need to identify metadata associated with the records and how these metadata are generated. Metadata are essential because they bind the various components of a record together to provide the context for how the records are created and managed. Without metadata there can be no digital records preservation. The metadata relate records (both paper and digital) to each other and to the business processes, functions and activities that contributed to the records' creation. Properly generated they play an important role in preserving the integrity of digital records. This means that metadata must be available to address not one but all of the issues that pertain to the preservation of digital records (i.e. preserving content, context, structure, appearance, behaviour, and performance). Identifying and understanding the characteristics of existing metadata and identifying the gaps should be a key objective of the survey.

Three types of record-keeping metadata are needed in order to begin developing strategies for digital records preservation:

- *registration:* metadata that give a record its unique identity in the system such as a unique reference number that is never re-used.

- *content, structure and context*: metadata that provide information about a record's content (eg its title and description); about its structure (eg its type and format, Microsoft Word 97-2003 document) and about its context (eg its classification, information about who created it, and its relationship with other records)

- *record-keeping processes:* metadata that provide information about processes affecting the record (eg being viewed, transmitted, having custody transferred, being accessed, reviewed, retained, preserved and being disposed of).

Record-keeping metadata are not static. They continue to accrue over time as the records are used, as they are migrated in relation to changing technologies, and as they are managed over. Record-keeping metadata are the digital audit trail validating the authenticity and reliability of the records. Preserving metadata is as important as preserving the records themselves.

During the assessment of digital records metadata, records professionals should find out whether the metadata are 'linked', 'wrapped' or 'embedded', as this will affect the development of preservation strategies. These technical terms are explained in more detail later. Essentially:

- *Linked and wrapped metadata* can be stored separately from the digital record and linked through a unique identifier, so that when the record is uploaded, the associated metadata will also be available to users.

- *Embedded metadata* cannot be disassociated from the digital record so the size of the record will grow as more metadata are embedded each time the records are used, modified or changed. As the digital record grows, it may become so large that this

may itself become a preservation issue.

If metadata are missing, insufficient or fragmented, records professionals should consider whether the metadata should or can be reconstructed to ensure the on-going authenticity and reliability of the records. If it is not feasible to reconstruct the metadata, another method is to create a document describing how digital records were managed, the systems in which they were created and the how they were kept. This document will have to be updated regularly to include information about new preservation activities, such as migration or refreshing.

Ultimately metadata should be based on metadata standards and managed in stand-alone or integrated in application systems. The following is a list of metadata standards that might be applied for record-keeping metadata:

- ISO Standard *23081*: Metadata for Records (in 2 parts)
  ISO 23801 provides a framework for the use, creation, and management of records management metadata which complies with the requirements of ISO 15489: Information and Documentation - Records Management

- Preservation Metadata: Implementation Strategies (PREMIS)
  The PREMIS Data Dictionary for Preservation Metadata is the international standard for metadata to support the preservation of digital objects and ensure their long-term usability. Developed by an international team of experts, PREMIS is implemented in digital preservation projects around the world, and support for PREMIS is incorporated into a number of commercial and open-source digital preservation tools and systems.

- Metadata Encoding and Transmission Standard (METS)
  METS is the Metadata Encoding and Transmission Standard, which is applied to encoding metadata via a standardized XML schema. METS handles all types of metadata that is relevant to preservation: descriptive, administrative, and technical/structural metadata are all included in the schema, and a METS document will serve as the container for all of this information about a digital object. The schema was initially developed for the digital library community, and has thus extended to the digital repository and preservation communities.

- Record-keeping metadata standards developed by various jurisdictions. Two examples are:
  NOARK 5 standard: Developed by the National Archives of Norway, this standard identifies not only record-keeping functional requirements for information systems in the Government of Norway but also the metadata elements necessary to provide the context to digital records creation as well as authenticity and reliability.
  DoD 5015.2: The US Department of Defense *Electronic Records Management Software Applications Design Criteria Standard* is another example of a functional requirement for record-keeping system that also includes metadata requirements.

- Archival standards (ISAD(G), EAD).

ISAD(G) (General International Standard Archival Description) defines the elements that should be included in an archival finding aid. It was approved by the International Council on Archives (ICA) as a standard to register archival documents produced by corporations, persons and families.

EAD (Encoded Archival Description) is a non-proprietary standard for the encoding of finding aids for use in a networked (online) environment. Documentation is hosted by the Library of Congress. The standard is maintained and developed by the SAA Standards Committee's Technical Subcommittee for Encoded Archival Description.

For additional guidance on the overall management of metadata, refer to the companion module in this series, *Managing Metadata to Protect the Integrity of Digital Records*.

Identifying Technical and Staff Capacity

Digital preservation initiatives that comply with international good practice and standards require a clearly defined technical infrastructure and trained personnel.

Skills are needed to implement, support and maintain digital records to ensure their authenticity and reliability over time. A needs assessment should determine what competencies are needed, what capacity there is within the organisation and what expertise needs to be obtained from outside the organisation.

Ideally, digital preservation would be managed by a 'digital archivist' who has in-depth knowledge of both information management and IT. Qualifications for a digital archivist include:

- Master's degree in Archives, Information Studies or a related discipline
- conceptual and practical knowledge of digital records preservation research, techniques and strategies
- experience in managing digital records in a library or archival environment
- familiarity with metadata standards such as METS, Dublin Core, PREMIS and MODS
- understanding of trusted digital repository standards such as OAIS, RAC, TRAC, DRAMBORA and related standards
- project management skills.

The capacity assessment should determine records professionals' qualifications and those of the IT specialists who will be working closely with the team developing the digital records preservation initiatives. If no one in the organisation is capable of supporting some or all of these competencies, a plan is needed to fill the gaps. One possible solution is to group key information management and IT specialists in a core digital preservation team with clear responsibilities and communication channels.

For more information on digital archivist qualifications, see an article published on the Library of Congress website in February 2012 at: https://www.asis.org/asist2012/proceedings/Submissions/283.pdf.

According to basic human resource planning concepts for obtaining the right skills would involve the following steps:

- *Define* (or confirm) the nature of the work of preserving digital records based on clearly articulated roles and responsibilities derived from defined principles and objectives. This is important because it could lead to changes in the way the work is perceived.

- *Identify* the knowledge, skills and abilities needed to do the work. These should be defined within the context of the knowledge, skills and abilities needed to manage digital records throughout their life (ie from creation and capture to final disposition).

- *Develop* a competency profile[17].

- *Assess* the gap between the available competencies and what the competency profile requires.

- *Build* recruitment strategies as well as training and education strategies designed to fill the gaps.

- *Establish* a rewards and recognition approach that offers a wide range of methods recognising and rewarding performance.

- *Establish* a method for reviewing and evaluating performance against goals, results and outcomes and for evaluating the effectiveness of the capacity building strategy.

Assess the technical infrastructure needed to support long-term retention and preservation. Analyse the current server space, and as far as possible, identify short, medium and long-term needs, including contingencies, to ensure that space does not run out at any point. Assess the technologies needed to support the selected digital records preservation strategy. Will the existing technical infrastructure accommodate the strategy or will additional hardware, software and technology tools be required? Review the cost implications.

The competency and technical assessments can be adapted from the existing Trusted Digital Repository (TDR) certification and audit standards. While these standards are likely to be too rigorous and detailed for lower resource organisations, they are useful in guiding records professionals in the assessments. In a reduced form, they also can be useful in designing benchmarks for the initial digital preservation initiatives and ultimately for the

[17] Tools for producing competency profiles have been developed by several organisations around the world; these typically cover the competencies for the life cycle management of records for which preservation is one component.

organisation-wide programme.

Level of the Strategy

Strategies for preserving digital records can be developed at basic, enhanced and advanced levels. Any one of the three levels can be appropriate, depending on the nature of the records and preservation requirements and on the resources available. Many organisations wishing to build a systematic approach to digital records preservation proceed through the three levels in sequence. A brief description of the activities involved at each level follows.

Basic Level:

- Undertake and maintain, as a continuous process, a review of the types of digital records being created, their uses and the methods of storage, resulting in a constantly updated register of records types, their associated metadata, file formats, storage locations etc.

- Understand the types of metadata created by ICT systems in which the records reside.

- Assess capability to store digital records and monitor their accessibility, and ensure that sufficient security and backup measures have been applied.

- Establish criteria and communication channels for software and hardware migration processes. When the IT departments think about replacing systems, people in charge of records and archival management get the news as early as possible; the same people are able to undertake an assessment on the risks associated with the migration by using the register of records types and comparing it with the capabilities of the new system(s).

Enhanced Level:

In addition to the previous recommendations:

- Ensure that all new IT systems maintaining records have possibilities for exporting records and their metadata into a platform independent format.

- Convert digital records to durable, accessible formats.

- Maintain relationships between records in one set of formats to records (normalised) to standard formats via metadata.

- Enhance access (eg through viewer software and advanced search capabilities).

- Provide high quality metadata (archival description).

Advanced Level:

In addition to the previous recommendations:

- Describe and validate records in all formats.

