INTERNATIONAL RECORDS MANAGEMENT TRUST

Module 1

UNDERSTANDING THE CONTEXT OF ELECTRONIC RECORDS MANAGEMENT

Training in Electronic Records Management

MODULE 1

UNDERSTANDING THE CONTEXT OF ELECTRONIC RECORDS MANAGEMENT

Training in Electronic Records Management

General Editor, Laura Millar

MODULE 1

UNDERSTANDING THE CONTEXT OF ELECTRONIC RECORDS MANAGEMENT

INTERNATIONAL RECORDS MANAGEMENT TRUST

Module 1: Understanding the Context of Electronic Records Management

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

Printed in the United Kingdom.

Inquiries concerning reproduction or rights and requests for
additional training materials should be addressed to

International Records Management Trust
4th Floor
7 Hatton Garden
London EC1N 8AD
UK
Tel: +44 (0) 20 7831 4101
Fax: +44 (0) 20 7831 6303
Email: info@irmt.org
Website: http://www.irmt.org

Version no. 1/2009

TERM Project Personnel

Project Director

Dr Anne Thurston, founder of the Trust, is a pioneer in defining international solutions for the management of public sector records. Both as an academic and as a programme director, she has extensive experience of working with many different governments to provide practical solutions for strengthening record-keeping systems. Her groundbreaking survey of record-keeping systems across the Commonwealth resulted in the establishment of pilot projects to restructure records systems in The Gambia and Ghana, and she established the Trust in 1989 to develop and extend this work. She joined the staff of the School of Library, Archive and Information Studies at University College London in 1980 to develop the Masters' in Records and Archives Management (International); she was also a Reader in International Records Studies. In 2000 she was awarded an OBE for services to public administration in Africa; she received a lifetime achievement award from the UK Records Management Society in 2006. She was awarded the Emmett Leahy award for Outstanding Contributions to the Information and Records Management Profession in 2007.

General Editor

Laura Millar divides her time among three careers: in archives as an archival and information management consultant and educator; in publishing as a writer, editor, and instructor; and in distance education as a curriculum developer, instructional designer, and course author. She received her MAS degree in archival studies from the University of British Columbia, Canada, in 1984 and her PhD in archival studies from the University of London in 1996. From 1994 to 1999, as Managing Editor of the Management of Public Sector Records Study Programme for the International Records Management Trust and the International Council on Archives, she was responsible for the development, testing, and delivery of 18 distance education training modules and 15 associated publications in archives, records and information management. She is the author of a number of books and articles on various topics in archives, publishing, and distance education.

Project Manager

A New Zealand born Australian based in Seattle, Washington, Michael Hoyle has a Masters degree in Information Management and Systems from Monash University in Australia. Prior to moving to Seattle in 2005, he was the Group Manager, Government Recordkeeping at Archives New Zealand. He has also worked in various information management and other roles in several government agencies in Australasia, including ten years at Archives New Zealand and six years at the National Archives of Australia. Michael has been a council member of the Archives and Records Association of New Zealand (1996 to 1999) and served the Association of Commonwealth Archivists and Records Managers (ACARM) as Deputy Chair (2000 to 2002) and as Chair (2002 to 2004). He also served the Pacific Branch of the International Council on Archives (PARBICA) as Secretary General (2002 to 2003) and President (2003 to 2004).

Module 1: Understanding the Context of Electronic Records Management

Authors

Segomotso Keakopa
Laura Millar
Greg O'Shea
Lori Podolsky Nordland
Jim Suderman

Additional Contributors

Christine Ardern
Andrew Griffin
Lekoko Kenosi

Reviewers

Andrew Griffin
Michael Hoyle
Jim Suderman
Setareki Tale
Anne Thurston
Richard Wato
Zawiyah Mohammed Yusef

The International Records Management Trust would like to acknowledge the support and assistance of the Department for International Development (UK).

Contents

Figures

PREFACE

ABOUT THE *TERM* PROJECT

This module is part of an educational initiative called *Training in Electronic Records Management* or *TERM*, developed by the International Records Management Trust as part of a wider project to investigate issues associated with establishing integrity in public sector information systems. Begun in 2006, *Fostering Trust and Transparency in Governance: Investigating and Addressing the Requirements for Building Integrity* in Public Sector Information Systems in the ICT Environment was a project designed to address the crucial importance of managing records in the information technology environment. The focus of the study was pay and personnel records, since payroll control and procurement are the two major areas of government expenditure most vulnerable to misappropriation, and payroll control is, therefore, a highly significant issue for all governments.

The project provided an opportunity to explore the management of paper records as inputs to financial and human resource management information systems, the management of electronic records as digital outputs and the links between them. It also involved examining the degree to which the controls and authorisations that operated in paper-based systems in the past have been translated into the electronic working environment.

The primary geographical focus of the study was eastern and southern Africa, and two significant regional bodies participated: the Eastern and Southern Africa Regional Branch of the International Council on Archives (ESARBICA) and the Eastern and Southern African Association of Accountants General (ESAAG). Four countries from the region (Zambia, Botswana, Lesotho and Tanzania) hosted case studies, and comparative studies were carried out in West Africa (Ghana) and Asia (India).

The products of this project, which will be available without charge, include

- route maps for moving from a paper-based to an electronic information environment
- good practice indicators to measure records management integration in ICT control systems
- these training modules on the management of records in electronic form.

The project deliverables also include case studies conducted in Botswana, Ghana, India, Sierra Leone, Tanzania and Zambia. The studies focused primarily on issues related to the management of human resources and payroll functions in governments and involved research into paper-based and computerised personnel management systems. However, they provided an opportunity also to examine records and information management in the public sector in these countries. The case studies are most relevant to those readers focusing on personnel and payroll management.

However, the findings also offer valuable insights into the challenges of automation and electronic government, and the issues involved with making the transition from paper-based to electronic records and information management. The final case studies are being made available on the Trust website at www.irmt.org.

The case studies all point to the general need for greater integration of records management in the design and implementation of electronic information and communications (ICT) systems. The good practice indicators produced by this project are intended to help governments determine whether or not records management requirements have been integrated in ICT systems and to provide a high-level guide to records management integration. The indicators are particularly relevant to Modules 2 and 3. The good practice statements that underpin the indicators are derived from generally accepted international standards but are also informed by the findings of the case studies.

It is hoped that the research conducted as part of this project will offer governments the resources they can use to increase their capacity to manage paper and electronic records as accurate and reliable evidence in electronic environments. Their ability to measure progress toward accountability will be enhanced, and there should be a higher success rate of e-governance applications.

Project Steering Team

An international steering team oversees the work of the project, consisting of the following members.

- **Stephen Sharples**, Chair of the Steering Committee, Senior Governance Adviser, Africa Policy Department, UK Department for International Development
- **Anne Thurston,** Project Director and International Director, International Records Management Trust
- **Michael Hoyle,** Project Manager, International Records Management Trust
- **Andrew Griffin,** Research Officer and UK Director, International Records Management Trust
- **Jerry Gutu,** Chief Executive Officer, East and Southern African Association of Accountants General (ESAAG) (2006)
- **Cosmas Lamosai,** Chief Executive Officer, ESAAG (2007 and 2008)
- **Kelebogile Kgabi,** Chair, Eastern and Southern African Branch, International Council on Archives (ESARBICA), and Director, Botswana National Archives and Records Services (2006)
- **Gert Van der Linde,** Lead Financial Management Specialist, Africa Division, World Bank
- **Peter Mlyansi,** Director, Tanzania Records and National Archives Department and Chair of ESARBICA (2007 and 2008)
- **Nicola Smithers,** Public Sector Specialist, Africa Region, World Bank

- **David Sawe,** Director of Management Information Systems, Government of Tanzania
- **Ranjana Mukherjee,** Senior Public Sector Specialist, Asia Region, World Bank.

More information about the project and the other deliverables can be found on the International Records Management Trust website at http://www.irmt.org/building_integrity.html.

About the Modules

The following modules have been produced as part of this project:

Module 1 *Understanding the Context of Electronic Records Management*

Module 2 *Planning and Managing an Electronic Records Management Programme*

Module 3 *Managing the Creation, Use and Disposal of Electronic Records*

Module 4 *Preserving Electronic Records*

Module 5 *Managing Personnel Records in an Electronic Environment.*

As well, the following two resources have been produced:

Additional Resources a bibliography of key resources related to the management of electronic records.

Glossary of Terms a consolidated glossary of relevant records management, electronic records management, information technology and computer terms.

These materials are primarily intended for use by records management practitioners in developing countries. The focus is on providing both a conceptual framework and practical guidance about important issues related to electronic records management. The goal is to produce a series of resources that can be used in a variety of ways, such as

- for self study
- for in-house training
- for management training institutes
- as a resource for university or college courses
- as supporting information for distance education courses.

A series of self-study questions has been included at the end of each module. These questions can be used by readers to assess their own understanding of the content provided in the module. The questions may also be used by trainers or educators to develop activities, assignments or other assessments to evaluate the success of any training offered. In order to facilitate the widest possible use of these questions by both learners and educators, they have been gathered together in one place at the end

of the module rather than interspersed throughout the text. Readers interested in developing educational or training initiatives using these modules are also directed to the MPSR training resources developed in 1999, and listed below, which offer guidance on how to adapt and use educational tools such as these.

Contributors

A number of records and information professionals were asked to contribute to the modules, including representatives from such countries as Australia, Botswana, Canada, Kenya, Singapore, South Africa, the United Kingdom and the United States. The following people have contributed to the project as contributors, editors, reviewers and production assistants.

- Keith Bastin, United Kingdom, reviewer
- Adrian Brown, United Kingdom, contributor
- Luis Carvalho, United Kingdom, administrative coordinator
- Donald Force, United States, editor
- Elaine Goh, Singapore, contributor
- Andrew Griffin, United Kingdom, contributor
- Greg Holoboff, Canada, graphic artist
- Michael Hoyle, United States, contributor
- Shadrack Katuu, South Africa, contributor
- Segomotso Keakopa, Botswana, contributor
- Lekoko Kenosi, Kenya, contributor
- Charles Kinyeki, Kenya, reviewer
- Barbara Lange, Canada, desktop publisher
- Helena Leonce, Trinidad and Tobago, reviewer
- Mphalane Makhura, South Africa, reviewer
- Walter Mansfield, United Kingdom, contributor, editor
- Peter Mazikana, Zimbabwe, contributor
- John McDonald, Canada, contributor
- Laura Millar, Canada, contributor, editor
- April Miller, United States, contributor
- Patrick Ngulumbe, South Africa, reviewer
- Greg O'Shea, Australia, contributor
- Lori Podolsky Nordland, Canada, contributor
- Peter Sebina, Botswana, contributor
- Anthea Seles, Canada, contributor
- Elizabeth Shepherd, United Kingdom, reviewer
- Kelvin Smith, United Kingdom, contributor
- Jim Suderman, Canada, contributor, reviewer
- Setareki Tale, Fiji, reviewer

- Louisa Venter, South Africa, reviewer
- Justus Wamukoya, Kenya, reviewer
- Richard Wato, Kenya, reviewer
- Geoffrey Yeo, United Kingdom, reviewer
- Zawiyah Mohammad Yusef, Malaysia, reviewer.

Relationship with the *MPSR* Training Programme

The modules are designed to build on and support the *Management of Public Sector Records* training programme, developed by the International Records Management Trust in 1999. The MPSR training resources consist of over thirty separate training tools that address basic records management issues for developing countries. While some information found in those earlier modules may also be found in this new training programme, the concept behind this new set of modules is that they build upon but do not replace those earlier fundamental records management training tools. However, this new TERM programme focuses on the electronic record-keeping environment that is becoming so prevalent in the early years of the 21st century.

Readers wishing to orient themselves to basic records management principles will want to refer back to those MPSR resources, which are available free of charge from the International Records Management Trust website at www.irmt.org. Those training resources are identified below.

Training Modules

1 The Management of Public Sector Records: Principles and Context
2 Organising and Controlling Current Records
3 Building Records Appraisal Systems
4 Managing Records in Records Centres
5 Managing Archives
6 Preserving Records
7 Emergency Planning for Records and Archives Services
8 Developing the Infrastructure for Records and Archives Services
9 Managing Resources for Records and Archives Services
10 Strategic Planning for Records and Archives Services
11 Analysing Business Systems
12 Understanding Computer Systems: An Overview for Records and Archives Staff
13 Automating Records Services
14 Managing Electronic Records
15 Managing Financial Records
16 Managing Hospital Records
17 Managing Legal Records
18 Managing Personnel Records

Procedures Manuals

19 Managing Current Records: A Procedures Manual

20 Restructuring Current Records Systems: A Procedures Manual

21 Managing Records Centres: A Procedures Manual

22 Managing Archives: A Procedures Manual

23 Planning for Emergencies: A Procedures Manual

24 Model Records and Archives Law

25 Model Scheme of Service

Educators' Resources

26 Educators' Resources

- Introduction to the Study Programme
- Glossary of Terms
- Additional Resources for Records and Archives Management
- Educators' Resource Kit
- Writing Case Studies: A Manual.

Case Studies

27 Case Studies Volume 1

28 Case Studies Volume 2

29 Case Studies Volume 3

The introduction to each module in the TERM programme includes more specific information about relevant MPSR resources that readers may wish to review in association with the TERM module in question.

A Note on Terminology

As with any material related to computer technologies, these modules contain a great deal of specialised terminology. Every attempt has been made to define key terms the first time they are used. When important concepts are discussed cross-references are included as appropriate to earlier references or to the glossary of terms. Readers are also directed to the *Additional Resources* tool for more information on various topics, and web addresses are included whenever detailed information is provided about particular organisations or specific resource materials.

The modules are written using British English (programme, organisation) though of course many computer terms use American English: thus an organisation may run a records management 'programme' but it uses a particular software 'program.' Abbreviations and acronyms are defined the first time they are used in each module and are used as sparingly as possible.