- Deliver records in formats specified by the client. Clients may require that records are delivered in a specific format to facilitate re-use of the information or because the application in which they use the information can only support certain record formats. This requires a user needs assessment to be undertaken as well as an in-depth understanding of the designated user community.

Practical Digital Records Preservation Actions

Once the work processes and systems and the technical and staff capacities have been assessed, practical preservation actions need to be identified. This section will cover the storage issues that need to be considered by the digital preservation strategy. If the records are very valuable and need to be retained over the long-term but the supporting technical infrastructure for preserving them is very weak, printing the records to paper may be the only viable option. For records with a complex structure (eg 'case' records where parts of the record are located on different segments of a database and can only be pulled together through the use of software) this may not be helpful. However, in other situations, for example, where valuable emails and other electronic documents are stored on file servers, printing can be a practical option until the technical infrastructure can be upgraded.

If digital records are to be maintained through time and their integrity is to be preserved they must be stored in environmentally controlled conditions with security and access controls. IT specialists have a wide range of standards and practices for establishing these conditions. The digital preservation actions described below will fail if the records are not stored on high quality storage media in secure rooms and vaults, with humidity and temperature controls in place.

A well-managed IT programme must be developed and implemented with back-up recovery plans to ensure that data and records can be recovered in the event of a system failure or other disaster, such as fire or flooding. Creating back-ups or 'archiving' data (in the IT sense) is fundamental to any digital preservation strategy. Of course this does not in itself ensure that the records are complete, understandable, authentic and reliable for as long as they are needed. Various storage issues will need to be considered, and decisions will need to be made, often in partnership with the IT specialists.

Refreshing

Refreshing refers to reading and rewriting stored data to ensure the data is retained accurately. This can take place when hardware and/ or storage media are being upgraded to take advantage of technology advancements (eg increased storage capacity), to reduce costs or to accommodate new business requirements.

Upgrading storage media is especially important because unless the media are replaced periodically, their quality and integrity will deteriorate over time, placing the digital records at risk. When replacing storage media and hardware generally, steps should be taken to migrate the digital records from the old to the new media and hardware. IT specialists will know how to ensure that the bit stream on the old media (the stream of data in binary form, eg 00100110) is duplicated on the new media, which is an essential step if the preservation of the integrity of the digital records is to be assured.

Refreshing should be planned carefully and properly resourced. A media refreshment plan is needed so that IT specialists know when new media need to be purchased and old media retired. This includes any consolidation of digital records on to a smaller number of media. Finally, there must be a means of checking that the records have been copied in their entirety. IT specialists should have the knowledge and tools to carry out these steps. The goal is to ensure that the bit stream on the source media is the same as the bit stream on the new media.

Migration

Migration involves moving a digital record to either a newer format (eg from Microsoft Word 97 to Word 2007) or to another format (eg from Word 97 to PDF). Software programmes are frequently updated, and sometimes digital records created in older versions are not readable by the newer versions. There are instances where software is discontinued or is not easily available (eg Wang). There are also examples of records created using one version of a software programme becoming inaccessible or incomplete using later versions of the same software (eg fonts have changed or graphics are altered). Decisions about upgrading software from one version to another or changing the software altogether should not be made without considering the implications for the records and their ongoing integrity. Migration can occur when the software is acquired, or the records can be normalised (ie converted to a standard format) as a separate step apart from the software migration. Another option is to leave the records in their native (ie original) format and migrate or convert them only as required.

Normalisation to a Standard Set of Recording Formats

Normalisation involves converting digital records to a standard format to reduce the number of formats that must be managed. Retaining digital records in many different formats can be challenging and costly. The formats and supporting software must be monitored regularly to ensure that they are not obsolete or that their integrity has not been

eroded by changes in the technology. Using standard formats reduces the risk to the integrity of the records making it possible to access them by software that supports the standard formats.

The survey of work processes and systems will identify which records need to be retained long-term and the recording formats on which they are held, and the recording formats to be used to retain them. Decisions can then be made about whether to convert to a standard format. The international standards community has developed a number of standard formats that have been adopted by software vendors around the world. Conversion to these standard formats increases the likelihood that the records can be read and that their integrity ensured regardless of the software being used. Some national archives around the world have developed lists of acceptable format standards for the long-term retention of archival digital records. An approved list of acceptable format standards can guide the process of normalising digital records for long-term retention and continued accessibility, and help to reduce long-term costs.

Word processing files, for instance records formatted in proprietary formats such as .doc or .docx, can be converted to PDF(A). Digital photographs recorded in proprietary standards can be converted to TIFF (preservation format) and JPEG (access format). These examples, and there are many others, are common to the lists of format standards used in archives and record-creating organisations that have adopted normalisation strategies.

In the case of normalising photographic records, records professionals may need to choose one format that will support access and another format that will support preservation. Records in TIFF format are much larger in size than those in JPEG. Both may meet the objectives of the normalisation strategy (integrity of the records, software independence, etc) but the records recorded in JPEG have advantages for access, such as smaller files to be transferred and the ability to re-manipulate. TIFF files, because of their higher resolution, offer the highest level of quality from a preservation perspective. Preservation formats are uncompressed, whereas access formats are compressed. Access formats compress large record formats like TIFF smaller. This makes it easier to send, receive and access the records, especially when bandwidth is an issue. To make a format smaller, however, parts of the bit stream are lost through the on-going and repeated compression process. Over time so much can be lost that the file is corrupted and is no longer readable. The preservation format, on the other hand, is less subject to corruption because it is uncompressed, and in spite of repeated copying there will be no loss of the bit stream.

Preservation formats and access formats should be kept in separate locations. Some organisations keep access and preservation formats on different servers. Others keep access formats on web servers and preservation formats on external hard drives stored in air-conditioned vaults. The preservation formats are the ‘authoritative’ digital record from which access formats are generated. The preservation format is used to generate new access versions if the records become corrupt.

In deciding whether or not to normalise the recording formats of digital records, records professionals, working with IT specialist colleagues need to evaluate when and by whom the normalisation will take place, what process will be used and how much it will cost.

Regardless of the format selected, care is needed to ensure that the relevant metadata is migrated with the records, and that the new format can enable the metadata to be retained in an accessible and renderable form. Metadata that documents the format conversion and other aspects of the life of the record as it proceeds through changes in technology, software and formats, must also be captured and retained with the records.

The OAIS Standard calls the combination of the preservation format and related metadata an Archival Information Package (AIP); it calls the access format and related metadata is called a Dissemination Information Package (DIP). See Figure 1. Typically, a DIP may contain only a limited amount of metadata (eg descriptive metadata) because only a limited amount is needed to access and use the records. There are exceptions, users generally do not need all of the metadata associated with the entire life of the record to understand the digital record they are viewing.

Migration on Request

In this strategy, digital records are only converted when there is a request for them. The records are left in their native format, and a special-purpose conversion tool is developed to ensure that if there is request, the selected records can be converted to a format that can be read and understood. This saves the costs of converting entire series of digital records. This is a useful strategy when it is likely that only a few records will be accessed. There is the risk that the records, if they are dependent on a single technology tool, could become inaccessible over time, but this approach does eliminate or greatly reduce the costs of conversion. Some have argued that repeated conversions resulting from of changes in standard formats could raise the risk of records becoming corrupted. Leaving the records in their native format but ensuring their continued access through the use of a special purpose conversion tool can reduce this risk.

Adopting of this strategy requires careful assessment of the risks, including dependency on a technology tool and a process that may not be sustainable through time.

Emulation

Emulation refers to keeping the original operating system used to create and/ or manipulate the digital records. For example, if a record was created in an IBM DOS system, an emulator can re-create the original operating platform and software used to render the record in its original environment. Emulation is regarded as an interim measure until systems are developed that can re-create the digital record, without emulation software. Specifications need to be kept describing how the original environment operated so that it can be re-created.

One of the weaknesses of emulation is that it is expensive and requires emulation software to render the digital record. Emulation software itself will become obsolete over time. To

ensure continued access, organisations will need to continue purchasing new emulation software to emulate the existing emulation software and enable the record to be accessed through this.

Migration and emulation have their own strengths and weaknesses. Records professionals and their partners and stakeholders need to take costs, access requirements and whether or not the records must be retained permanently into account, and then select the most appropriate preservation strategy.

Encapsulation

The concept behind encapsulation is that the digital records to be preserved should be self-describing, in that the content of the record with all the metadata needed. This is accomplished using XML 'wrappers' that encapsulate the record and contain the metadata describing the logical relationships:

- between the components of the record
- between the record and the process that generated it and any other metadata needed to understand the record.

This approach makes it possible to access and render digital records now and in the future using emulators, viewers or convertors.

An example of this strategy is the Victorian Electronic Records Strategy (VERS), developed by the Public Records Office of the State of Victoria, Australia. In the VERS approach, record content received from agencies is accepted in standard formats, including text files, PDF, PDF-A, JPEG, TIFF and MPEG. The records are encapsulated, using an XML 'wrapper' containing a standard set of metadata elements, and authenticated using a digital signature. Each record that is encapsulated can contain multiple documents that together form a record. It is a similar approach to emulation, without the need to include specifications to rebuild the original hardware and software exactly in order to access the record. Rather, the metadata provides a hardware and software independent method for understanding the record over time.