One exception is ERM for 'electronic records management': this acronym is used regularly throughout all the resources as appropriate when referring to the general concept of managing computer-generated records. When referring to an electronic

records management system – that is, to specific software programs designed to manage electronic records – the term ERMS is used. It is recognised, however, that ERMS software may also offer document management features: supporting the creation, use and maintenance of both documents (such as works in progress) and records (official, final documents). When referring specifically to software that manages both documents and records, the acronym EDRMS is used, but the acronym ERMS is used more often, particularly when the concept of electronic records management systems is discussed more generally.

For More Information

For more information or to download a copy of these resource materials free of charge, go to the International Records Management Trust website at www.irmt.org. The Trust can be reached as follows:

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

phone +44 (0) 20 7831 4101
fax +44 (0) 20 7831 6303
email info@irmt.org
website www.irmt.org

INTRODUCTION

Around the world, individuals, organisations and governments have embraced information technologies. In 1977 there were fewer than 50,000 personal computers in use; as of 2002, over one billion computers had been shipped around the world. Over 40 percent of the computers in use world-wide are found in the United States and 25 percent are in Europe. Nearly 20 percent of the world population has Internet access. There are over two billion cell phones in use worldwide: 600 million in China alone, and, given the convergence of technologies, these phones are effectively extending the widening range of internet coverage. Whereas ten or fifteen years ago computer technologies were seen as tools used by governments and institutions in wealthier, more developed countries, today they are increasingly seen as essential resources in countries around the world.

The increasing prevalence of information technologies is a challenge to good government and accountable record keeping precisely because computers are seen as so important to business and daily life. Information technologies are considered by many to be 'the solution' to information management problems, and often computer equipment is installed in organisations with little consideration for what tasks they will perform and how the products of those actions – the records – will be managed.

Unlike computers, paper-based record-keeping technology is so familiar it can be hard to notice. Everyone working in a typical office environment recognises the nature and purpose of paper, typewriters, carbon paper for creating duplicates, pre-printed forms, filing cabinets, ledgers for entering accounts, warehouses for storing volumes of paper records and mail rooms for sending and receiving paper-based records. The paper records environment is easily understood even by people who have not worked in offices before.

Part of the challenge of moving from paper to electronic record keeping, therefore, is to understand the fundamental differences between the two technologies. In an electronic records environment, the stability of the record is at much greater risk. The reality is that it is not as easy to preserve an electronic record, as one can preserve a paper record by placing it in an acid-free folder and keeping it in a secure and environmentally sound storage facility.

When composing a letter, for instance, the writer takes a piece of paper, which may be pre-printed letterhead, and types or writes the content directly on the paper. When the letter is stored, its contents – the words on the page – and the medium – the paper with the letterhead on it – remain wholly intact. The paper medium is integral to the transmission and storage of the record. Retrieval is simple: someone just pulls the document out of the file in which it is stored and its content is immediately accessible to the human eye.

As will be explained in this module, an electronic record can consist of many different elements: different bits of digital information that require different computer operations to make them 'work.' It is necessary to store the different elements that make up an electronic record according to the particular storage requirements for each element. Then, in order to retrieve the record, it is necessary to have the computer recall the different components and reassemble them, creating, in effect, a replica of the original record that is, or should be, essentially identical to the original though in fact it is not the 'same' item.

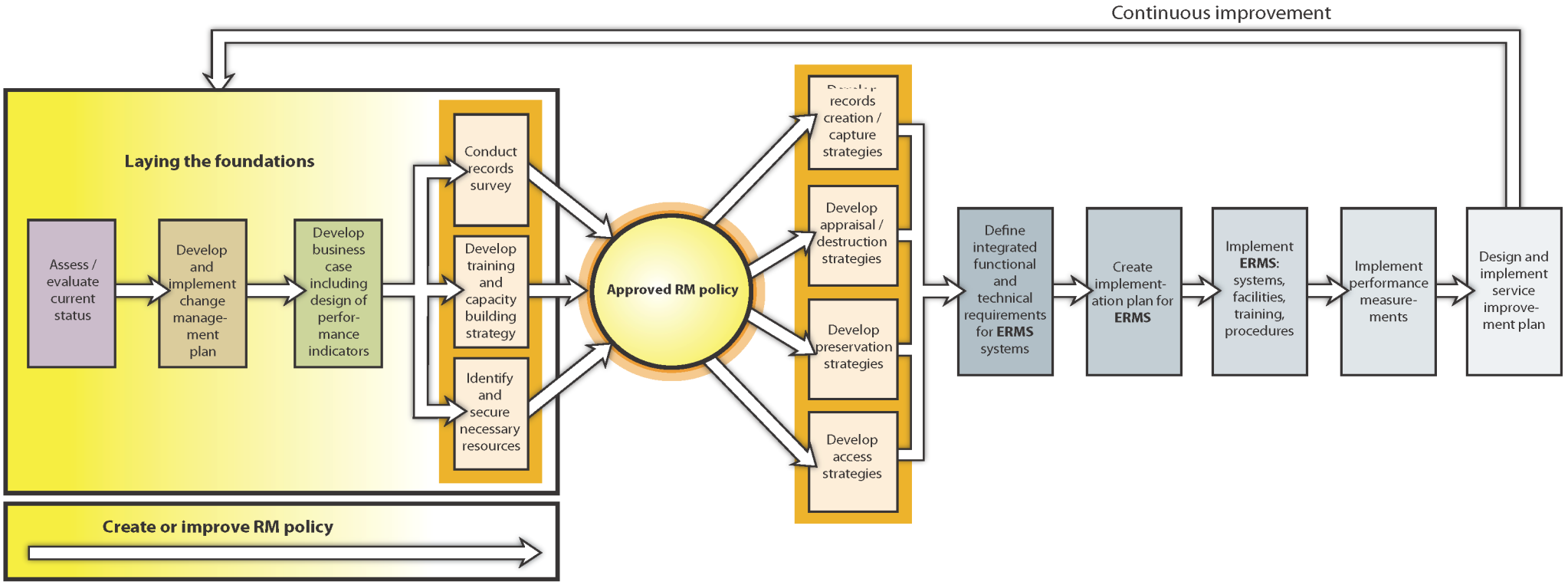
An electronic message similar to the paper letter discussed above may contain at least two elements: the name and address component in the computer – a digital 'letterhead' in effect; and the message itself. The two components come together when the message is saved or transmitted, but they are not saved in the same place in the computer. In order to reconstitute the message later, both elements need to be preserved and linked together.

Since paper is a reasonably durable medium, it can last a very long time. And little work is required to protect it: as long as it is kept dry and away from fire or water, the document will usually outlast its administrative and legal lifespan, and if properly preserved it can last for hundreds of years. The durability of paper led to the development of the life cycle concept, because it was possible to argue that records could be active and in regular use, then be kept in semi-active storage once they were no longer immediately valuable and then either destroyed as obsolete or kept as archival. This life cycle could take upwards of 30 to 50 years or more to evolve. Paper records could withstand the experience of being stored and essentially ignored until they were needed, no matter how long the wait.

Because an electronic record is made up of discrete bits of data, it cannot be accessed or used without some form of computer technology. There is no 'original record' as it is understood in a paper-based environment. The electronic record only exists when the different digital components are brought together in the way they were created in the first place. Therefore, the concept of the life cycle has a very different application in the digital environment. Applying the record life cycle concept in the digital environment requires that records professionals participate actively in the management of the record even before it is created, rather than waiting until it has been created, used and transferred to storage before making appraisal and retention decisions. The management of electronic records also requires the development of strategies and the implementation of technologies that will maintain the digital components so that they may be reassembled in order to replicate the original electronic record.

As a result of changing technologies, the focus of life cycle records management has shifted away from the management of the physical record itself to the creation of record-keeping strategies and processes for the life cycle management of records within an electronic information system. The route map which follows (Figure 1) illustrates this change in focus.

Figure 1: Route Map for Implementing Electronic Records Management[1]



[1] See Route Maps developed by International Records Management Trust © 2009

ABOUT THIS MODULE

In order to understand issues associated with the management of electronic records, this module introduces key concepts related to computers, information technology and information systems.

Unit 1.1 considers the opportunities and challenges brought by electronic information technologies. Among the benefits of computer technologies are: increased access to information, flexibility in the creation and use of information, improved efficiency and effectiveness, increased economic and business opportunities and improved capacity for audit and compliance. Among the drawbacks to electronic technologies are the dangers of technological obsolescence and dependence; the risks to reliability and authenticity in an electronic environment; the loss of security and privacy; increased costs as a result of the need to manage changing technologies; and the difficulties of accessing decentralised information sources.

Unit 1.2 examines the nature of computers and electronic records, examining the structure of a computer system, considering different types of information systems, defining electronic records, addressing the idea that electronic records can consist of many different elements, illustrating different formats for electronic records and describing the challenge of the multiplicity of electronic records.

Unit 1.3 looks at the technological framework for electronic records management. It explains the concept of information architecture and examines critical information technology infrastructures needed to ensure electronic records are created in a secure and sustainable environment, including adequate power supplies and networks, bandwidth and connectivity, technical support and backup systems.

Unit 1.4 examines the legal and organisational environment for electronic record keeping. Legal issues that must be considered include the protection of electronic records as evidence, the need for compliance with evidence laws, the challenges of meeting audit requirements, the importance of adequate budgets and the importance of identifying relevant legislation and policies. Organisational issues to consider include understanding organisational cultures and addressing the unique qualities within the organisation, particularly with regard to human resources, politics, policies and the physical and economic environment.

Unit 1.5 explains the importance of standards, particularly record-keeping standards, in the preservation of electronic records as authentic evidence. Specific standards examined relate to records management, digital preservation and archival description. Archival codes of ethics are also discussed, and key issues involved with applying standards are introduced.

Unit 1.6 looks at the nature of metadata and explains its importance as a mechanism for preserving the authenticity and integrity of electronic records through capturing critical information about their content, context and structure.

At the end of the module there is a series of study questions that readers may wish to review in order to help them reflect on the topics discussed throughout the text.

FOR ADDITIONAL INFORMATION

Readers are reminded to review the *Additional Resources* document for more information about publications, websites, associations and other resources relevant to the general topic of electronic records preservation. The *Glossary of Terms* includes definitions for key records management terminology. Readers wishing to study some of the fundamentals of records management as related to this specific topic may wish to review some of the MPSR training modules, available online at www.irmt.org.

Of particular relevance to the preservation of electronic records are the following MPSR products:

Training Modules

- The Management of Public Sector Records: Principles and Context
- Developing the Infrastructure for Records and Archives Services
- Managing Resources for Records and Archives Services
- Understanding Computer Systems: An Overview for Records and Archives Staff
- Automating Records Services
- Managing Electronic Records

Procedures Manuals

- Model Records and Archives Law
- Model Scheme of Service

Case Studies

- Chris Seifried, Canada, Management Decision Making and Teamwork Case Study
- Greg O'Shea, Australia, The Transition to Electronic Government – The Challenge for Records Management
- Terry Cook, Ed Dahl and Ann Pederson, Australia/Canada, Living with Your Conscience at the End of the Day: Ethical Issues and Archives/Records Managers
- Ann Pederson, Australia, Management Case Study: Revising the Record Keeping Programme for the Widget Manufacturing Company
- Ann Pederson, Australia, Advocacy/Marketing for Record Keeping: A Case Study
- Ann Pederson and Trudy Peterson, Australia/ USA, Archival Control: Case Studies
- Margot Thomas, St Lucia, Reinvigorating the National Archives of Verdant Isle

UNIT 1.1

THE OPPORTUNITIES AND CHALLENGES OF ELECTRONIC RECORDS

There are both benefits and drawbacks to the use of computer technologies to create and manage information and records. This unit examines both the opportunities and challenges presented by electronic technologies; the goal of the unit is to set the stage for a discussion of the nature of electronic records and the importance of understanding the issues involved with preserving and protecting quality information and records in a digital information environment.

Benefits of Electronic Technologies

There are many benefits associated with the use of new technologies in managing electronic records, including

- widespread access
- flexibility
- efficiency and effectiveness
- economic benefits
- general business opportunities
- auditing capabilities for regulatory compliance.

Widespread Access

Traditionally, records and archives have been created and maintained in paper form as physical objects. Their physical composition limits access to a specific time and place: only one person can use a record at one time and only in one physical location. Producing multiple copies is expensive and time consuming, requiring access to photocopiers or printers. Duplication also leads to confusion about which of many versions of a document is the official record.

Electronic records, on the other hand, can be shared widely and they can be accessed and used by several people at the same time, even if they are in different places. In environments where resources are scarce or distances are great, the ability to provide access to information without the boundaries of time or space can dramatically improve service, increase information sharing and enhance operations.

In some countries, for example, the ability to share an electronic record among government offices in different parts of the country saves money and time. Copying

and mailing or faxing documents across thousands of miles can become prohibitively expensive and can slow down operations and delay decisions and actions. But even in some less developed countries, governments today are installing computers in community outposts in rural, underdeveloped areas so that people in the area can keep abreast of government activities and world events. Even though there may only be a handful of computers available within large geographic areas, people still have greater access to information than before computer technologies were available.

Flexibility

Information technologies enhance flexibility in the creation, storage, use and management of information and records. In a paper environment, records are created, received and filed in one office, and they accumulate in one place. Electronic records can be stored remotely or on compact disks (CDs) or tapes, allowing people to share records and use their information resources more dynamically. Because so many people in an organisation can have access to electronically stored records at the same time, they can carry out their duties without being hindered by a lack of information. They also have better access to more up-to-date information, since they can access information technologies such as electronic records storage facilities or databases directly and not have to wait for materials to be filed in a central registry and then located and retrieved when needed.

Efficiency and Effectiveness

The use of information technologies improves information handling and allows for the speedy retrieval of records and information through electronic search facilities. As a result, policy makers can make informed decisions quickly and efficiently, contributing to the effectiveness of the organisation. Further, when the retrieval of records and information happens swiftly and decisions are made on time, the image of the organisation improves as it is seen to be reliable, capable and responsive to the needs of its clients or the public.