The advantage of the encapsulation approach is that the content and contextual information (metadata) are kept together to minimise the risk of loss. On the other hand, in order to keep the amount of metadata within reasonable limits, they are typically restricted to metadata pertaining directly to the records (ie metadata for ensuring the continued accessibility, understandability and usability of the records). The potentially voluminous metadata about the records creators, organisational context, the functions and activities are not encapsulated. Other means need to be found to ensure that important relationships between the records and the broader context within which the records were created and managed are identified and preserved.

Steps Toward Establishing a Trusted Digital Repository

Establishing an organisation-wide digital records management and preservation framework will prepare the way for developing a trusted digital repository (TDR). While few organisations have established organisation-wide TDRs, and their implementation may be beyond the means of most organisations in low resource environments, it is important to be aware of their role and their characteristics. A TDR can provide the basis for a comprehensive trusted environment for preserving digital records generated throughout an organisation.

Developing a Trusted Digital Repository (TDR) may seem to be beyond the capacity of organisations in lower resource environments. However, it is an important goal, ultimately there must be a central, professionally managed repository for the long-term retention of valued digital records. Records professionals, their IT colleagues and others such as business unit managers, will find it valuable to understand the role and characteristics of a TDR. This section provides guidance on establishing a TDR, based on processes introduced in OAIS as well as the certification and audit standards. The guidance assumes that a regulatory framework is in place to facilitate the digital preservation programme.

A trusted digital repository enables organisations to store digital records with on-going value and maintain their integrity. Failure to store the records in a trusted environment will lead to questions about their authenticity and trustworthiness. This is why any digital records preservation strategy must ensure not only the quality and integrity of the records but also of the repository that holds the records. The international community has made a real effort to develop standards and certification methods for developing and managing Trusted Digital Repositories (TDRs). A TDR has to be a significant feature in any digital records preservation plan.

> *A trusted digital repository is one whose mission is to provide reliable, long-term access to managed digital resources to its designated community, now and in the future*.[18]

A trusted digital repository is different from a record-keeping system. A record-keeping system, such as an EDRMS, controls the creation and management of active digital records but normally does not have the functionality to manage records over the long-term. A TDR on the other hand, especially those modeled on the OAIS standard, supports the functionality needed to preserve the integrity and authenticity of records through the long-term. Ultimately it acts as an archive for digital records, preserving their on-going value. Interlinking the TDR with the record-keeping system ensures that digital records can be transferred for preservation, freeing up space in the digital record-keeping system to support organisations ability to create and use active records. Records professionals need to emphasise the difference between a record-keeping system and a TDR.

[18] *RLG-OCLC Trusted Digital Repositories: Characteristics and Attributes (2002)*

The most important requirements for establishing and operating a TDR are the organisational structure and the regulatory framework. The organisational structure will dictate the configuration of the digital repository software and its rollout. The regulatory framework will ensure that records are regularly transferred to the TDR for preservation and will govern the operational procedures of the repository.

There are many different ways to design and operate a TDR. In some programmes, transfers to the TDR are strictly defined by legislation and by the policies and procedures for the ingest of the records. In Norway, for example, there are strict procedures governing the way that ministries, departments and agencies to transfer records to the trusted digital repository. The Norway case study at the end of this lesson provides more detailed information. In other countries, departments may transfer digital records in any format with limited metadata requirements (US Washington State Digital Archives, UK National Archives). Regardless of the TDR transfer or management process, there are some steps that organisations in lower resource environments can take straight away.

The steps described below are designed to help records professionals in lower resource organisations establish a systematic approach to establishing a TDR, breaking down the design and implementation into phases.

Designing the TDR

Digital preservation standards presume that records professionals preparing to design and implement TDRs understand the types of digital record formats being produced in the organisation. The records and systems survey described earlier will give records professionals a basic understanding of the types of digital records requiring preservation. The central focus maybe on the targeted work processes and systems identified through the bottom-up approach. However, if the TDR is meant to be an organisation-wide system, records professionals will need to survey all digital records and systems of long-term value in the organisation.

Standards such as OAIS and TDR audit and certification standards can provide important guidance on TDR design. Even though not all the elements included in these standards may be applicable or transferable to lower resource environments, records professionals can use the standards to define the roles and responsibilities of business units in the organisation when they transfer records to the TDR. Using *Submission Information Package* (SIP) agreement records professionals and the records producers can then negotiate acceptable record types and related documentation that must accompany the transfer to contextualise the creation of the digital records and anything that impacts their authenticity and reliability. Their agreement should be captured in a *Submission Information Package* (SIP) agreement. The SIP agreement should be governed by an organisation-wide policy that states that all departments are required to transfer records of enduring value to the Trusted Digital Repository. If such a policy does not exist then the SIP agreements will need to be negotiated unit by unit. This process is discussed below under the heading *Transferring Records.*

Questions related to the ingest, preservation and access process need to be decided during the design phase of the TDR. The following questions should be asked:

- Will the TDR require records to be normalised before transfer to the repository? Will the digital records professional be responsible for normalising the records?

- What type of metadata needs to be attached to the digital record? Will the digital archives accept any type of metadata formats? If not, will a metadata schema have to be designed to standardise metadata fields for transfer?

- What will the digital records professional have to do if key metadata fields are missing?

- What kind of technical infrastructure will be needed to support the TDR to ensure the integrity of the records through time? How will the technical infrastructure itself be maintained such that it is capable of carrying out its role through time?

- What kind of management structure should be in place to manage the TDR? Who should be in charge and what are the roles and responsibilities of those responsible for the TDR?

- When will digital records have to be migrated? When will hardware be refreshed? When will software be migrated?

- What will be the ingest process once materials are transferred? Virus checks? Quarantining? Validation? Assignment of a permanent identifier?

- How will users get access to digital records in the repository?

- Can the TDR architecture be shared among many similar organisations?

These questions underline the complexity of the TDR design and implementation process. For many organisations, such a process may not be possible yet. However, it is important to understand what is involved in order to begin planning for the eventual migration of digital records to a TDR and to keep the TDR as a goal.

What to Do if a TDR Cannot be Implemented Immediately

Initially the digital preservation programme may not have the funds or the capacity to begin implementing a trusted digital repository. However, there are some actions that can be taken as interim measures until there is sufficient capacity to support a TDR.

Firstly, if an organisation has a digital records management system, records can be retained in that system. This is an interim solution because record-keeping systems do not have the same level of integrity as TDRs. However, they provide far better security and integrity

controls than if the records were left uncontrolled. Digital records stored in record-keeping systems need to be monitored periodically to ensure that they remain readable and accessible. Migrations or alterations to the records need to be documented, preferably in the metadata. If that is not possible, a note should be attached electronically to the records to log the event.

Using a records management system as a storage area for inactive records is only a temporary measure. Although there are major exceptions (eg Norway's Noark Standard), many digital record-keeping systems cannot capture and attach the vital metadata to the digital record, for instance validations and preservation interventions. Over time this can damage the authenticity and reliability of the digital records, especially if the notes attached to the records are not properly updated. Moreover, the records will begin taking up a large amount of room on the record-keeping server and they may slow the operation of the record-keeping software. This is why their eventual transfer to an environment supported by TDR software is necessary.

A networked shared drive can be used to store records as an interim measure in the absence of an electronic document/ records management system. The approach to identifying digital records of long-term value in the shared drive will depend on how well the records are organised. If records are poorly organise,d and their records evidentiary value is not clearly identified, the most effective solution is to identify the most important offices creating digital records of longer term value. These records can be moved to a separate folder entitled 'Archives' or 'Digital Preservation' where they can be further organised by office if necessary. Records professionals need to work closely with IT specialists, business unit managers and internal audit to make a case for access to records that are potentially sensitive. The business case for a digital records preservation programme provides a strong basis for advocating the transfer or separation of records for preservation. Some records users may be concerned that their access will be restricted when the records are transferred to the preservation strategy or they may feel that staff will have uncontrolled access. Records professionals should therefore have a strategy for allowing access in a timely manner while ensuring the security and integrity of the records. Strategies that can be considered are:

- Restrict access to the 'Archives' folder. Specified users with the appropriate security clearance must ask records professionals to send by email copies of digital records in the 'Archive'.

- Create sub-folders under the main 'Archives' or 'Digital Preservation' folders and restrict user access to the records in these folders.

Regardless of how records professionals choose to make digital records accessible, they need to log all migrations or preservation interventions. Logs of migrations (eg transfers to the 'Archives' folder) or preservation interventions (eg a change in a record's format to preserve its accessibility) need to be retained along with the records. This can be accomplished using Excel or Word. This is not an automated process. It requires diligence on the part of the records professional to ensure that any alterations to digital records are faithfully recorded. Otherwise the continued integrity and trustworthiness of the records

could be at risk. Again, this type of measure should be temporary. As with the record-keeping system solution, there is no effective way to ensure that validation metadata or any preservation interventions will be comprehensively logged. This is another reason why it is important to begin planning for a TDR environment that will account for these and related digital records preservation measures.