Certainly, if someone knows where records are stored, whether in paper or electronic form, he or she can retrieve them in good time, but too often knowledge about where manual records can be found maybe held by only one person in the organisation, and if he or she is not available then access to records is delayed. And once the volume of records reaches a certain point, no one person can ‘remember’ where everything is. Well-designed computer systems will facilitate easy retrieval of electronic information, improving the speed and quality of service.

Economic Benefits

In the paper environment where records are physical objects, their accumulation requires ever-increasing amounts of space, including office space, shelves, filing cabinets and storage boxes. Several staff members may be needed to carry out routine procedural work such as filing documents and retrieving boxes.

Through the use of new technologies, organisations are able to economise in terms of storage space, as computer systems can store large volumes of data and records in a small physical space. Database management systems, electronic mail systems, web

and multimedia software programs are all good examples of information technologies that can store far more information than traditional paper records storage systems. In a well-managed organisation, it is also possible to manage staff resources more effectively. Much of the day-to-day work of filing and retrieval will be done by officers throughout the organisation as part of their daily routine, leaving time for other staff to participate more actively in activities such as appraisal and retention.

General Business Opportunities

The professional image of an organisation can be enhanced by improved information flow, and the organisation may be able to take on more complex work because it is more efficient and cost-effective. Computers can improve communications, reduce the loss of essential information, speed up the completion of projects and increase public awareness of the organisation. The use of technologies also exposes organisations to communities outside of their normal client base, locally, regionally, nationally and internationally. For example, the creation of an institutional website can raise awareness and increase interest from clients or members of the public far removed from the physical location of the organisation's head office.

Auditing Capabilities

Well-designed records and document management systems also allow an organisation to regulate and oversee actions and decisions. Many electronic records management software programs include mechanisms to maintain audit trails, encouraging more accountable record keeping and promote compliance across the organisation. The development of information technologies also usually involves the development of records management legislation and regulations, which are designed to control the process of creating, maintaining and using records. As a result, public accountability and transparency are enhanced.

Challenges of Electronic Records Management

While information technologies have brought many benefits to organisations, they have also introduced a number of challenges and difficulties, including

- technological obsolescence
- technological dependence
- increased risk of lost data and records
- risks to reliability and authenticity
- loss of security and privacy
- increased costs
- decentralisation of information
- the increased need for information technology specialists.

Technological Obsolescence

Rapid changes in software applications and computer hardware have led to what is commonly referred to as technological obsolescence. As new innovations in computer

technology appear, old systems become out of date and are no longer supported by the computer industry. Some examples of this obsolescence include Commodore 64 and WANG computers – first introduced in the 1970s and 1980s – which are no longer made or supported at all. Consider also the fact that 8 inch, 5¼ inch and 3½ inch floppy disks are now rarely if ever used, even though they were the predominant storage devices for electronic records for decades.

Technological obsolescence is not just applicable to hardware. Many software programs that were once extremely popular are also now obsolete, including WordStar and early versions of Microsoft Word and Corel WordPerfect. Some of these changes in technology are a consequence of changing economics and markets, while others resulted from advances and changes in software and hardware.

The risk of technological obsolescence is further compounded by the harsh environmental conditions in which computer storage media are sometimes stored. Magnetic and optical media will deteriorate quickly when exposed to high temperatures, humidity and contaminants, often resulting in the partial or complete loss of electronic data.

Overcoming technological obsolescence often requires frequent and perhaps considerable investment in financial, human and technological resources. Conversely, a lack of committed resources will render any electronic records management strategy ineffective and unsustainable. If an organisation is going to commit to using information technologies, it needs to guarantee that it will provide the resources needed to maintain and upgrade those technologies indefinitely.

Technological Dependence

Electronic records depend on technology. They are created and managed by computer hardware and software. Therefore, electronic records require mediation in order to be accessed. It is not possible to hold a computer disk up to the light and read it, as one can read a paper document or even, with the aid of a magnifying glass, a frame of microfilm.

Because information technologies keep changing, and because electronic records cannot be used without the necessary technologies, individuals and organisations can quickly become dependent on technologies for their essential information. Hardware and software have to be upgraded regularly to ensure continuing access to information and records. As technology changes, records need to be moved to new systems – migrated – so that they can be used. Otherwise, the formats in which records exist are incompatible and the records are increasingly inaccessible. An electronic document cannot be placed on a shelf, like a bound ledger or folder of documents, with any guarantee that it will remain usable in ten, five or even one year into the future.

Risks to Reliability and Authenticity

As mentioned, changes in information and computer systems require that information be migrated to new technologies if the information is to remain accessible over time. This process of migration can affect the authenticity and reliability of information, as the process itself can change the content or structure of the records. Unlike paper

records, which can be moved, filed, refiled, copied and otherwise used and reused without change, electronic records need to be managed and preserved in such a way as to secure their authenticity as evidence.

Similarly, the way in which electronic records are created can limit their value as authentic records. For example, computerised electronic mail (email) systems do not always capture accurate information about the author of the original email message. Further, as email messages are forwarded, copied, replied to, they may be edited or altered, and the integrity of the original message may be lost as the email communication progresses. To establish the uniqueness and integrity of a record in such a system, one has to know which system was used, who sent the message, who received it, and when it was sent, received, replied to, forwarded or otherwise acted upon. The email software may not have the ability to capture all this information, which is essential to understanding the structure, content and context of record.

Loss of Security and Privacy

The introduction of information technologies has also affected the way government and private organisations preserve and make available records in their custody. As mentioned, computers allow organisations to create large and complex databases and make huge amounts of data available electronically. Databases containing personal financial and medical records, for instance, may be extremely useful to the individuals themselves. But without proper security protections, that information may also be accessed by others, threatening the privacy of the owners of that information. People have an inherent right to privacy that can be violated, intentionally or by accident, in an electronic environment.

For instance, the risk of identity theft is now very real in the electronic world. Some unscrupulous individuals and companies compile and sell personal information about people; this information has been gathered, usually illegally, from electronic sources such as credit databases, land title files, motor vehicle records or medical files. This information may be used to gain access to credit cards, bank accounts and even property title documents.

All governments and organisations using computers to manage personal information have an obligation to ensure that the data and records in their care are well protected from theft, damage or loss. All necessary measures, from the use of passwords in the office to the creation of appropriate legislation for the jurisdiction as a whole, have to be put into effect to ensure that the information is secure.

Security can pose its own problems, however. If, for example, only one person in the organisation knows the passwords or access codes to computer systems, what happens if that person is not in the office when information and records are needed urgently? Good security allows only those with permission to access certain records, but it also ensures that the right people have access to passwords and permission codes. Security measures also protect against the transfer of computer viruses or other malicious software. The goal is to ensure that the organisation's operations are not hindered by inadequate security, but also to avoid installing so much security that people cannot perform their required duties effectively.

Increased Costs

The costs of hardware and software can be very high. Costs are incurred not only when acquiring technology in the first place but also, more importantly, when upgrading equipment and systems, which is essential in order to keep pace with changing technologies. For organisations, or countries, with limited resources to tackle other problems, this ongoing cost poses a serious challenge.

When considering the acquisition of computer equipment or the implementation of an electronic records management system, most organisations focus on the initial budget requirements: hardware; software; licenses; supplies; and staff time to develop and install the equipment. But annual and unexpected costs also need to be considered, including: system maintenance fees; upgrades and repairs; and staff training. It has been argued that the cost of maintaining and administering computer systems can exceed seven times the cost of acquiring the equipment in the first place.

The organisation also has to consider the intangible costs of moving to a new working environment. Time and resources are required to comply with new regulations and legislation; to file, store, retrieve and access records; and to support office workers as they adjust to new technologies and methodologies. Because most organisations going through this transition are doing so by choice, these costs can be considered a part of the necessary learning curve involved with moving to the electronic working environment. There may be intangible savings as well, of course, including improved workflow, enhanced security and so on, that offset these costs.

Decentralisation of Information

The decentralisation of information and records management has shifted the responsibility for managing records from records professionals to the people who create and use records on a daily basis. Unfortunately, users are not trained to know what documentation to keep for evidential purposes or how to describe, file or maintain records. Without centralised oversight of the records management process, it can be more and more difficult to ensure that essential evidence has been protected adequately. Thus, even though the computer systems allow for widespread access to information, there is no guarantee that the information needed will be available or that it will be easily retrieved by anyone other than the individual who created and used it. Careful monitoring of the way in which electronic records are created and used is essential to developing an effective work environment.

The Reality of Electronic Records

The opportunities and challenges presented by electronic records will not change, but records professionals can take advantage of the opportunities and mitigate the risks by the effective implementation of electronic records management programmes and the creation of reasonable and clear policies and procedures for creating and managing records in all media.

Electronic technologies are a reality of life in the 21st century. They bring a range of benefits to governments, organisations and society, including improved communi-

cations, increased efficiency and greater accountability and transparency. Records professionals must not turn their back on the difficulties of implementing electronic records management programmes. Instead, they must use the opportunities presented by digital technologies to improve the framework for all records management.

It is important, however, to bear in mind the following points about electronic records:

- Electronic records are entirely dependent upon technology.
- Rapid changes in technology require continuous review and modification of electronic records management strategies.
- The challenges of technology, particularly relating to technological obsolescence and dependency, have complicated the long-term management of and access to information.
- Currently, no single strategy exists to address and 'solve' all electronic records management issues.
- Digital media are especially vulnerable to loss and destruction, making preservation both more difficult and more important.
- Generally the approach to electronic records management has been ad hoc or reactive.
- Records professionals need to approach electronic records management with a long-term vision and with an awareness of their responsibility to continue to upgrade their knowledge about electronic records and current technologies.

The next units in this module explain the nature of electronic records and examine the technological, legislative and organisational contexts in which electronic records management takes place.

UNIT 1.2

WHAT ARE ELECTRONIC RECORDS?

The nature of authentic and reliable records is that they are fixed in time and space: they cannot be altered in any way without creating a new record. The great danger to the protection of authentic records is the ease with which electronic records can be manipulated and changed. Paper records were 'finished' once they were typed or printed or written, but every time an electronic record is altered the old record can be lost and a new record created in its place. Thus it is critical to establish sound and effective mechanisms for creating and preserving quality electronic records: records that remain authentic and reliable evidence of actions and transactions, regardless of the technology used to create them.

This unit examines some key concepts, including the nature of computers and information systems, the nature of electronic information and electronic records, the difference between data and records, the different formats in which electronic records can be found, the fact that multiple copies of electronic records are common and the importance of distinguishing between electronic data and electronic records.

A Note on Terminology

As computer technologies have developed, information technology experts, computer programmers, records managers, archivists and others involved with information and records have developed different interpretations for terminology related to electronic technologies. For example, one of the most common miscommunications between information professionals and computer professionals arises from the different uses of the terms 'archiving' and 'archives.' From an archivist's and a records manager's perspective, these terms refer to the actions taken by an archives to preserve a document that needs to be kept permanently and to the institution that houses records with historical value.

On the other hand, computer programmers and information technology professionals – often including electronic management software vendors – use the terms 'archiving' and 'archives' to mean very different activities. To them, 'archiving' is the process of putting an electronic record into a computer storage environment, no matter whether the record will or should be kept for the long term. In their eyes, 'archives' are the digital repositories in which records are kept until they are no longer needed by the organisation; any permanent preservation of the record is not included in this interpretation of 'archives.'

It is also important to note that in the field of information management and data processing, a 'record' is defined as a grouping of inter-related data elements forming the basic unit of a computer file. This concept is entirely different from the record-keeping concept of an electronic record and the two should not be confused. The focus in this unit, and in this training programme, is on the record as evidence, not as a group of data elements making up a record.

This difference in the perception of the concept of records and archives has caused confusion and conflict in the past, but now both professions are working toward a common understanding of the terminologies used. Greater coordination is particularly important for effective electronic records management, since electronic records are technologically fragile and are subject to unique preservation challenges.

What Is a Computer?

A computer can be defined as

> any programmable machine or other device that can process information to produce a result.

Regardless of the size or complexity of computers, they all perform three basic steps. They accept input; they process the input according to specific rules (as defined by computer programs); and they produce output. These steps are detailed below.

- **The computer accepts input.** Computer input is whatever is entered or fed into a computer system. Input can be supplied by a person (such as by using a keyboard) or by another computer or device (such as a USB device or CD-ROM). Some examples of input include the words and symbols in a document, numbers for a calculation, instructions for completing a process, pictures, video and so on.
- **The computer processes the input,** manipulating the data in many ways. Examples of processing include performing calculations, sorting lists of words or numbers, modifying documents and pictures according to user instructions and drawing graphs.
- **The computer produces output.** Computer output is information that has been produced by a computer. Some examples of computer output include reports, documents, music, graphs, videos or pictures. Output can be in generated in different formats, such as paper, CD-ROM, DVD or on screen.

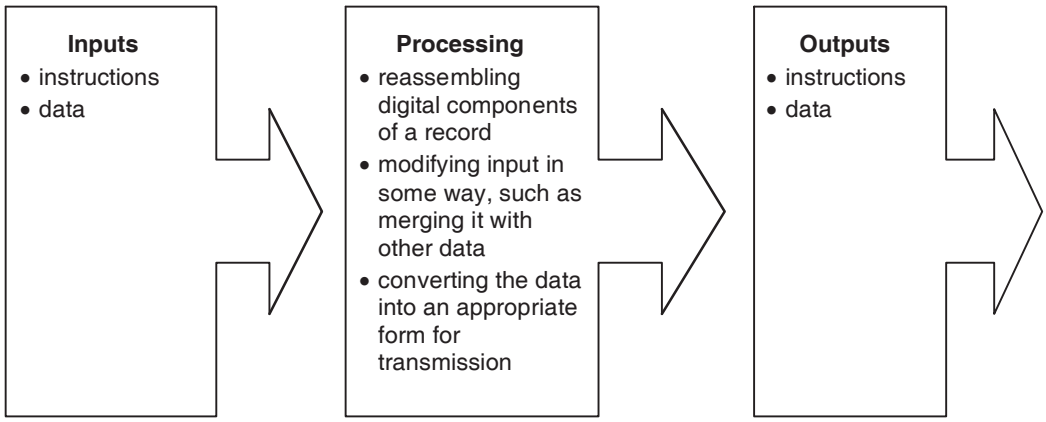
During each function the computer must store data. Most computers have more than one location for storing data (the hard drive or C:\, for instance, or a remote storage device such as magnetic tape). The place where the computer stores the data depends on how the data are being used.