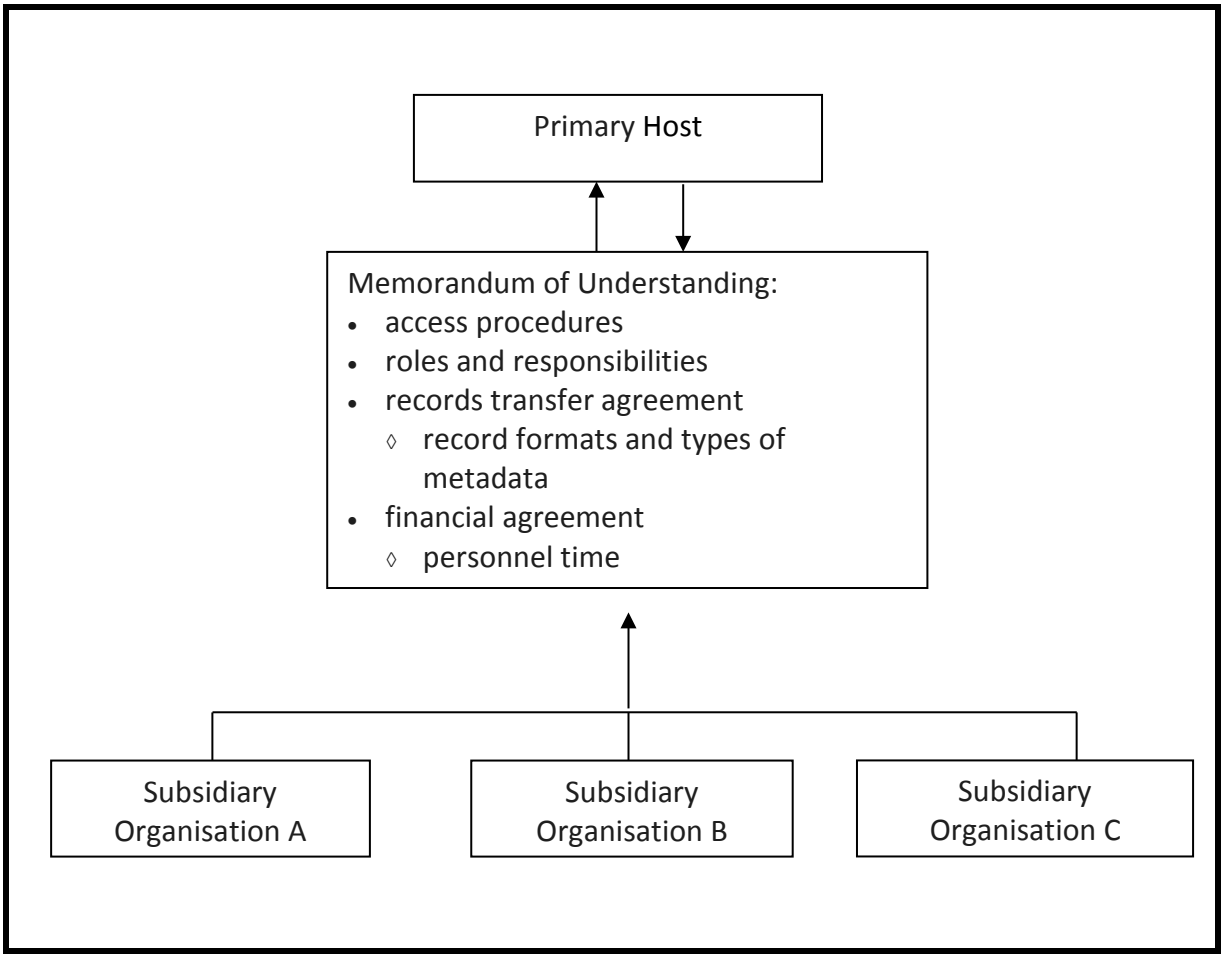
In addition to a lack of expertise in implementing a TDR, many organisations do not have the financial resources to establish a TDR and its supporting environment of policies, standards, procedures and qualified people. It is an expensive undertaking, though it is important to note that the major costs are for hardware and staff time. The software can be open source and freely available. Ultimately, the loss of the records, and the ability to access them, is far more expensive than the cost of developing a TDR.

One way to distribute the costs for TDR development and implementation is to partner with other organisations facing similar digital records preservation challenges or that have taken active steps to develop their own TDR. Examples include the rising number of commercial establishments that have built or are building repositories (or what might be termed 'databanks') for the long-term retention of records in digital form. Other examples include the growing number of government agencies, especially those in the environmental sector, that are building repositories for the long term retention of their valuable digital resources (e.g. environmental data). Computer service bureau, increasingly the product of the consolidation of IT services across the government, are also prime targets for partnerships because they have a vested interest in ensuring the integrity of the data that they are holding and managing in trust on behalf of their numerous government clients.

While some may not be as far along as others in terms of the extent to which their repositories meet all of the requirements of a TDR, organizations such as those cited above, at least provide the basis upon which a partnership, drawing on the strengths of both parties, could be established.

In establishing such a partnership, one organisation can act as the primary host, with the other organisation making contributions towards the purchase of the required hardware and software. The contribution could be, for example, an annual fee paid to the primary host based on the volume of digital records stored in the TDR. This distributed TDR network would need to be based on a Memorandum of Understanding (MoU) between the organisation hosting the TDR and the other organisations. The MoU would need to provide details of the procedures for records transfers, access procedures, cost sharing and budgeting arrangements and other issues.

Figure 3: Distributed TDR Model



The solutions proposed in this step are interim measures, meant as a stop-gap to prevent the loss of vital digital records. Again, in spite of the challenges of implementing a TDR, organisations are encouraged to include what they plan in their overall digital preservation strategy.

Choosing a Digital Repository Software Package

The selection of a TDR software package must be based on a careful assessment of the digital preservation requirements of the organisation. There are a number of TDR software packages available on the market. Software packages are often designed to address specific issues in a given environment or community of practice, which may not meet the organisation's needs. Organisations should investigate what is available and choose a package that meets their preservation needs, personnel capacity, IT infrastructure and budget.

Four well-known TDR software packages are:

Archivematica

https://www.archivematica.org/wiki/Main_Page
Archivematica is an open source, freely available digital repository programme, designed specifically for use in archival environments. The programme meets international standards and good practice measures, such as OAIS. It uses several metadata and encapsulation standards including PREMIS, Dublin Core and METS. Archivematica is fairly easy to use and, as an open source software package, it can easily be customised for user needs. Customisation has the drawback that it may not be possible to receive and upload updates.

Fedora

http://fedoraproject.org/
Fedora is a digital repository software programme, initially developed for libraries but adapted for use in archives. The package is open source and freely available, but unlike Archivematica it may take some IT expertise to get it running. However, because it is open source, it is easily customised for different user environments. Fedora is widely used and has a strong support network to assist in trouble shooting implementation and maintenance problems.

Lots of Copies Keeps Stuff Safe (LOCKSS)

http://www.lockss.org/
LOCKSS was developed by Stanford University Library to manage its digital contents (primarily electronic journals) although now it has been extended to include publications and archives. LOCKSS is an open source, freely available software programme. Like Fedora, it will need IT support to make it operational. It can be customised to meet organisational needs like other open source software packages.

Repository of Authentic Digital Objects (RODA)

http://www.roda-community.org/what-is-roda/

RODA is a digital repository that delivers functionality for all the main units of the OAIS reference model. RODA is capable of ingesting, managing and providing access to the various types of digital objects produced by large corporations or public bodies. RODA is based on open-source technologies and is supported by existing standards such as the OAIS, METS, EAD and PREMIS.

ESS Arch

http://www.essolutions.se/ESSArch

ESSArch is based on OAIS (Open Archival Information System, ISO 14721:2003) and further

developed to include both PreIngest and PreAccess functions, Storage Methods and flexibility to add any metadata standard required. The main conceptual functions are based on traditional archiving preservation processes.

Transferring Digital Records to the TDR: Practical Considerations

Practical considerations are very important when implementing a TDR programme, especially in regard to how the digital records will be transferred to the repository. Any type of ingest process[19] should clearly define the roles and responsibilities of the records producer (the department or office) and the digital records professional. A Submission Information Package (SIP) agreement should detail transfer requirements. The requirements can include responsibility for normalisation, format of the SIP, acceptable record formats and the types of metadata fields that must be attached to the records. The SIP agreement should also highlight the minimum access requirements, such as how quickly a record and its metadata should be made available to the transferring organisation, whether or not there is an online catalogue that can be used to order records, what metadata will be made available in the catalogue, etc. The drawback with SIP agreements is that they must be negotiated with each transferring organisation. This process can be simplified if an organisation-wide policy standardising the ingest process is approved, adopted and enforced.

Another consideration when examining the ingest process are the metadata elements that will be required by the TDR when information is transferred. Some of the software packages included above may only support a certain number of metadata elements. To prevent undue problems during the ingest process, it is important that digital archivists have an understanding of organisational needs for records authenticity as well as the capacity of these software applications to support those needs. It should be noted that many of the TDR software programmes are customisable to meet organisational needs, though too many customisations may prevent the ability to upgrade to newer versions of the TDR software.

Digital records professionals need to consider the best way to transfer the records from the producer into the digital repository. Bandwidth is an important issue that needs to be addressed before to the actual transfer of records. If the bandwidth at the producer's end is slow or limited, a digital records transfer via an internet connection, depending on the size, could slow or prevent internet access for other users. The question of bandwidth becomes particularly important if organisational operations are dispersed across a wide area with varying internet connectivity. For example, government offices may be distributed across the country and connectivity may be limited or sporadic in some areas, This could make any records transfers over fixed line internet connections (ie copper wire or fibre optic) impossible.

[19] 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. (OAIS Reference model).

In order to address the issue of limited bandwidth, some organisations have asked digital records producers to transfer records using external hard drives for any transfer over 200MB. This method can also include transfers via CD and external thumb drives. The only drawback to all of these methods is that it requires a secure method for tracking and ensuring the safe delivery of the external storage devices. If possible, these devices should be encrypted to prevent illicit access.

If an organisation is small and centralised, or if the TDR will only be implemented in one location, the organisation's intranet or a networked drive can be used to facilitate the records transfer via a secured FTP (file transfer protocol) space.

Managing and Preserving Digital Records in a TDR

As noted establishing a trusted digital repository is dependent on having an appropriate regulatory framework in place, including records management policy and the standards and procedures established under them. The following elements are needed:

- *legislation and/ or a high-level policy:* This gives the archives and records management programme oversight of digital records preservation, in partnership with information technology. The support and cooperation of senior management, business managers and IT specialists is essential.

- *metadata policy:* This sets out the minimum metadata elements that must be transferred to the TDR to ensure the authenticity and reliability of records.

- *migration and refreshing policy and procedures:* These are developed with input from the IT department. They should detail when migrations will take place, how they will be carried out, how the bit stream will be properly maintained, and who will be responsible for carrying out migration and quality control measures.

- *normalisation policies and procedures:* These are designed in coordination with IT, according to international good practice. They should detail who will carry out normalisation (records producers, digital archivist or IT), the list of preferred access and preservation formats, metadata elements to be carried over and quality control measure.

- *Submission Information Package policies:* Although in some organisations the SIP agreement may be unit by unit, the policy can detail minimum requirements for submissions, how submissions should be formatted for ingest and the negotiation process (eg contacting the TDR; acceptable document types and metadata; preparing the submission; and validating the submission).

Persistent Uniform Resource Locators (PURL)

Once digital records have been ingested into the digital repository, they should be assigned a Persistent Identifier (PI). The persistent identifier is a unique number that facilitates management of the digital record and links it with its supporting metadata. Digital records and their supporting metadata are often stored in two separate areas of the digital repository. The Persistent Identifier enables these two elements to remain connected, ensuring the authenticity and reliability of the digital records. Examples of persistent identifiers are given below.

http://www.purlz.org/
These are persistent identifiers for web objects that can also be applied to records. While a URL is an address on the World Wide Web, a *Persistent* URL is an address on the World Wide Web that points to other Web resources. If a Web resource changes location (and hence URL), the PURL pointing to it can be updated. A PURL user always uses the same Web address, even though the resource may have moved. This concept is applied to digital objects[20] including records. Software is available for download to assist users in assigning unique identifiers to their digital objects. An example of a template for a PURL is: http://purl.org/net/example/myfirstPURL

Archival Resource Key (ARK)

https://wiki.ucop.edu/display/Curation/ARK
This is a freely available resource but organisations need to register and conform to the ARK standard. An example of a unique identifier using the ARK standards is: http://bnf.fr/ark:/13030/tf5p30086k.

Digital Object Identifiers (DOI)

http://www.doi.org/
In order to assign a DOI to a digital record, an organisation must subscribe to be a member of the DOI consortium. Any organisation wishing to join this group must meet the DOI consortium standards before being permitted to assign persistent identifiers. An example of a DOI is: doi:10.1108/10650750710831466[21]

Assigning a Persistent Identifier

If an organisation has a digital repository software programme, a persistent identifier will be

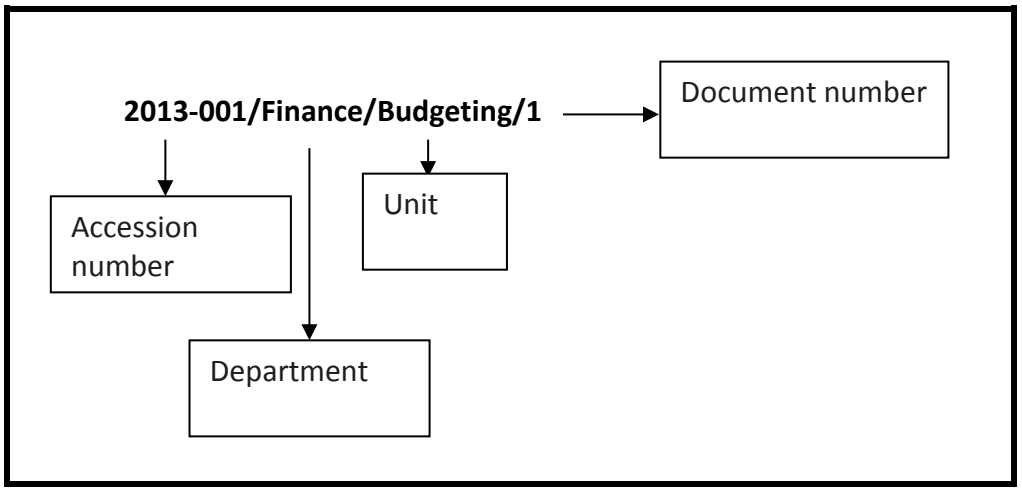
[20] Digital Object: An object composed of a set of bit sequences (Alliance for Permanent Access glossary) Digital objects include, for instance, digital records, digital photographs, audio and video files, e-mails, spreadsheets, digital surrogates (images created by scanning or digitally photographing paper records), etc.

[21] This DOI will link to the following object: Elizabeth Yakel. 'Digital Curation' *OCLC Systems & Services* 23(4) 2007. 335-340

assigned by the system. If the organisation does not have the software, a unique number can be assigned by a records management or information management system as an interim measure.

A simplified method of assigning a unique identifier is to create one that is specific to the organisation. As shown in the example below:

Figure 4: Persistent Identifier



Any records being transferred into the TDR must be validated, quarantined and checked for viruses at the point of ingest. The steps for this part of the ingest process are as follows:

- Prior to ingest, records should be validated or run through a checksum that creates a numerical summary of a digital record (eg a count of the number of bits in the record). This enables the receiver to check to see whether the bit stream received is exactly the same as that sent. Checksum software includes JHOVE and jacksum.

- Another checksum should be run once the digital records are transferred to the repository.

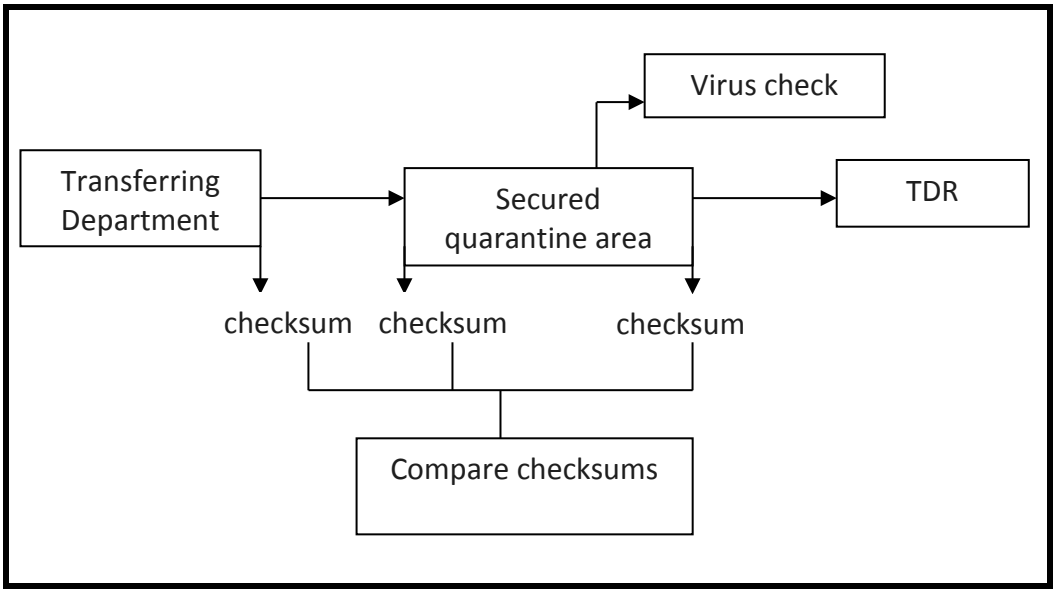
- The two checksums then should be compared. If they are identical, the record has been correctly transmitted to the digital repository.