What Is a Computer System?

The actions of input, process and output are referred to collectively as a 'system.' It is common, particularly in governments or organisations, to talk not about 'computers' but about 'computer systems,' 'information systems' or 'digital information systems.'

Information systems also involve people, who operate the technology, and the systems may generate records, activities, instructions or other products. A graphic representation of a simple system is shown in Figure 2 below.

Figure 2: Simple Representation of a System



Computer or digital information systems can be made up of hardware, software, data and network technologies. Computer systems usually consist of several different parts, as listed below:

- the application software, which is used to create and use data
- a management system, which controls the movement and location of the data and communicates between the application software and the central processing unit (CPU)
- the operating system, which manages the operations of the computer and software
- the CPU, which manages all the processes undertaken by the computer
- the physical disk storage, which holds the data entered into or created by the computer
- the computer and its component parts, including internal and external communication components (such as the monitor, and modem and so on)
- the people operating and using the computer system.

Without access to each of these parts of a computer, it is impossible to 'find' and use an electronic record or other electronic data.

Consider the difference with paper records. A paper record has only three layers: the paper itself (the carrier), the information on it (the data) and the viewer (the interpreter of the data). A person has to be physically in the presence of the paper record in order to use it, but he or she needs no other technology to access the information. When a person wants to read an electronic record, he or she might be in another city or another country and able to access the record using computer technology. But that record will not be readable to anyone, whether they are close by or far away, if the parts of the computer described above are not in place.

Figure 3 below, drawn from information provided in Keri E. Pearlson's *Managing and Using Information Systems,* sets out the four basic elements of any information system, identifying the elements itself, who works with it and where it exists. The four layers in the illustration should not be considered an exhaustive list, but these layers will appear (with the rare exception for networking) in most information systems.

Figure 3: Characteristics of an Information System[2]

Element	What It Is	Who Works with It	Where It Exists
Hardware	computers servers tape and disk drives routers, etc.	users managers	physical location
Software	programs and applications for • the business • managing the computers • communicating between systems	users managers	resides on the hardware
Data	bits of information stored in the system: literally the 1s and 0s	users managers owners	resides on • the hardware • removable media (tapes, disks)
Network	connections to other computers • cables • modems, etc.	users managers service providers	physical locations cables wireless transmitters

The four rows on the table also illustrate the layered nature of digital information systems: each layer can and should be considered independently of each other layer. For example, data can be changed without necessarily changing the hardware or software. Similarly, computer software can be upgraded without changing hardware, and the installation of new networks does not necessarily result in a change in the data.

It is true that several years ago, in the early years of the development of digital information systems, hardware, software and data were effectively inseparable: that is, programs were written for specific hardware and only the program that created a piece of data could access and use that data. Today, the layers are somewhat more independent of changes in the other layers. Of course, significant changes to any layer will frequently require some kind of remedial work in one or more of the other layers.

[2] For more information on these characteristics, see the description in Keri E. Pearlson, *Managing and Using Information Systems: A Strategic Approach* (Toronto: John Wiley & Sons, Inc., 2001), pp. 27-28.

Digital Security

An additional layer common in larger information systems is a security layer. With the development of software viruses and other malicious intrusions into computers, system security is now a significant issue when using information technology. System security is now normally an element in every information system and may range from simple log-on passwords to dedicated programs called firewalls that monitor and restrict inputs into and outputs from a system or to programs that scan for and disable viruses.

System security may also reside outside of any specific computer system. For example, a municipal government may operate several information systems, such as one for financial management and another for managing responses to emergencies. The government's first method of system security may be to establish a secure computer network and provide computer access only to municipal employees. In other words, it is building a firewall to prevent external computer systems from interacting with the municipality's own systems. Many people within the organisation may have access to the financial management system but no one outside of the government will be able to get into that computer system. The municipality may then implement more specific technologies, such as special hardware or software, to protect individual information systems more fully. Similarly, only a handful of people may have access to the emergency response system; most employees would not be given permission to access such sensitive operational areas.

Types of Information Systems

Information systems can be separated into several broad categories based on the business function they are put in place to support. Therefore, it is possible to identify information systems based on an analysis of the type of work they were designed to manage. Information management specialists Kenneth and Jane Laudon have identified six types of information systems, each of which operates at one of four levels in an organisation. These types and levels are set out in Figure 4 below.

Note that not all of the systems indicated in this illustration appear in every organisation. For example, it is unlikely that a group of people responsible for strategic planning will need to access or use a transaction processing system. Similarly, staff involved with tracking accounts receivables will rarely be involved in any work related to human resources planning. But the activities these systems represent are usually found at some point in any large-scale organisation, particularly in the public sector.

Consider these examples of information systems that exist in different organisations.

- An office that plans and executes road and bridge construction will have some kind of engineering work system.
- A store that sells merchandise will have an inventory system.
- A government with hundreds of employees will have a payroll system.
- A records centre that provides offsite storage will have a transaction system for processing requests for records.

- A company that invests funds will have a financial analysis system.
- An organisation that schedules events will have a calendaring/scheduling system.
- A factory will have an equipment scheduling and plant management system.
- A company that produces designs and illustrations will have a graphics management system.

Figure 4: Types of Information Systems[3]

Strategic Level	***Executive Support Systems***
	sales trend forecasting operating plans budget forecasting profit planning human resources planning
Management Level	***Management Information Systems***
	sales management inventory control annual budgeting capital investment analysis
	Decision Support Systems
	sales analysis production scheduling cost analysis pricing and profitability analysis
Operational Level	***Transaction Processing Systems***
	order tracking order processing machine control and plant scheduling material movement and supplies control securities trading cash management payroll accounts receivable accounts payable training and development human resources management
	Knowledge Work Systems
	engineering work stations graphics work stations
	Office Automation Systems
	word processing document imaging electronic calendars

[3] Illustration based on information provided in Kenneth C. Laudon and Jane P. Laudon, *Management Information Systems: Organization and Technology in the Networked Enterprise,* 6th ed. (Upper Saddle River: Prentice Hall, 2000), p. 39.

The Nature of Electronic Information

Electronic information is different from manual or paper-based information in a number of ways. Some important qualities of electronic data are the small 'size' of the data and information; the ease with which data can be replicated; and the consequent portability of electronic data, which can be moved and used in various locations in the same room or on the other side of the world.

In computer systems the 'size' of the data and information is extremely small. Therefore, tremendously large quantities of data and information can be managed in extremely small spaces relative to other forms of information, such as paper-based records. Whereas it might be necessary to rent a warehouse to store a large quantity of paper-based information, the equivalent amount of electronic information may fit into a computer server the size of a refrigerator. This small size makes the storage of electronic data seem relatively inexpensive and means it can be much easier to copy, manipulate and move information. Essentially, electronic data are more easily accessible by a greater number of users, which can be a good or a bad thing.

On the positive side, the ability to copy or move data means that people can use records and information from just about anywhere, if they have access to a computer. Further, the ability to copy data ensures that the records can be available in an emergency: a computer system can go up in flames but the records can be retrieved as long as another copy of the information is safely stored elsewhere.

On the negative side, this portability makes it easier for unauthorised people to access records, since more people, both inside or outside the organisation, may be able to gain entry to the computers and extract data. And the proliferation of copies means that people may be less concerned about protecting the 'original' information, since they may assume it is already protected somewhere else. And there are costs associated with managing electronic storage environments, particularly with addressing continuing technological changes, that add to the costs of electronic records management. Ironically, therefore, the very quality that makes electronic data and information most useful – portability – is the same quality that makes it most vulnerable.

A person working with electronic information does not need to be in the same physical location as the data to access, analyse or copy it. Through networked computing, users can view and manipulate data and information from anywhere in their office, or country or from overseas as long as they have appropriate access. Access can even be achieved illegally by 'hackers.' Accordingly, the actual location of the information becomes a secondary issue. What counts is whether the data are accessible and authentic, a critical concern for records, because of their importance as evidence. The next issue, therefore, is to understand the nature of electronic records and the difference between records and data in a computerised environment.

What Are Electronic Records?

Records can be defined as

> documents, regardless of form or medium, created or received, maintained and used by an agency, organisation (public or private) or individual in pursuance of legal obligations or in the transaction of business, of which they themselves form a part or provide evidence.

Traditionally, records have been identified as physical objects: paper-based documents, maps, photographs and so on. These records were captured on a medium (usually paper) by means of symbols (letters, numbers, figures and so on) that people could access, or read, directly. Users of the records did not need any technology – such as a computer – to make use of the information in the record.

The Attributes of Records

Records have three important attributes: content, context and structure.

- *Content* is what the record says.
- *Structure* relates to both the appearance and arrangement of the content (for example, the layout, fonts, page and paragraph breaks, tables, graphs, charts and so on) and the physical or, more appropriately, logical relationship of the record to other related records in the system (for example, where a document is found in a file folder or in a bound journal).
- *Context* is the background information that helps explain the meaning of the document. One piece of information identifies the particular document, such as the title, author and date of creation. Another piece of information identifies the creator and the purpose of creation, such as the nature of the business function or activity or the creating agency and unit concerned.

The Nature of Electronic Records

Unlike a physical record, an electronic record can be manipulated, transmitted or processed by a computer. An electronic record is

> a record that is created, generated, sent, communicated, received, or stored by electronic means and that requires some form of computer technology to access and use.

An electronic record is

- written on magnetic or optical medium, such as magnetic tapes, CD-ROMs, DVDs, hard disks, USBs (universal serial buses) and other digital storage devices
- recorded in binary code
- accessed using computer software and hardware
- easily manipulated, updated, deleted and altered.

Essentially electronic information is made up of zeros and ones to form a byte. Most often one byte consists of eight bits or a combination totalling eight zeros and ones that represents a character. For instance, a capital ‘H’ is represented in binary code as

01001000. A lower case ‘h’ is represented as 01101000. Multiple bytes are formed to create a word or an image.

The word ‘computer,’ for example, is made up of the following codes:

c = 01100011

o = 01101111

m = 01101101

p = 01110000

u = 01110101

t = 01110100

e = 01100101

r = 01110010

An electronic record is made up of the bits (digital representation) and an observable or perceptible product generated from the bits. The product, which may be visible, such as a text document, or audible, such as a sound recording, is created instantaneously as the person inputs data or instructions into the computer, using a keyboard or other device.

In order to ‘create’ an electronic record, neither the perceptible product nor the digital representation can be separated. In other words, in order to generate that observable product again at any time in the future, it is necessary to preserve the digital representation – the bits – in a stable and secure form. Preserving an electronic record, therefore, is not a matter of preserving a ‘record’ – as is the case when preserving a letter or a black and white photograph. Rather, preserving an electronic record involves preserving the ability to recreate that observable product again and again, so that the record continues to fulfil the purpose for which it was created.

The software used to create a record is not itself a record – it is simply a tool – but nevertheless access to the software might be critical to being able to open and use that record. Thus managing electronic records also involves managing, or replicating, the software used in the first place, or eliminating the need for that software by saving the record in some other form.

Formats for Electronic Records

Electronic records are recorded on a medium such as a magnetic tape or a disk, but their status as records is not dependent upon that medium: the medium is not the record. Electronic records must be viewed as logical rather than physical entities because they cannot be read directly without the aid of computer software and hardware to interpret the codes used to represent letters, numbers, figures or other information.

Electronic records can be created in a range of different formats. One common form of electronic record consists of data sets contained in databases (sometimes referred to

as data files). Other common types of electronic records are text-based records such as word processed documents or spreadsheets containing text and numbers and allowing for automatic calculations.

Broadly speaking, electronic record format types include the following.

- *Data sets:* groups of related electronic records organised and treated as a unit. Data sets are created, managed and used in the context of a database. For example, a data set could contain information about employees in an organisation.
- *Text-based documents:* documents that contain little other than words, and that can be read by text editors or word processing software programs. For instance, a spreadsheet from Microsoft Excel could be imported into a memo being created using Microsoft Word, or a snapshot of a web page or a slide created using Microsoft PowerPoint could be included in a report created using a publishing software.
- *Multi-dimensional documents:* records that can be represented in more than one way on the screen and on the printed page. For instance, a spreadsheet can be represented as a set of figures or as the result of the calculations. Both representations are part of the record, although it may not always be necessary to retain both of them. Similarly, a PowerPoint presentation may consist of a set of slides and notes displayed and used in different ways.
- *Multi-media documents:* documents composed of a number of different elements, which interact together to display their full meaning. These records may include graphical, moving image, sound and text documents, which may appear differently at different times in response to variations in user interaction.

File formats can often be identified by file extensions. For example, .doc indicates a word processed document, and .mp3 indicates an audio file. Internet media might include text or .html files, and other file formats include PDF, TIFF and JPEG. Each file format will have different characteristics and require different approaches to preservation, and so understanding the different file formats in use is important to managing the content, context and structure of the records.