- Once validated, digital records need to be quarantined to ensure that newly ingested digital records will not infect the digital repository with any viruses. All records ingested into a digital repository should be quarantined on a separate server or location on the network for up to 30 days before they are actually placed in the repository. This is for virus scanning programmes to update their virus detection databases, thus ensuring that all viruses can be detected and removed.

- Once the virus check has been performed, one final checksum should be run and compared to the checksum upon ingest, again to ensure that the digital record has not

been corrupted or altered during any of the ingest procedures.

Figure 5: Checking the Integrity of Digital Records



All of these actions either need to be logged in the metadata that is ingested with the records. The product is an Archival Information Packet (AIP), as described earlier.

Preserving and managing digital records requires server space. During the planning process for the digital records preservation programme, there should be a careful assessment of the short, medium and long-term technical needs of the programme and, in particular, the amount of server space needed to support the TDR. As the programme becomes well-known, a greater number of units or organisations will want to transfer their records. An estimate of required server space can be calculated at the time of the records survey, point the records professional has an idea of the amount of digital objects and metadata to be managed. If, initially, there is limited server space available, ingest will need to be carried out strategically, and only to plan the most important and vital records should be transferred first. It will also be important for contingencies, for example, to allow for the transfer of newly identified vital records. Because every intervention performed on records must be logged in the metadata, the metadata files will also grow. Sufficient space will need to be available so that all relevant actions and interventions can be logged.

In summary, all digital records preservation and management must be supported by a strong regulatory framework and trained personnel. A TDR is more than just the technical components that support the operation of the digital repository software. It requires the policies, procedures and guidelines that govern digital repository operations and the staff to understand and comply with them. This section has attempted to provide some technical issues to consider when establishing a TDR, but ultimately any configuration depends fundamentally on the organisation's resources, the regulatory environment and the available capacity. It also will depend on the types of digital records and related metadata

that need to be managed.

Accessing the Contents of the TDR

Establishing a TDR and a digital preservation programme is not just about preserving the records. They are very much about providing access. In the effort to build the TDR and ensure that the myriad preservation considerations are accounted for, the issue of providing access by users to authentic and trustworthy records is sometimes not addressed to the extent that it should be. The OAIS standard requires that digital repositories include an access component, to enable end-users to retrieve and use the records stored in the TDR. Records professionals, along with stakeholders and partners, must decide the most efficient and effective method for end-user access, based on the organisation's needs and IT infrastructure and capacity. This is especially important when dealing with vendors of TDR software packages or service providers. They must be capable of responding to what could emerge as a sophisticated set of access requirements. Failure to address these requirements could undermine the overall design of the repository itself.

There are two types of access: Website/ online access and intranet/ onsite access. These methods can of course be combined but must meet user requirements.

Intranet access is an internally accessible networked environment where users in an organisation can search and retrieve materials on the TDR. To ensure that users can find what they need, it is important to speak to various users (management, technical and administrative) find out how they search for information. The TDR interface can then be designed to return search results that meet users' needs. The TDR interface should be designed with the help of IT staff. By engaging IT professionals, the TDR user interface can be optimally designed, while working within the limitation of the software. Most TDR software is open source, and add-ons can be built into the application. Records professionals need to consider access restrictions on some sensitive record groups.

A *web portal* provides a public-facing version of the TDR. The design of the site and the search features must take into account both internal and external users' needs. Again IT unit assistance is essential particularly in relation to the website or online portal (if there is one). Often websites keep statistics that detail the demographics of website users. This can be used to gain an understanding of potential TDR site users and help to predict who will be using the TDR. Another important aspect of TDR website design is security, such as firewalls. Decisions need to be taken about which records will be publicly available and which will only be accessible internally to the organisation's staff. In making these decisions, records professionals need to involve business managers and senior managers, to ensure that no sensitive records are accessible through the web portal.

Evaluating the TDR

A mechanism is needed to assess the extent to which the TDR has met its objectives and

continues to meet requirements. Certification and audit standards and guidelines are available to help organisations assess their digital records programmes and TDRs. These tools can also be used to confirm that a digital repository is a *trusted* repository, that is, a repository that is capable of managing the integrity, authenticity and continued accessibility of digital records. Although these standards and guidelines are rigorous and exacting and were developed for well-resourced environments, they can be useful as benchmarks in lower resource environments that are in the process of developing their digital records programmes are being developed.

A number of audit tools and certification standards are available. These have been developed for specific environments and may only be partially applicable in lower resource environments. Organisations need to select the tools that can best be adapted to suit their assessment needs.

Repository Audit and Certification (ISO 16363)

Repository Audit and Certification (*ISO 16363*) is the most recent audit and certification standard, approved by ISO in 2012. The standard was developed by the Consultative Committee on Space Data Systems (CCSDS), the same body which developed OAIS. *ISO 16363* is intended to support and complement OAIS requirements. However, it also combines elements of other standards such as TRAC, NESTOR and DRAMBORA. The standard can be used for self-assessment and for third-party accreditation.

Network Expertise in the Long-term Storage of Digital Resources (NESTOR)

(http://www.dcc.ac.uk/resources/repository-audit-and-assessment/nestor)
'Nestor', one of the earliest TDR certification standards, was developed in Germany around 2003. The nestor method includes soft certification (self-assessment) and hard certification (externally accredited) as assessment methods. There are 14 criteria against which organisations can assess the performance of their digital repository. This good practice method is freely available online.

Trusted Repository Audit and Certification (TRAC)

(http://www.crl.edu/sites/default/files/attachments/pages/trac_0.pdf)
Trusted Repository Audit and Certification criteria was a joint project between the Research Libraries Group and the US National Archives and Records Administration. TRAC is a checklist of requirements that digital repositories should have in order to be certified as 'trusted'. The criteria are divided into three categories: Organisational Infrastructure; Digital Object Management; and Technologies, Technical Infrastructure and Security. TRAC is freely available via the website address provided above.

Digital Repository Audit Method Based on Risk Assessment (DRAMBORA)

(http://www.repositoryaudit.eu/)
DRAMBORA was developed and tested by the Digital Curation Centre and Digital Preservation Europe. This assessment tool uses risk as the basis for creating a strategic approach to digital repository operations, prioritising the issues to be addressed based on their potential impact. The method seeks to provide users with concrete methods for measuring and assessing digital repository operations. DRAMBORA is freely available and can be downloaded by users, once a secured account is created.

National Archives of Norway: A Case Study

The business case for a digital records programme should describe short and medium-term goals to provide senior management with an understanding of the way forward once the programme is established. However, a longer term vision is necessary to give a strategic direction for growth and innovation.

A good example of a strong long-term strategic vision for digital records management and preservation, and one that could serve as a reference for any organisation establishing a digital records programme, is the Noark (Norwegian Archive Standard) framework established by the National Archives of Norway. Norway's vision is achieved through a powerful combination of interconnected 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 is the emphasis on protecting the security, content and context of the information and reducing the time between creating records and providing public access. The Government is committed to meeting increasing citizen expectations for rapid, almost real time access to government information.

The components of the framework, which are fundamentally the same as those described in Lesson 1, are described in the following sections.

Laws and policies

In Norway the Constitution, the Freedom of Information Act and the National Archives Act provide a comprehensive legislative umbrella for the creation, maintenance, access and preservation of digital records throughout government.

The Constitution of the Kingdom of Norway, under article 100, enshrines the right of access to government information by stating that it is the responsibility of agents of the State to,

'…create conditions that facilitate open and enlightened public discourse'[22]. However, access to information requires properly managed information. This is facilitated through the requirements and provision of the National Archives Act and the Freedom of Information Act. The National Archives Act requires that all government information systems use the Noark standard to log types of metadata fields. These metadata fields are then abridged and uploaded to an online citizen 'access to information' portal. The latter is mandated by the provisions of the Freedom of Information Act.

This legislative framework has meant that the term 'archives' applies to the entire life cycle of records. It also means that the National Archives is mandated to facilitate the proper management of records including those in digital form. Ultimately, the legislation has facilitated the establishment of a government-wide approach to managing the integrity of records and in strengthening the position and impact of the National Archives.

Governance and Management

To be effective, a digital records programme requires oversight and direction from senior management. In Norway, this is provided by a high level senior steering committee comprising senior officials from lead ministries and including the National Archives. This direction is aided by the existence of an effective governance structure for approving standards to support the work of the National Archives of Norway. A government-wide policy assigns responsibility for the management of records to officials at all levels across the government.

Noark

Noark has been used as a record-keeping standard by ministries, departments and agencies in Norway since 1984. The original intent of Noark was to standardise the metadata fields for electronic registry software being used in the Norwegian civil service. Noark has been updated over the years, but it was Noark 4 that marked a significant change in the functional requirements for government systems: it was the first of the Noark series to include sections on email and case management. Noark 5, the newest version of the standard, builds on Noark 4 by streamlining national and international standards on electronic record-keeping. Noark 5 is a modular standard, with a minimal number of mandatory requirements. The intent is to offer flexibility to users while enabling basic records integrity requirements to be met so that the National Archives can ensure the on-going preservation of, and access to, digital records. Noark contains:

- requirements for the functionality that must be respected by systems if records are to be properly managed through their life cycle (capture, maintenance, retrieval, disposition)

[22] Constitution of the Kingdom of Norway, Article 100.