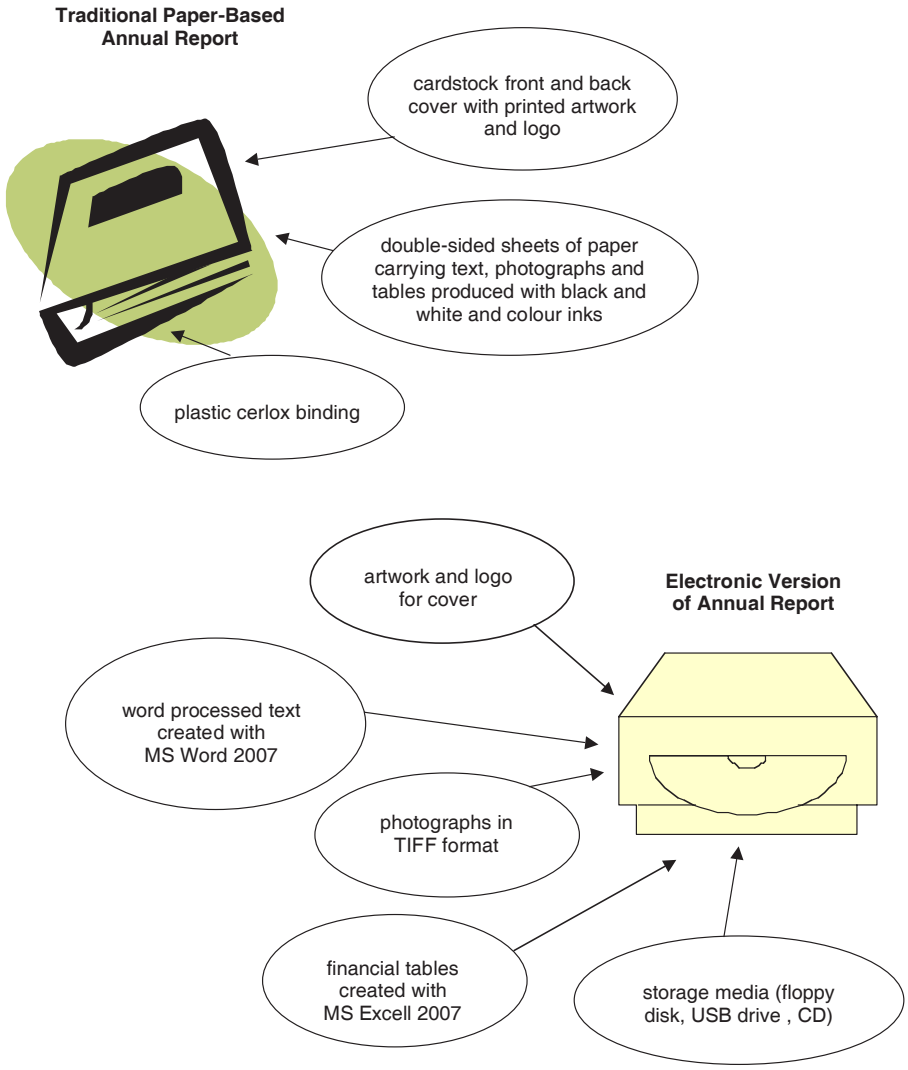
Components of Electronic Records

One electronic document may be composed of separate parts – often called digital components – that can be stored in different parts of a network, brought together as a 'virtual' document and presented in different forms for different uses. For instance, note and voice annotations can be added to text-based documents; and digital sound, video, 3-D modelling and simulation can be added to presentations, reports or other documents. An electronic record component, also called an element, can be defined as any component of information created electronically that forms part of an electronic record and that is usually stored separately within the digital file making up the electronic record as a whole.

Every electronic record consists of at least one digital component or element, such as the bits of data that come together to create a word processed document. But some electronic records contain many different elements. For instance, an electronically generated report may include an image of a web page, as well as a photograph, a PowerPoint slide, a spreadsheet page, an extract from a database and even a clip of a video or sound recording. And the web page or video clip may contain different computer elements that are needed in order to make that image visible or allow the video clip to be played.

Each component in a complex electronic record may have different requirements for storage, reproduction and use, which is why it is critical when preserving an electronic record to ensure that mechanisms are in place to allow for preservation of and access to every element within the record. Figure 5 introduces the idea of the simplicity of a traditional paper-based record compared with the complex nature of an electronic record.

Figure 5: The Different Parts of Paper and Electronic Records



The Multiplicity of Electronic Records

Another important factor to bear in mind when considering how to manage and preserve electronic records is the fact that it is much easier to create many copies of an electronic record than it is to create copies of a paper record. In fact, computerisation can cause people to accumulate more records than the original records creator ever intended. Consider the example of electronic mail.

An electronic mail message is 'created' when a person types input – words and instructions – into a software program such as Microsoft Outlook or Lotus Notes. The input is processed when the person clicks the 'send' button on the computer: the computer reads the instructions about who the message is going to and what text the message will contain. The output – the message in the sender's computer that includes information about who created it, when it was sent and to whom – is an electronic record.

The person receiving the message receives input. This input provides instructions to his or her own computer about how to process that message: specifically, to file it in the computer's email 'in box.' When the person opens the message, he or she provides new input that leads to a new computer process: opening the message. The output of that series of events is the image of the message on the computer screen. The message in the recipient's computer is also a record.

As a result, at least two records have been created: the message in the sender's computer, and the message in the recipient's computer. Which should be kept? For how long?

It is important also to recognise that the act of processing is not a record, but it can generate a record. For example, when an electronic message is filed into the computer system, the input will be the message itself, but it may also be instructions telling the computer to record who in the office filed the document and to keep track of whether and when the message is answered. The computer then processes the message and the tracking instructions. The output may be confirmation that the message was filed.

Later, a manager may want to know if the message in question has been answered. He or she could 'ask' the computer for information about the message. When he or she inputs a request into the computer, the output is tracking information about that message. Now the original message is not the only record being created and used. Other records include instructions about tracking and the results of the tracking request. The original email record is now joined by another three, four or five electronic records, including copies of the original email and associated documentation about what happened to that email over time.

The challenge for records managers and organisations is how to determine what evidence to keep and for how long, and how to ensure that documentation is kept securely. Because so much data can be generated within digital systems, it is incumbent on the organisation to determine which of the many inputs and outputs flowing through computer systems should be considered the official records of the organisation. Only then can appropriate resources be directed to maintaining those important records and not wasted preserving information that has no long-term value.

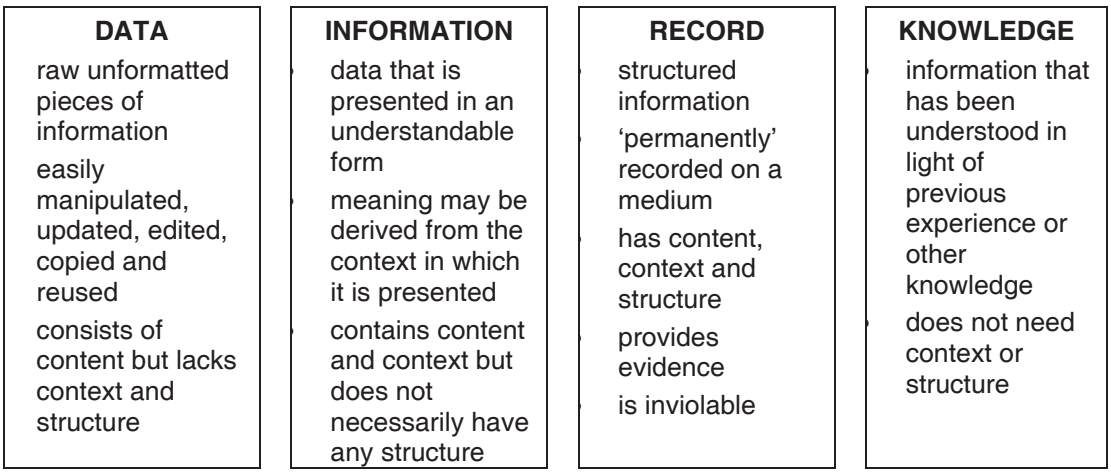
The information provided in these modules, along with a strong understanding of basic records management principles, will help records professionals identify those electronic products that can be considered evidence of actions and transactions; those are the products that should be preserved as records.

Electronic Records as Evidence

It is important, therefore, to emphasise that electronic records and information are not the same thing, and data and information are not the same either. There is an evolution from data to information, from information to records and from records to knowledge, as shown in Figure 6 below.

Data comprise raw unformatted information and can be easily updated, edited, copied and reused. A list of numbers is data. **Information** is data that carries some meaning to the user. A list of numbers with names beside them could be a statement about how much income employees in the organisation received each month. A list of numbers and names could become a **record** if it is used as the evidence for issuing cheques to staff: it might confirm who got paid and how much they received. That record can be used to gain **knowledge** if senior managers review it to determine how much their annual payroll costs are and whether they need to consider reviewing their staffing structure as a result of cost overruns.

Figure 6: Data, Information and Records



Whereas records derive meaning from their context and structure as well as their content, data lack context and structure and therefore are meaningless on their own. In an archival context, the authenticity of a record is paramount to its acceptance as evidence, so that it is not simply considered information or data. The authenticity of an electronic record derives from three essential characteristics: reliability, integrity and usability.

Reliability

To be reliable, a record must be a full and accurate representation of the business activity to which it attests. This requires the establishment of trust in the record

keeping and archival processes used to manage the record throughout its life cycle, and the continued ability to place the record within its operational context so that its reason for being, and the way in which it was created and used, are both easily evident. Reliability is ensured through the operation of transparent and fully documented preservation strategies and the provision of the metadata describing the content, context and structure of the record.

The importance of metadata is discussed in detail in Unit 1.6.

Integrity

The record must be maintained to ensure that it is complete, and it must be protected against unauthorised or accidental alteration. Integrity is the quality of confirming that the record has not been altered and that all authorised actions undertaken with the record – such as opening it electronically, reading it and filing it – have been managed and documented in accordance with established business requirements.

Usability

The record must remain usable: authorised users must be able to access it across time and in changing technical environments. To achieve usability, the record must be locatable and retrievable by users and the technology needed to open, read and understand the record must be available.

An electronic record can be considered authentic if it retains all the significant properties upon which its authenticity depends, including reliability, integrity and usability, and if the actions taken to preserve the record over time can be demonstrated.

In order to determine how best to manage electronic records so that they are reliable, authentic and usable, records professionals next need to understand some important technological issues associated with the creation and management of digital information. The technological framework for electronic records management is the subject of the next unit.

UNIT 1.3

THE TECHNOLOGICAL FRAMEWORK FOR ELECTRONIC RECORDS MANAGEMENT

At the simplest level a computer such as a laptop needs power (either from a battery or a central electricity supply); software to enable the computer to operate and to be used for different purposes; and occasional maintenance or upgrading by a person with sufficient knowledge and skill. At a more complex level a computer network in an office building needs much more support, including: a continuous power supply from a combination of primary and backup electricity sources; a temperature-controlled and clean physical environment; and technical support from people with a range of technical knowledge and skills to manage the hardware, software, networks and databases.

An information system is put in place specifically to perform or to assist in the performance of a certain business activity or function and capture and manage information resulting from that activity or function. The success of that information system depends not just on inputs and outputs but also on the technological framework in which the system operates. In other words, it is necessary not just to consider what a computer can do but why it has been installed in the first place, and what conditions are necessary in order to allow it to perform its functions appropriately.

Thus, in addition to considering the business functions served by the computer, it is important for the records professional not only to understand some of the fundamentals of how computers work but also to consider the technological framework in which information systems operate. Are power supplies adequate? Is there sufficient bandwidth to transmit data efficiently? Is there adequate technical support for computer systems?

This unit examines the concept of information architecture and then looks at critical information technology infrastructures needed to support quality electronic records management, including adequate power supplies and networks, bandwidth and connectivity, technical support and backup systems.

The Importance of Understanding Information Architectures

Information architecture is defined as

> the structural design of shared information environments, including both manual and electronically generated information.

Information architecture involves analysing, designing and coordinating the various elements that make up an information system, including: hardware, software, data, networks, business processes, staff and resources. An organisation's information architecture should be managed as a corporate or enterprise-wide activity, based on requirements and strategies suitable for the entire corporation.

For example, a government administration may want to centralise the management of revenues and expenditures, so that it can maintain control over finances. Modern information and communication technologies, such as computers, telephone lines and Internet cables, make it much easier to decentralise such specific jobs as receiving payments, processing credit cards, collecting taxes and so on. In order to ensure that these jobs are executed as part of a centralised government approach, the administration needs to plan its operations as part of a strategic goal or business requirement for the whole organisation and not let each department or agency establish its own practices without central coordination.

Centralised planning will involve developing policies and procedures, implementing appropriate business processes, acquiring suitable technologies and establishing a sufficiently robust technological infrastructure, including ensuring there is adequate electricity and installing appropriate telecommunications equipment. This centralised planning can be referred to as managing the government's information architecture, in this case in the area of financial management.

Historically, many organisations have not recognised the relationship between effective records management and the management of technology and information architecture. However, as access to records – or the absence of them – becomes more and more important, senior executives are increasingly aware of the need to ensure quality information and records are available by those who need them, when they need them. As organisations depend more and more on digital information, they are taking action to counter the negative effects of inadequate information technologies and unsuitable electronic record-keeping practices.

Imagine, for example, that a national government has installed an email system to allow employees to communicate with each other and with citizens and the public. When the email system was first deployed, the original business requirement may have been simply to save time by installing a technology that allowed for virtually instant communications. As the use of email grew, however, the volume of email, and the danger of losing valuable information, increased. The business requirement changed from communications to coordination and protection. The government needed not just to send and receive messages but also to ensure that a unified communications system was in place for the whole government and that critical records were protected by virus protection and security features.

As email continued to grow in popularity, government officials acquired new technologies, such as wireless and other portable communications devices. The government soon realised that a growing number of decisions being made by government officials – decisions for which the government can be accountable – were being communicated only via electronic mail. Often, no paper record existed of key decisions; the only evidence was the email messages, which may have been stored in desktop computers, in laptop computers, in wireless personal digital assistant devices or in different backup systems throughout the government. The government's business requirement changed again, as it sought to improve storage capacity for electronic mail and to implement or improve its records management practices so that email could be categorised, classified and filed according to government rules in a consistent and accountable fashion.

In some organisations, it might have taken upwards of ten years to move from the installation of the first email software system to the realisation of the need for a coordinated approach to electronic records management. Unfortunately, in those years, no one knows how many important records might have been lost or damaged through inadequate management. The records manager may not have been invited to participate in decision making about electronic mail until the systems had been in place for years, since senior managers might not have recognised the close relationship between information technologies and records.

In order to play a more central part in managing the products of information technologies, the records professional needs to 'stay on top' of current technological issues as they affect records and information. This means that the records manager needs to understand, at a strategic level, what the organisation's business requirements are and how the existing information infrastructure meets, or fails to meet, those requirements. The records professional can make a critical contribution to the effective management of records and information by also staying abreast of technological change and understanding the impact of new technologies on information management in general as well as the specific information architecture environment of the organisation itself.

Critical Information Technology Infrastructures

Electronic information systems and information technology (IT) networks are only as good as the technical infrastructure supporting them. And the technical infrastructure is only as good as the management support for it. An organisation may purchase a sophisticated computerised data backup system, for example, but if it does not also implement procedures for ensuring the right records are backed up properly and regularly, the money spent on the system is as good as wasted.

Information technology infrastructures can be defined as coordinated technical frameworks that support the use of computers throughout an organisation. These infrastructures are most often distributed physically throughout an organisation, with computers, telecommunications systems, printers, scanners and other devices connected so that they operate in a systematic fashion throughout the agency.

Planning successful electronic records management programmes and ensuring a robust information architecture environment involves understanding the nature of, and strengths and weaknesses of, IT infrastructures. Success also depends on establishing strategies and procedures to ensure information and records are protected in the event of IT damage or failure. Critical to all IT systems and networks are adequate power supplies, robust networks, sufficient bandwidth, suitable technical support and effective computer backup systems.

Power Supplies and Networks

Adequate and consistent supplies of electricity are essential for the successful operation of IT systems. Without power, it is impossible to access anything within an electronic system. While it is often beyond the ability of any single organisation to improve the quality or consistency of power supplies in the region, that organisation still can and should be prepared to protect its own systems in the event of power failures or interruptions.

The most effective first step in protecting information technology systems is to install what is called an uninterrupted power supply or UPS system. UPS systems, also called continuous power supply (CPS) systems, battery backups or emergency power systems, supplies power when central electricity supplies are not working. The length of time the UPS system can operate depends on the size of the system and the strength of the energy source, which might be battery powered or run by a gas- or diesel-powered generator.

Another protective action is to install surge protectors at different levels in the information technology system, from individual personal computers to computer routers and servers. A surge protector is a tool designed to protect electrical equipment from unexpected changes in the voltage (level of energy) being supplied to the equipment. A surge protector detects when too much electricity is being sent into the equipment and blocks the 'surge' so that the equipment is not damaged.

In order to ensure that computers are not damaged or information lost when power is cut, another important action is to develop procedures to 'power down' and turn computer systems off and on again in a controlled fashion. It is also important to ensure that there is no one 'single point of failure': no one place in the information technology system that, if it malfunctions, can put the entire network out of commission. In essence, any computer system should be designed to ensure there are at least two ways that data can flow to and from computers throughout the network. That way, if one connection fails, a second link can be activated immediately. This 'fail over' capacity is usually automatic and built into the network communication devices (switches and routers) and servers.

While records professionals are not expected to be technology experts, they have an important role to play in planning and designing information technology networks. IT specialists will be responsible for determining computer capacity; wiring; bandwidth; the placement of switches and routers; and peak loads. Records managers need to work closely with IT specialists to advise them on the information and records needs that will determine the way in which computer systems are configured. Who needs

what information when? How much information is generated throughout the organisation? How many people need access to electronic mail technologies? Which computer systems create valuable records and information that must be protected?

Bandwidth

Bandwidth is the capacity of the wire ('pipe') or wireless connection in a computer network to carry information. Bandwidth is usually expressed in kilobytes or megabytes per second. A dial up modem usually transmits data at 56 kilobytes per second (kbs), whereas a more powerful Ethernet cable transmits data at 10 megabytes per second (MBS). Clearly, the Ethernet cable is dramatically faster than the dial up modem. The difference is like comparing a two-lane road with a four-lane highway; the latter can move traffic much faster than the former.

Generally, the people who use computers do not think about bandwidth as such. Instead, they focus on the response time of their computers. But the length of time it takes to complete a task, such as downloading a document from a central server or accessing information from the Internet, will depend on the bandwidth available in the information system. The more bandwidth, the quicker the process.

The time needed to access digital information also depends on what is being accessed, however. Accessing a text document requires less bandwidth than accessing a photograph or a video. Of particular importance to records professionals is the fact that electronic record-keeping systems, which are discussed in later modules in this training programme, can be difficult to use in environments with low bandwidth. The software is so complex that it runs best on larger, more sophisticated computer systems that have been equipped with powerful networks and adequate bandwidth.

The records professional can play an important part in ensuring electronic information systems operate effectively by working with IT professionals to estimate user needs and thus determine the possible demands for bandwidth throughout the organisation.

Technical Support

'Technical support' is one of the most-used phrases in IT management. Unfortunately, despite the popularity of the expression, the concept is not well understood. Every software application and every piece of hardware acquired by an organisation should come with a technical support component. For example, whenever commercial software is purchased, a licence fee is paid allowing the purchaser to use the software legitimately. This licence fee then entitles the user to a level of service and support from the company that created the software. The software usually comes with a time-limited warranty: a guarantee that the company will address any errors or faults in the software for a certain period, such as one, two or five years.

Depending on the level of support and maintenance provided, the purchaser of that software is able to access certain services, like 'help desk' support to get answers to questions immediately. The purchaser can also access various updates and 'fixes' in the event that changes have been made to or problems occur with the software. Warranties on hardware operate in generally the same fashion: the purchaser has the right, for a certain amount of time, to ask the manufacturer for help if something goes wrong.

Technical support is like insurance. The service may never be needed, but without it the organisation can place its information systems at high risk. In the event of a problem, someone qualified and knowledgeable needs to be brought in quickly or the business of the organisation will grind to a halt, and its records and information will be in danger.

In the ideal world, all organisations will not only have purchased equipment, software and technology with adequate licences and warranties, but they will also ensure they have access to qualified computer network engineers, either onsite or within easy reach, to provide overall network support on an ongoing basis. However, easy access to such technical experts is often a luxury. Therefore, the organisation needs to assess and plan its information architecture needs so that its operations remain sustainable even if something happens to its computer systems. A formal plan for technical support should be developed, in order to outline who is responsible for what tasks and the steps the organisation should take to address system problems.

Backup Systems

Information and communications technologies can fail, whether because the storage device 'crashes' or because the computer becomes 'infected' with a computer virus or other malicious code. Such failures can result in lost or corrupted data. People can also accidentally delete files from their computers, or auditors can ask to see records that are no longer in current use. To protect valuable data, special backup applications are usually run, ideally every day, to allow an organisation to re-establish a system to its last known 'good' configuration and providing access to copies of records that may not be available otherwise.

Backups are usually copies of data stored on low-cost storage media, such as magnetic tapes. Magnetic tape technology has a long and reliable history, at least in computer terms. However, just as with any other recorded medium, tape is prone to deterioration over time. And if the storage conditions in which the tapes are kept are substandard, that speed of deterioration may increase.

Even before the medium deteriorates, however, the actual hardware used – the tape drive – that reads the data on the tape may become obsolete. Technological change happens very quickly and can render older equipment effectively unusable. In an electronic environment, the concept of 'old' might apply to equipment that is only one or two years of age. Some manufacturers support a certain amount of 'backward compatibility' – where a newer computer product can operate with data or software programs designed for use with an older computer product. Still, an organisation's data are at risk if the information is not copied forward onto newer media as soon as possible after any technological change, so if backups are made onto, say, magnetic tape, the organisation needs either to keep that tape drive operational or move the backup data to newer tape technology when new equipment is acquired.

The challenge to accessing data in backup files is compounded because the software used to create the records in the first place may also have changed over time. The magnetic tape drives may still be usable, but without access to the original software programs the records may be inaccessible. This problem is particularly pronounced

with commercial, proprietary software: software owned and controlled by a specific company. Companies may not support older software systems after a short while, in an effort to remain competitive and encourage users to upgrade to new software. Further, the computer business is driven by economics, and buyouts and mergers of different companies are common. One computer company that has purchased the products from another company may choose not to support the other company's software or systems for very long, leaving users of that software forced to upgrade to a new system in order to maintain access to their records.

The Hazards of General Backups

Often, backups are done on a general or wholesale basis: all data in a computer system are copied all at once. General backups are usually run to copy all data as fast as possible. Copying all data does not just mean records needed to run a business, but all the files and structure to operate or re-establish the whole system. While the backup process certainly copies records, it does not do so in a way that is relevant to the record-keeping needs of the business unit. Even though records have been copied, they may be difficult or impossible to recover.

For example, it may be necessary to restore the entire system that has been backed up in order to recover a single data file, because of the way the backup process was configured. A wholesale backup is similar to taking every paper document in an organisation out of file folders and throwing them all into a big box, with no labels or other identifying information. If an organisation were audited or asked to provide evidence in a court of law, someone would have to sit down and open every file in the box to find out if it contained the information or evidence required. To find every relevant electronic record, someone would have to search through every part of every data tape.

Even then, the technology available may not allow the organisation to retrieve the electronic record in its original form, rendering it inadmissible as evidence. Frequently IT sections do not test their backups to ensure successful recovery, either because they do not have the staff to do so or their systems do not have the capacity to do so without interfering with the daily operations that the technology supports. It may turn out that date and time information on electronic mail messages has been lost, for instance, or it may be impossible to prove that a word processed letter has not been changed between the time it was created and the time it was presented to an auditor or lawyer. And the time and cost involved in searching through all electronic data storage devices is so great that many organisations simply cannot comply with requests.

As a result, organisations end up paying fines, losing court cases or otherwise being punished for their inability to fulfil their obligations for information disclosure. They are not suffering from a lack of computer technology but rather from the absence of an effective electronic records management infrastructure to guide the management of information created using that computer technology.

As well as making it difficult to find specific records, a wholesale backup process can make it difficult to find every copy of those specific records. An organisation-wide

backup results in an enormous amount of data duplication. For instance, many people in the organisation may have their own copies of monthly staff meeting minutes and agendas, and everyone is storing their own electronic copy on their own computer hard drive or other storage device. Whenever a wholesale backup is done, every copy of those minutes and agendas is captured, meaning there could be five, ten or one hundred copies of the documents on the backup tape.

From the perspective of computer systems management, this duplication is desirable, because it reduces the chance that all data are lost. From a record-keeping perspective, however, duplication means that digital information that is supposed to be destroyed may actually still exist on backup media. If the organisation is required to destroy certain records after a set time – to protect privacy or confidentiality for instance – the existence of those records on backup media means the organisation is in breach of its legal or regulatory obligations. In order to ensure that records that *must* be destroyed *are* destroyed, records managers must establish formal policies and procedures for backing up and storing electronic records.

In the end, the process of backing up data does not guarantee it can be recovered. If backup systems are not tested regularly, software or hardware problems may not be discovered and records may not be retrievable when the time comes. It is important to test the procedures for restoring data from backup media regularly, in order to decrease the chance of loss or damage.

Establishing a Formal Backup Routine

Rather than rely on a general backup process that copies all data and all associated software programs, it is more effective to establish a formal backup routine that targets the most important records and data created by the organisation. A typical backup routine for a networked, client-server environment, which focuses on backing up formally identified resources, usually follows these steps.

- During a designated period every business day, the backup application is scheduled to run.
- This backup will either copy all the data in the targeted system (a complete backup), or it will copy only those files which have been modified since the last backup was run (a partial backup).
- These backups are called daily backups, and the tapes or other media used for these backups are reused regularly according to an established schedule: each tape, for instance, may be reused seven days after its previous use.
- A complete backup will be scheduled for once a week; this backup will be saved for a set period.
- Another complete backup may be prepared at the end of each month, and another complete backup at the end of each year.
- Usually the annual backups are retained indefinitely. However, the length of time that daily, weekly and monthly backups are kept can vary dramatically, from a few days to months or years.

As can be seen, the assortment of backups made, and the variations in the length of time they are kept, means that an organisation could have multiple copies of an electronic document somewhere among its dozens of backup tapes. Managing all those copies, making them available when needed, and ensuring unwanted records have been destroyed, completely and finally, makes electronic records management extremely complex and yet critically important.

The procedures established to manage the record-keeping and technological environment in an organisation will be more or less sophisticated, depending on the organisation's purpose, functions and structure. Therefore in order to understand the overall context of electronic records management, the next issues for the records professional to consider are the legal and organisational environments for electronic records management. Those topics are addressed in the next unit.

UNIT 1.4

LEGAL AND ORGANISATIONAL ENVIRONMENTS

Understanding the technological context of electronic records management is important, but it is equally important to appreciate the business context in which records are created and used. Only by comprehending how the organisation operates, and why, can the records professional develop a strategic approach to managing the organisation's electronic information resources.

Every organisation is subject to laws and policies, which govern the way the agency transacts business. These laws and policies also affect how electronic records are created, captured and managed. As well, organisations have their own 'culture' or way of operating, which influences the decisions they make and the actions they take.

Understanding the legal and organisational environments in which records are created and used is essential to establishing a successful and effective records management programme. Even if the existing laws or policies in a jurisdiction do not yet address electronic technologies, the records professional should still understand, and work to create, the legal and organisational infrastructure required for quality electronic records care.

This unit examines the legal environment for electronic record keeping, considering legal issues such as the protection of electronic records as evidence, the need for compliance with evidence laws, the challenges of meeting audit requirements, the importance of adequate budgets and the importance of identifying records-related legislation and policies. The unit also looks at organisational issues, including the importance of understanding organisational cultures and addressing the unique qualities within any organisation, particularly with regard to human resources, politics, policies, the physical environment and economics.