- 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
- rules for identifying and authorising system users, allocating and administering access rights, and establishing log and audit trails.

Compliance with the Noark standard is mandatory for government ministries, as well as information management system vendors. Noark complements and reinforces existing Archives Act regulations that require government ministries to keep a journal logging all incoming and outgoing records. The standard requires additional contextual information relating to records creation and maintenance to facilitate the transfer of digital records to the National Archives of Norway's trusted digital repository.

The National Archives of Norway is developing its TDR as a technology-neutral means of preserving digital records using standardised digital preservation models that comply with international IT security standards, as well as with the Open Archival Information System (OAIS) Standard and the Trusted Repository Audit and Certification checklist. The Noark Standard ensures that the TDR will be able to ingest digital records and metadata through a standardised process. Copies of digital records are currently being transferred to the Archives within five to 10 years of creation to protect records' integrity even if the original record is retained within the creating agency for 25 years as required by law.

Finally, Noark requirements not only support the management and preservation of digital records but also access to them, as mandated by the Freedom of Information Act. Every information management system used by an agency must capture a set of metadata elements at the point of registration. Under FOI, every agency is required to produce a register of this metadata and make it available through an online portal (the OEP). This register of metadata is an abridged version of the Noark required records registration metadata. The OEP portal provides central access to all records. Government employees, citizens, businesses and other users can use the metadata to access records across central government. 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. The register covers any record type, including emails. The metadata is uploaded to the OEP a few days after creation to allow time for staff to ensure that the records do not contain any personal or restricted information.

People

Civil servants in government ministries, departments and agencies are trained in Noark and in complying with the work processes for identifying, indexing and protecting records

documenting government actions and decisions. This ensures that records are properly logged and managed in the system.

The National Archives staff are qualified to assume a leadership role in developing and maintaining Noark and ensuring its effective application and use across the Government. Furthermore, they have the expertise, in partnership with others, to build all the components of the digital preservation programme vision.

Assessing Student Understanding of the Lesson

At the end of this lesson, your understanding of digital records preservation should have grown to the point that you are ready to start to undertake actions to address the issue within an organisation.

To test your understanding, prepare short answers to the questions that follow (no more than 200 words) or work a friend or colleague and explain your replies verbally to see whether you understand the issues clearly.

- What role does the business case play in developing a digital records preservation strategy?

- Why are metadata so important for digital records preservation?

- What is the difference between storage and refreshing? Migration and normalisation? Encapsulation and emulation?

- What are the components of a regulatory framework?

- How does digital records preservation fit within an organisation-wide records management framework? What issues would you consider to be most significant to address in your environment? What would be the appropriate level of strategy in your situation?

- What is a trusted digital repository, and what advantages does it offer? Is it feasible to develop a TDR in your situation, and if not, why not.

What is a Submission Information Package agreement and what issues should it address?

- What is the difference between a trusted digital repository and an electronic records management system?

- What is a persistent identifier and why are persistent identifiers important for digital records preservation?

- What is a checksum and why are they important for digital records preservation?

- Either as an in-depth essay or as a group discussion, outline the ways in which the National Archives of Norway's strategic vision for digital records management (described at the end of this lesson) addresses the general principles described at the beginning of this lesson). Is the vision a) feasible, sustainable, practical and appropriate, b) multi-disciplinary, flexible, streamlined and integrated. Which aspects of this vision would be helpful/ achievable in your environment?

Finally, to help you start to undertake actions to address digital records preservation, undertake some or all of the following exercises:

1 Consider the different ways in which you would explain the need for digital records preservation to a) a business unit manager or b) an IT specialist. What are the top three arguments that you would use in each case?

2 What information would you need to gather when undertaking a digital records preservation survey? What difficulties might you have in gathering this information?

3 Write a job description for a digital records preservation officer working in a large organisation in your country.

4 Produce an outline structure of the section headings in a business case and briefly describe what will be covered under each one.

5 Research one of the TDR software packages listed in this lesson and write a brief evaluation of it. What challenges would you face in introducing this package in your country?

6 Describe the main steps that should be followed when transferring digital records into a trusted digital repository. What challenges might you face in your situation?

LESSON 4: COMMUNICATING THE MESSAGE

This lesson provides advice on how records professionals working in lower resource environments can communicate the concepts, issues and strategies associated with the preservation of digital records to stakeholders. The information here, and indeed the module as a whole is intended not only to enhance knowledge but also to encourage and help records professionals to engage in constructive communication with the other stakeholders who should help to protect and preserve digital records.

Partners and Stakeholders

Sometimes the most challenging step in the process of building digital preservation programmes is to begin the discussion with senior managers, IT specialists, legal affairs specialists or others involved in creating, using and managing digital records. This is a critical step because records professionals cannot on their own address all the records management issues involved in preserving digital records. Partnerships are necessary especially with business managers and IT specialists. Often records professionals do not feel that they have the knowledge and expertise to engage in a meaningful conversation. As a result, discussions are not held, partnerships are not formed and digital preservation issues continue to pose serious risks for the organisation.

Records professionals need to build partnerships with IT staff responsible for information security. These specialists are needed during the design and implementation phases of the digital records management systems and of the digital archive (TDR) to ensure that records are properly secured. Among the key stakeholders that should be approached is the E-Government Office. In virtually all developing countries, an E-Government office is in place as an organizational unit that is often separate from the Government Computer Bureau or Centre. Partnering with the e-Government Office as well as the Government Computer Bureau is a must given their importance and profile within the government.

Another key partner in a digital preservation programme is an organisational 'champion' to promote the programme at senior management level. The champion should hold a senior position and be able to support budgetary requests as well as regulatory and workflow changes. This includes senior managers with responsibility for programmes and systems that create records needing long-term preservation or with a direct stake in digital preservations issues. It is important to identify a champion early in the planning process.

Finally, internal audit staff can be strong partners. The internal audit department understands the importance of properly organised and accessible digital records as audit staff rely on this information. Working with audit staff can give records management and

digital records preservation a higher profile. Audit reports and assessments can incorporate findings in relation to digital records and can help build a stronger basis for establishing an organisation-wide digital preservation programme. The case can be strengthened further if the internal audit reports are supported by external audit reports, such as those produced by the Auditor General, especially if they highlight the implications of poor record-keeping. In collaborating with audit staff, records professionals will be able to identify and sometimes quantify the risks associated with digital records management which, in turn, will help senior management understand the value of a digital preservation programme.

Communicating the vision and gaining support must be part of a broader approach to engaging with key stakeholders in the organisation. The next section provides suggestions for doing this.

Communicating with Stakeholders

This section offers guidance on how records professionals can communicate digital preservation concepts, issues and strategies to key stakeholders to secure help in incorporating digital preservation in organisational systems and work programmes, and in obtaining resources to fund this work.

It can be daunting to begin talking to senior colleagues and IT specialists. Will they ask difficult questions? Will they say it's not a priority? Will they say it is not a matter that should concern a records manager? Gaining their support is essential because records professionals cannot address digital preservation issues on their own (or any records management issue involving the management of digital records). Partnerships are essential, especially with business managers and IT specialists; in most organisations, at a relatively early stage, it is necessary to have senior management support. Unfortunately, few records professionals feel they have the knowledge and expertise to engage in a meaningful conversation. As a result, discussions are not held, partnerships are not formed, and the failure to tackle digital preservation issues continues to put the organisation at risk.

Before beginning the conversation, records professionals should prepare themselves. They need to:

- Review the material covered in this module and to be comfortable with the concepts, the examples and the suggestions being made.

- Research the organisation:

  - 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 interests them? 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 long-term preservation issues and are only really interested in maintaining existing systems. However, there will be some (perhaps not working full time in your organisation) such as business systems analysts, data managers or information architecture specialists. They will be familiar with preservation concepts and should be interested.

- Based on this research, identify digital preservation issues that affect individual and organisation-wide work processes. 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 should be highly visible and fundamental 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 digital preservation.

- 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 digital preservation issues within key work process(es) supported in the individual's area of responsibility. Examples should be relevant to the key work processes and may be based on what you know from your own observations or what you have been told by reliable colleagues; 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 for addressing the issues. This could involve further meetings, perhaps with the individual's work group, or more senior staff and other stakeholders, where you would present the results of your initial discussions. This could, for instance, be a plan to introduce digital records preservation measures in an existing systems development initiatives or to establish an entirely new initiative.

- Use the concepts, issues and suggested approaches described in this module to shape the nature of your 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 also should be relevant to individual interests and needs.