Records and the Law

Every country makes laws (usually through a parliamentary process), implements laws (through a government bureaucracy) and enforces laws (through a judicial and law enforcement system). The exact nature of any legal system will vary from country to country. Ideally, the judicial arm of the system will be independent from the governmental and bureaucratic arm to allow for decision making without political interference.

There can be different layers of government – national, provincial, state, municipal, regional and local. The nature and scope of the laws created, implemented and enforced in a country or in the different regions will vary depending on the political and administrative structure of that country or region.

Laws have a direct impact on the ways in which governments, organisations and individuals carry out their daily affairs. As well, laws affect the way in which people create and use records since, in virtually all parts of the world, records form the basis for legal evidence. In the case of disputes – between governments and citizens, between organisations and employees, between different levels of government – records are the means for proving or disproving claims or complaints. Therefore, understanding how to manage records, particularly electronic records, requires understanding the legal context in which records can and should be created and managed.

The absence of legislation and the existence of ineffective and outdated laws can also affect how records and information are managed. Therefore, it is equally important for the records professional not just to accept that any legislation is good enough; it may be that obsolete laws need to be revised and restructured in order to address the realities of electronic records care in the 21st century.

Records as Legal Evidence

In most parts of the world, legal systems depend on access to trustworthy evidence, which may take three forms: (a) spoken evidence provided by first-hand witnesses or by experts; (b) objects presented, such as weapons found at the scene of a crime; and (c) documentary evidence. Documentary evidence can be written, such as letters or memos, but films, photographs, maps and other types of records can also be considered documentary evidence.

It is up to the courts to examine the item presented (a witness, an artefact or a document) in order to determine its reliability and authenticity as evidence. Therefore, the ability to access reliable and authentic information and records is vital to any legal system, since decisions are made based on the analysis of evidence. If a judge or other legal official has any doubts about the reliability, authenticity or accuracy of evidence, he or she may decide it is inadmissible or unacceptable for use in court.

While the consistent and accountable management of records will not guarantee that they will be accepted as evidence by the courts, efficient record keeping will greatly improve the chance that these documentary materials will be considered authentic and reliable. It is the job of the records manager to maintain the reliability, authenticity and accuracy of the documentary evidence created, acquired and used within the organisation. Modules such as this one are written in order to help equip records professionals with some of the knowledge and skills needed to help them achieve this difficult but important goal.

Reporting and Compliance

As well as making laws and determining criteria for the admission of evidence, governments and judicial systems also establish requirements for how agencies and organisations will operate. In order to support transparency and accountability across

government and in the private sector, many jurisdictions require organisations to provide regular reports about their activities, such as annual reports submitted to parliament or to regulatory authorities.

Organisations may also establish their own internal compliance requirements, instituting rules and regulations to ensure the effectiveness of different business processes, such as the expenditure or funds or the delivery of programmes. All these reporting and compliance processes require the maintenance of and access to good records. Records will also be created as a result of these reporting processes, and they too must be managed effectively.

Audit Requirements

An audit is a formal process intended to review the work of an agency and confirm it has complied with any legal, regulatory or other obligations. The audit also serves to identify the effectiveness of the agency's operations. Most people think of audits as focusing only on financial accounts, but in fact auditors also review a wide spectrum of programmes and services. Other types of audits might focus on computer security, information technology, environmental conditions, the application of standards or guidelines, performance measures, telecommunications systems or health and safety issues.

Typically, governments undertake two levels of audit: a large-scale government audit of a wide range of operations, which reports back to the highest levels of government; and an internal audit, usually conducted on a smaller scale and designed to address more specific issues or concerns. In the private sector, auditors are often called upon to certify an organisation's financial accounts, but audits can also be conducted to ensure compliance with regulations or requirements such as workplace safety laws or environmental controls.

External auditors are required to work outside the control of the agency they are auditing, or they must at least be independent of the specific programme within their organisation that is under review. Internal auditors may be used to help an organisation assess and improve its own performance, whether or not it must comply with any external requirements. Most governments follow generally accepted accounting principles and audit standards for their work, whether those audits are conducted internally or externally. In the United States, for example, the national government adheres to the auditing requirements set out by the Government Accountability Office (GAO). (See, for example, the guidance offered on the GAO's official web page at http://www.gao.gov/govaud/ybk01.htm.)

Records, both paper and electronic, are essential for the conduct of any audit. The inability to produce appropriate records hinders the audit process and can reflect poorly on the organisation or area being audited. It is common for auditors to comment on the quality of, or problems with, record keeping, as they review the effectiveness and success of the programmes under review. Therefore, records professionals need to understand the importance of auditing and, more specifically, they need to identify and adhere to the specific requirements and standards in place for auditing in their own jurisdictions. More importantly, they need to have the

authority and responsibility to establish quality records management operations to support audit requirements.

Budgetary and Financial Requirements

Records are essential to documenting the financial operations of any organisation. Along with policy development and delivery, budgeting and financial management are at the heart of effective organisational management. Financial records identify the resources to be used for different programmes, document whether funds were used for the intended purpose and track the expenditure of funds over a set time. Financial records are inevitably subject to high levels of scrutiny both internally and externally and so must be managed in an effective, accountable and transparent fashion.

Identifying Records-related Legislation

People often talk about 'records-related' or 'records-oriented' legislation as those laws specifically affecting the creation and use of records. In reality, however, virtually every piece of legislation created by a government can have record-keeping implications. In order to ensure the appropriate management of records, the records professional needs to identify all legislation and regulations that could have an impact on the creation and retention of records.

The list shown in Figure 7 below identifies some of the many laws that can influence the way in which records are created and used. It is important to note that this list is representative, not comprehensive. When determining how to manage certain types of records, records managers need to carry out detailed research into specific situations relevant to their own jurisdiction.

Figure 7: Records-related Legislation

- Access to information
- Archives and historical records
- Computer use and misuse
- Copyright, designs and patents
- Corporations and organisations
- Criminal code
- Data protection and information security
- Defence and security
- Education and training
- Electronic transactions
- Emergency planning and business resumption
- Employment
- Evidence
- Health information
- Heritage management
- Human rights
- Identity theft and identity protection
- Information management
- Insurance
- Labour relations
- Privacy
- Records and document management
- Social security and benefits
- Statistics
- Taxation and financial management
- Privacy

Regulatory and Policy Issues

In addition to researching legislative frameworks, it is important for the records professional to understand – and if possible influence – the policies and regulations under which information and records are created, used and managed. Information technology regulations and policies address issues related to the technologies used to

create and use records and information. These regulations need to be established in concert with suitable information management policies that focus not on the technology but on the procedures used to create, use, share and preserve information and records.

Regulations are usually subordinate legislative instruments to actual laws: there ought to be a law in effect before a regulation is established. Laws can have quite a broad scope, but regulations are usually quite detailed. Policies can also be very broad: a policy on data management, for instance, could clarify who owns the organisation's data (the organisation, not the individual) and confirm that it will be stored according to accepted standards, but the policy will not outline the specific procedures involved in ensuring those requirements are met. Policies can be difficult to enforce as they can be interpreted as optional and desirable but not essential.

Figure 8 provides a list of some important records-related regulations and policies.

Figure 8: Records-related Regulatory and Policy Issues

- Acquisition of records
- Appraisal of records
- Contracting of IT services
- Data management and storage
- Database management and use
- Destruction of data on electronic storage devices
- Disaster recovery and business continuity
- Disposal of records
- Electronic mail management
- Electronic records creation and use
- Information technology procurement
- Network management
- Remote access to servers and networks
- Scanning and imaging of records
- Security and privacy
- Training of records staff
- Transferring and storing records
- Use of wireless computer devices
- Web access and use

Understanding Organisational Cultures

Just as every country has its own unique culture, every organisation has its own distinct reason for existing and its own way of operating. In order to manage the records of a particular government agency or organisation effectively, it is important to understand the 'culture' of that organisation: the socio-political, economic and organisational environment in which that agency operates.

Is the organisation a corporation, a government, a non-profit agency or an association? Is it a department within a larger agency that serves a very specific function? What is the mandate of that organisation or department? What services does it deliver? Is it bound by formal laws and regulations, by internal policies or by informal codes of conduct? Is it managed according to formal structures or is it more

laissez faire and outcome oriented? Answers to these questions will help reveal the nature of the organisation and explain, at least in part, how it creates, uses and shares information and records.

For instance, the activity of maintaining electronic maps of a city – showing its streets, sewers, cabling, street lighting and other features – is a substantially different activity from the task of registering and tracking correspondence within an office or the work of paying employees every two weeks. Because these activities are very different, the actual hardware and software needed to support the creation and use of those maps, and need for and capacity of computer networks will be different from the resources and technology needed to manage correspondence or payroll.

Similarly, different levels within an organisation will create and use information and records differently. For instance, strategic-level systems serve the leadership of the organisation, whereas operational-level systems serve day-to-day requirements. The information contained in the various systems may be more or less important: some systems may produce evidence of transactions – records – whereas others may contain mostly raw data.

For example, a five-year budget forecasting system used by executives to plan organisational strategies will draw on data accumulated at the management level, within an annual budgeting system, and at the operational level, within the systems that control accounts payable and receivable. Similarly, an information system that notes daily attendance will create different records from the system that authorises and tracks the payment of invoices. Because each of these systems exists for a different purpose, each will have different technological and record-keeping requirements.

Understanding the organisational culture also involves considering the different elements that make up the organisation, including the following.

- **The mandate:** why does the organisation exist; when and why was it established; has its purpose changed over time; does it perform functions other than those identified as its core business?
- **The people:** how many people work in the organisation; what do they do; what are their qualifications; how are they hired, monitored and compensated?
- **The financial structure:** what is the organisation's budget; what are its usual financial expenditures; what economic constraints does it face and how does it decide on priorities?
- **The physical environment:** what kind of building(s) are in use; what hazards or risks exist inside or near the facility; what is the nature and level of services (such as temperature control, electricity, water supplies); what environmental hazards exist in the area (flood, fire, earthquake and so on)?
- **The geopolitical environment:** is the jurisdiction in which the agency operates stable; is war or civil strife a reality or strong possibility; do governments and administrations change frequently or remain the same for years?
- **The technological environment:** what is the state of the technological infrastructure (as discussed earlier in this module); what level of technical support is available to the agency to manage electronic information resources;

what technical constraints are in place that may hinder effective electronic records management?

- **The information environment:** what is the level of control over records and information; is information used regularly or well to support business functions and activities; what support is in place for improvements to information resource management?

In order to assess organisational culture, it is necessary to research the nature, scope, history and operations of the agency. Records such as mission statements, mandate, business plans and reports can help explain the nature and scope of the agency. Interviews with staff, review of meeting minutes, analysis of financial statements and surveys of office operations can all provide important insights into how the agency performs, and why.

Without taking into account the unique attributes of the organisation, it is that much more difficult to develop and manage an effective electronic records management programme. The work an organisation performs may be the same work carried out by other organisations throughout the country, but the *way* in which the work is performed may be unique to that organisation. Understanding which tasks and functions are or are not unique to a particular agency is essential to determining how best to manage the information and records resources generated by those tasks and functions.

One of the most recent challenges in record keeping involves the changing culture of communications in many offices and organisations. Increasingly, staff members may take work home with them as electronic files stored on USB ports or memory sticks, or they may work on laptop computers in public places, or they may send and receive important messages using cellular telephones, Blackberry wireless devices or other telecommunications equipment. Managing the records generated in these remote locations is an important but very difficult challenge: the danger of losing records or exposing the organisation to security breaches is significant. The guidance offered in these modules is intended to help records professionals consider how best to manage electronic records not just in offices but in all these different work environments.

The next essential issue to understand in order to manage electronic records effectively is the role of record-keeping standards and guidelines. Standards and guidelines are examined in the next unit.

UNIT 1.5

THE ROLE OF STANDARDS AND GUIDELINES

Standards are agreed principles or protocols that are accepted as the required rules or norms for practice. Guidelines are similar to standards in that they identify recommended practice, but guidelines are often less rigorously applied than standards. Most organisations are required to follow certain standards to carry out their operations. For instance, a tea plantation that is bound by standards will not be allowed to sell its product if it does not meet an accepted level of quality. The tea need to be clean, free of pests and properly processed and packaged. Similarly, a car manufacturer who wishes to meet any required standards will need to ensure all cars made by the company is equipped with seat belts, air bags and door locks.

Standards exist to ensure that products and services are of high quality, safe and reliable. Standards also help organisations to meet benchmarks that might have been set by management or by external reviewers. And standards are the tool by which auditors and others can determine whether an organisation has achieved these benchmarks or goals. Often guidelines or requirements accompany formal standards; examples include guidelines for establishing an electronic records management programme, or functional requirements documents that describe the qualities a software package must have in order to support effective record keeping. Both formal standards and less formal guidance materials are designed to improve the effectiveness and consistency of organisational practice.

While all standards and guidelines are important, few are legally enforceable. Instead, their use may be driven by international trade agreements or commercial market decisions. And some standards and guidelines are more advisory: they do not demand precise adherence but instead recommend 'best practice.' The use of such guidance materials is by choice, and the failure to use them will not stop a business from operating. However, the tools are designed in large part to improve the consistency and efficiency of work, and so it is usually highly beneficial for an organisation to adopt them. Users understand the technical and business imperatives that dictate their use, and often there is really no choice but to follow the standards if the organisation wants to be taken seriously in the business place.

It should be noted that most formal standards documents come with considerable accompanying resource material, such as implementation guides, interpretive tools and practical manuals. These tools are designed to make it easier for organisations to apply the standards in their own environment. Ironically, however, it is often

necessary to purchase standards from standards organisations, such as the International Organization for Standardization (ISO) or national standards associations. Organisations wishing to comply with existing standards need to be prepared to expend the funds needed to acquire the actual standards documents.