- Test the effectiveness of the initial conversation(s) by asking yourself: Did the individual understand the message, the main idea, the point? Was it easy to get your message across? If the individual understood the message it, did he/ she want to do something about it? The individual needs to believe *who* is saying it, *what* is being said, and *how* it is being said. Otherwise communication begins to break down. Credibility is critical because the individual may understand your message, but not fully accept your credibility. The individual should not only understand the message but should want to spread the message among other stakeholders. The message 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 your meeting with the individual. Or, there could be a briefing with the individual's manager and/ or a group of key stakeholders to help make stakeholders aware of the issues and propose an overall strategy. The key is to use the initial meeting as a stepping stone for inserting the digital preservation inside the organisation's thinking and inserting yourself in the processes for building or modifying systems where preservation issues will need to be addressed.

The objective is to enhance awareness of the importance of digital preservation, and to have key stakeholders act on this awareness. It will be difficult to proceed any further if such awareness is not in place and stakeholders are not prepared to act. That is why it is essential to extend awareness to senior managers.

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 digital preservation in briefings on wider issues. These could be, for instance, the 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 digital preservation 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 digital preservation and the issues and risks the organisation faces. Rather than simply providing a briefing for information, it is best if the stakeholders themselves can propose initiatives to address the issues. The following steps are suggested for handling such a meeting. These steps can also be used to guide any meetings with managers or senior officials about digital preservation:

- 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.

- Explain the purpose of the meeting (eg to understand digital preservation issues; to obtain support for an upcoming meeting where digital preservation will be discussed; to request that they serve as a 'champion' for advancing the issue.

- Ask the senior managers or officials how they see their official responsibilities in relation to digital preservation and the wider issues of access to reliable and meaningful information. This will give you an idea why the points you are making will be important to them.

- Explain in their terms how you view digital preservation. Provide them with a general understanding of digital preservation 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; from the perspective of their own experience; of the functions and activities for which they are responsible and from the perspective of the organisation as a whole.

- Ask for suggestions for addressing the issues. Here is where you can offer some ideas, but be sure to present them in a way that the senior management understand and feel responsible for them.

- Bring the session to a close by returning the original objectives for the meeting: providing information to enhance awareness; asking them to support the digital preservation initiative (eg securing cooperation of the managers and staff in their business area; and in the organisation's senior management).

- 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 resolving digital records preservation issues. Equipped with the knowledge presented in this module and from the additional resources identified at the end, the records professional should be seen as a valued member of the team. The record professional has unique knowledge 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 business 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 achieve this goal.

Assessing Student Understanding of the Lesson

With the guidance in this lesson, you should now be able to identify the key stakeholders in building a digital preservation programme and start to devise a strategy for approaching them. The following activities should help you to prepare further:

- Prepare a list of the main stakeholder groups for a digital preservation programme within an organisation. If you are working in an organisation, start to identify the individuals who represent those stakeholder groups within your organisation. How could digital preservation help them?

- Have a friend or colleague time you, and give yourself one minute to make the case for digital records preservation 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.

- Practise making the case to a variety of different audiences. For instance, pretend that you are talking to a member of the public or a government minister, or your own manager and think about how you have to change what you say.

➢ ADDITIONAL RESOURCES

Glossary of Terms

All terms are from the InterPARES glossary (http://www.InterPARES.org/ip3/ip3_terminology_db.cfm) unless otherwise noted.

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.

Bitstream: Digital data encoded in an unstructured sequence of binary bits that are transmitted, stored or received as a unit.

Conversion: The process of transforming a digital document or other digital object from one format, or format version, to another one.

Data: The representation of facts, concepts, information, or instructions in a manner that is suitable for processing by an information system; the smallest meaningful units of information.

Digital Curation: The selection, preservation, maintenance, collection and archiving of digital assets. Digital curation establishes, maintains and adds value to repositories of digital data for present and future use. (Wikipedia)

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 preservation: The specific process of maintaining digital materials during and across different generations of technology over time, irrespective where they reside.

Digital records: 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.

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, Space Data and Information Transfer Systems, open Archival Information

System, Reference model *ISO 14721, 2003*).

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). *(Society of American Archivists)*

- 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).*

Migration (of records): The process of moving records from one system to another to ensure their continued accessibility as the system becomes obsolete, while leaving intact their extrinsic and intrinsic elements of form.

Normalisation: The process of creating and/ or storing digital documents or other digital objects in a limited number, often standardised, of data or file formats

Preservation: The whole of the principles, policies, and strategies that controls the activities designed to ensure materials' (data, documents, or records) physical and technological stabilisation and protection of intellectual content.

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 (InterPARES); 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*)

Record-keeping: The function of capturing, storing and maintaining records and information about them, and the set of rules governing such function.

Record-keeping System: A set of rules governing the storage, use, maintenance and disposition of records and/or information about records, and the tools and mechanisms used to implement these rules.

Trustworthiness: The accuracy, reliability and authenticity of a record.

Sources Used to Develop This Module

Archives New Zealand

Digital Record-keeping Standard, 2010
http://archives.govt.nz/sites/default/files/S5_Digital_Record-keeping_Standard_PDF_0.pdf

Archives New Zealand, Digital Continuity Plan
http://archives.govt.nz/advice/government-digital-archive-programme/digital-continuity-action-plan/html-version

Digital Curation Centre

DCC Digital Curation Reference Model
http://www.dcc.ac.uk/resources/curation-lifecycle-model

DCC Curation Reference Manual
http://www.dcc.ac.uk/resources/curation-reference-manual

DRAMBORA
http://www.repositoryaudit.eu/

TRAC
http://www.dcc.ac.uk/resources/repository-audit-and-assessment/trustworthy-repositories

Digital Preservation Coalition

Digital Preservation Handbook
http://www.dpconline.org/publications/digital-preservation-handbook

Electronic Resource Preservation and Access Network (ERPANET)

http://www.erpanet.org/guidance/index.php;
Relevant products include:
Ingest strategies
Costing orientation
Selecting technologies
Digital preservation policy
Risk management

International Council on Archives

Digital Records Pathways: Module One: Introduction – A Framework for Preservation
http://www.ica-sae.org

International Records Management Trust

Preserving Electronic Records: Module 4. Training in Electronic Records Management
http://www.irmt.org/documents/educ_training/term%20modules/IRMT%20TERM%20Module%204.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

ISO 14721: Open Archival Information System Reference Model

National Archives of Australia

An Approach to the Preservation of Digital Records, 2002
http://www.naa.gov.au/Images/An-approach-Green-Paper_tcm16-47161.pdf

Digital Preservation: Illuminating the past, guiding the future, 2006
http://www.naa.gov.au/Images/XENA_brochure%5B1%5D_tcm16-47233.pdf

National Archives of Australia, How we preserve digital records of Australian Government agencies
http://www.naa.gov.au/records-management/agency/preserve/e-preservation/index.aspx

National Archives of Norway

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

Preservation and Long-term Access Through Networked Services (PLANETS)

Numerous sources
http://www.planets-project.eu/

Public Record Office of the State of Victoria

Standard for Electronic Records
http://prov.vic.gov.au/wp-content/uploads/2012/01/Mgmt_Electron_Records.pdf

VERS, Electronic Records Project, State Records Authority of State of Victoria
http://prov.vic.gov.au/government/vers

Queensland State Archives

Digital Continuity: Ensuring the Continued Accessibility of the Queensland Government's Digital Records, April 2011
http://www.archives.qld.gov.au/Record-keeping/GRKDownloads/Documents/digital_continuity_report.pdf

Digital Archiving Discussion Paper: Informing an Approach to the Long-term Management and Preservation of Government Digital Records, May 2010
http://www.archives.qld.gov.au/Record-keeping/GRKDownloads/Documents/QSA-Digital-Archiving-Discussion-Paper.pdf

Digital Archiving Survey, August 2010
http://www.archives.qld.gov.au/Record-keeping/GRKDownloads/Documents/Digital-Archiving-Survey.pdf

State Records Authority of New South Wales

State Records Authority of New South Wales, Digital records preservation in the NSW public sector: a discussion paper
http://www.records.nsw.gov.au/record-keeping/topics/documents/record-keeping-digital/Discussion%20paper%20on%20digital%20records%20preservation%20Nov%202007.pdf

Guides produced on 'Digital Record-keeping'
http://www.records.nsw.gov.au/record-keeping/government-record-keeping-manual/guidance/guidelines/guidelines#digital-record-keeping

The National Archives (UK)

Digital Records Infrastructure Catalogue: First Steps to Creating a Semantic Digital Archive
http://www.nationalarchives.gov.uk/documents/information-management/xml-london-tna-rw.pdf

Digital preservation guidance notes
http://www.nationalarchives.gov.uk/information-management/projects-and-work/guidance.htm

PRONOM
http://www.nationalarchives.gov.uk/information-management/projects-and-work/guidance.htm

DROID
http://www.nationalarchives.gov.uk/information-management/projects-and-work/droid.htm

US National Archives and Records Service

Electronic Records Management Guidance
http://www.archives.gov/records-mgmt/initiatives/erm-guidance.html

Toolkit for Managing Electronic Records
http://www.archives.gov/records-mgmt/toolkit/