This unit explains the importance of standards and guidelines, particularly record-keeping standards and requirements, in the preservation of electronic records as authentic evidence. The specific tools examined relate to records management, digital preservation and archival description. The unit also considers the role of archival codes of ethics and discusses some of the issues involved with applying standards.

The ISO and Standards

The International Organization for Standardization (referred to as 'ISO') is a non-governmental organisation made up of the national standards institutes of 157 countries around the world. ISO exists to develop and publish international standards that serve the needs of public and private sector agencies as well as society in general. Established in 1947, ISO has issued over 17,000 standards related to issues such as health, safety and the environment; engineering; information technology and telecommunications; transportation; agriculture; and construction. As ISO notes, 'when standards are absent, we soon notice.'

ISO is responsible for setting international standards, but countries, provinces, states, businesses, professional associations and other agencies also identify standards and principles of practice for use in their jurisdictions. These standards range from accounting and auditing to manufacturing to health and safety. Often a national standard becomes an international standard, or an international standard is adapted for use in a regional or local environment.

Not all standards are legally enforceable, which means that it can be difficult to ensure compliance. Most organisations will recognise those standards that are most applicable to their core business, but the organisations will not necessarily feel bound by standards that are peripheral to their central mandate, especially if those standards are not legally binding. For example, the tea plantation will have to know about standards and rules that apply to the manufacture, preparation, packaging and labelling of food products such as tea. And a car maker will need to know about standards for manufacturing components, safety requirements or pollution and emissions. But neither organisation may even know about or care about standards in place for the size of mailing envelopes, the management of postal services or the manufacture of computer data storage devices – even though the organisations may use envelopes, stamps and CD-ROMs every day.

Information Standards

Many international, national and local standards exist for the creation and management of information. For example, there are standards for such diverse tasks as

- configuring keyboards or visual display terminals (monitors)
- scanning documents and images
- creating Internet addresses
- managing financial and banking information
- creating software documentation.

Consider the Internet, for example. In order for different computer systems to be able to communicate with each other across computer networks, each machine needs to create and send information that can be understood at the other end. The standard established for creating Internet addresses (called uniform resource locators or URLs) controls the sequence of information used and the elements required. When a website address is created according to the established standard, it means that someone else can access the site by typing in a standardised address.

Another Internet standard requires that all content put on to web pages be 'marked up' in either HTML (HyperText Markup Language) or XML (Extensible Markup Language). These two computer languages control how text is presented when it is placed on the Internet by standardising the codes used to denote certain text as headings, paragraphs, lists, computer links and so on. Without such standards for coding text, the Internet simply wouldn't work.

Functional Requirements for Record Keeping

A number of records-oriented guidelines and requirements have been developed around the world, including international, national and regional tools. Many of these products address the 'functional requirements' for effective record keeping. 'Functional requirements' refers to specific operations that a computer system needs to perform in order to achieve the desired output. Specifically, a function is a set of inputs, processes and outputs that leads to an intended product. Functional requirements are usually very specific and measurable.

For example, many guidance materials indicate that electronic records management systems must provide auditing capabilities. However, simply stating in the guidance document that 'the software must audit the use of records' is not enough. A blanket statement does not provide a computer programmer or software developer with sufficient information to provide the technical instructions necessary to allow the computer to support the audit process. Instead, the functional requirements need to detail every element in the audit process, along with any specific needs or exceptions.

Therefore, a detailed and effective guidance document should provide information such as shown below. This example is taken from a popular European record-keeping standard, called *MoReq2* or *Model Requirements for the Management of Electronic Records (2008)*, which is discussed later in this unit.

Figure 9: Excerpt of MoReq2 Requirements for Auditing Electronic Records[4]

Requirement
• The ERMS must keep an unalterable audit trail capable of automatically capturing and storing information about: any action taken on any record, any aggregate or the classification scheme the user undertaking the action the date and time of the action. *The term 'unalterable' in this requirement means that it must be impossible for any user or administrator to change or delete any part of the audit trail. The level of assurance needed will depend on the organisation; the level of assurance that can be achieved will depend on the level of security of the underlying operating system and system software.*
• Where the ERMS supports the transfer of audit trail data to offline storage, the ERMS must support secure processes for managing the offline data and demonstrate how offline data can be brought back online as and when required; and the ERMS must ensure it is not possible for this mechanism to be used as a means of bypassing the controls imposed by the ERMS (for example, by simply moving audit trail data out of the ERMS and changing or deleting it externally to the system).
• The ERMS audit trail parameters must be configurable so that administrative roles can configure which actions are automatically logged.
• All changes to audit trail parameters must be audited in the audit trail.
• *It should never be possible to turn off the auditing of changes to audit trail parameters; the ERMS should always keep a record in the audit trail of which person made changes and when.*
• Once the audit trail parameters have been set, the ERMS must track actions automatically and must log information about them within the audit trail.
• The ERMS must maintain the audit trail for as long as is required by the organisation's records policy.
• *This often will be at least for the life of the records to which the audit trail refers. However, there may be situations in which other policies apply, for example periodic scrutiny of the audit trail followed by its destruction and replacement by a certificate of scrutiny.*
• The ERMS must log in an audit trail all actions performed on records, volumes, sub-files, files, classes and retention and disposition schedules, regardless of whether the action affects one or more of them.
• The ERMS must log in an audit trail all changes to metadata values that apply to the metadata elements listed in the MoReq2 metadata model.
• Any annotation of or amendment to a record must be logged within the record's audit trail.
• The ERMS must automatically log in an audit trail all changes made to administrative parameters.
• *For example, if an administrative role changes a user's access permissions or reconfigures the audit trail.*
• The ERMS must ensure that audit trail data are available for inspection on request, so that a specific event can be identified and all related data made accessible.
• The ERMS must include features that allow all authorised users, including those who have little or no familiarity with the system, to search for information in the audit trail.
• *This is an ease of use requirement. The users may be external to the organisation, such as external auditors. Nonetheless, from the ERMS perspective, they will be users.*

[4] Excerpt from *MoReq2, Version 1.04, 8 Sept 2008, p. 48; available at* http://www.moreq2.eu/downloadsa.htm.

Below is a description of some of the best-known records management guidance materials in place today. Specific information about how to obtain copies of these tools is included in the section on *Additional Resources.*

> See Additional Resources for information about how to obtain copies of the standards and guidelines discussed below.

Note that the creation and preservation of metadata – data about data – is an essential part of the effective management of electronic records. A detailed discussion of metadata is included in the next unit.

ISO 15489: Records Management Standard

The most relevant 'best practice' standard in records management today is ISO 15489: *Information and Documentation – Records Management,* which was published by the International Organization for Standardization in 2001. The standard is divided into two parts.

Part 1, called 'General,' provides a high-level framework for record keeping. Specifically, it addresses the benefits of records management, the regulatory considerations affecting records management operations and the importance of formally assigning responsibilities for record keeping within an organisation. It also outlines records management requirements, describes the components of quality record-keeping systems and delineates the actual processes involved in records management, such as record capture, classification, retention, storage, access and so on. It concludes with an analysis of records management audit operations and records-related training requirements.

Part 2, called 'Guidelines,' provides more detailed guidance about how to implement the framework outlined in Part 1. For example, it outlines the elements of records management policy and responsibility statements, and it summarises the steps involved in designing and implementing an effective record-keeping system. Part 2 also provides practical guidance about the development of records processes and controls, such as creating thesauri of standardised terminology, developing retention schedules, creating security and access controls and storing and disposing of records. Finally, Part 2 provides specific guidance about establishing programs to monitor and audit records systems and to train staff in records management requirements and practices.

Any records professionals considering developing an electronic records management programme or upgrading or revising existing records management practices should review ISO 15489 as a first step. They should consider implementing as many of the recommendations as are relevant to the specific needs of the organisation. Later in this unit are some suggestions for actually applying standards to records management work.

Other Records Management Guidance

ISO 15489 is the best-known records management standard, but it is not the only records-related guidance material in place. Other tools in use around the world include the following.

Australia: AS ISO 15489

The Australian national standards organisation published Australian Standard (AS) 4390: *Records Management,* in 1996. In fact, this document formed the basis for ISO 15489, which was published by ISO in 2001. In 2002, Australia published AS ISO 15489-2002, *Records Management*, which replaced Australian Standard AS 4390. The 2002 document, AS ISO 15489, is an Australian codification of ISO 15489, with some amendments to recognise specific terminology or requirements in the Australian context. Since the Australian standard is so closely aligned with the international standard, it represents international best practice for record keeping and is considered the national standard for records management throughout Australia.

United States: DOD 5101.20

In the United States, the Department of Defense (DOD) issued a formal standard for the management of the records of that department in 1997. This standard was updated in 2007 and is known as DoD 5015.02-STD, 'Electronic Records Management Software Applications Design Criteria Standard,' April 25, 2007. The standard sets forth the functional requirements for records management application software used by the Department of Defense. The standard includes definitions of the required system interfaces and search criteria that records management applications must support and outlines the minimum records management requirements that must be met to comply with National Archives and Records Administration (NARA) regulations.

The DOD standard does not focus on general records management principles but instead specifically addresses the mandatory and desirable functional requirements that should be in place when selecting and implementing electronic records management software. Therefore, its guidance focuses specifically on a computerised record-keeping environment. However, the principles articulated in the standard can be valuable even in those situations where upgrading manual records management processes is the first priority.

Among the valuable information included in the DOD standard are descriptions of the components of file plans or record folders; information about essential records metadata to capture; and the identification of specific information that should be captured when documenting classified or protected records. The DOD standard is now used by both the public and private sectors in the United States and internationally as a basis for creating technical specifications for records management software and programmes.

Europe: *MoReq2*

In 1994, a meeting called the DLM Forum was held to research options for increased cooperation in the area of electronic archives management. The participants included representatives of the member states of the European Union, along with representatives from the European Union government itself. (When the DLM Forum was first established, the acronym 'DLM' stood for the French 'données lisibles par machine' – machine-readable data – but since 2002, the term has come to refer to 'document life cycle management.')

At one of the meetings of the DLM Forum, the participants suggested a need for a set of model requirements for the management of electronic records. The result was the publication in 2001 of *Model Requirements for the Management of Electronic Records* or *MoReq. MoReq* describes the ideal requirements for managing electronic records. In 2008, *MoReq* was updated as *MoReq2*. The primary focus of the document is on the functions an electronic records management systems should be able to perform in order to manage records as authentic evidence. For instance, *MoReq2* includes requirements to ensure that any software chosen will allow a number of important records management functions to be performed.

Figure 10 provides a list of some of the important functional requirements identified in the *MoReq2* standard; these are the tasks that any records management agency should be able to perform in order to ensure the creation and management of authentic and reliable records. Unlike the American DOD standard, *MoReq2* does not focus only on the operations of computer systems. Instead, it outlines the essential elements an electronic records management operation should put in place to ensure that records are properly managed, can be accessed at all times, are retained for as long as they are needed and then are disposed of properly. These elements can be considered principles for effective records management, even in a paper-based environment.

Figure 10: Selected Functional Requirements in *MoReq2*

- Create new files
- Maintain classification schemes and files
- Capture records
- Delete files and records
- Search for and read records
- Change the content of records
- Capture and change metadata about the records
- Manage retention and disposal transactions
- Export and import files and records
- View audit trail data
- Provide access to authorised users

United Kingdom: BS ISO 15489

The British Standards Institute (BSI) has adopted the ISO standard and refined it slightly for use within the United Kingdom. The actual tool is called BS ISO 15489: 2001: *Information and Documentation. Records Management. General.* The BSI has also produced a number of related guidance tools, including BS DISC PD 0025-1:2002: *Effective Records Management. A Management Guide to the Value of BS ISO*

15489-1 and BS DISC PD 0025-2:2002: *Effective Records Management. Practical Implementation of BS ISO 15489-1*.

The National Archives of the UK has also developed a series of guidelines for identifying the functional requirements for electronic records management systems. These guidelines, which are available for download on the official website for the National Archives (http://www.nationalarchives.gov.uk/), address different aspects of electronic records management, including functional requirements, metadata standards, case management, workflow and implementation issues and configuration and metadata issues. These resources are also available on the National Archives website.

Digital Preservation: *OAIS Reference Model*

One of the most important guidelines for digital preservation is *OAIS* or the *Open Archival Information Systems Reference Model*. The *OAIS* model was originally developed by the space science community to provide a generic structure for the organisation and management of digital archives; scientists were motivated by the need to manage the growing body of astronomical and related information that was being generated by national and international space agencies. Subsequently, the model has been adopted as an effective approach to digital preservation for information management communities around the world.

The *OAIS* model addresses the full range of archival functions, including ingesting, storing, managing and accessing records. The model also defines the requirements for describing archival digital resources. OAIS has been ratified as an international standard (ISO 14721:2003: *Space Data and Information Transfer Systems: Open Archival Information System – Reference Model*), and its terminology and concepts are now widely accepted among records and information technology professionals.

OAIS provides the following features to support the preservation of electronic records:

- a framework for increased awareness of archival concepts related to digital preservation and access, for both records professionals and those outside the discipline
- clearly defined terminology for describing information architectures and digital archival operations
- the information needed to compare different long-term preservation strategies and techniques.

OAIS and the Certification of Trusted Digital Repositories

OAIS also forms the basis for a certification scheme for the creation and management of trusted digital repositories. This scheme, developed by the American National Archives and Records Administration (NARA) in conjunction with the Online Computer Library Center (OCLC) and the Research Libraries Group (RLG) in the United States, is based on a checklist called TRAC or Trustworthy Repositories Audit and Certification. TRAC is designed as an audit mechanism for assessing the capacity

of institutions to establish trusted digital repositories that serve to preserve electronic records securely and reliably for the long term.

This TRAC checklist is intended to help support an objective standard by which institutions can measure, and be measured against, their ability to reliably store, preserve, and provide access to their digital collections. As such, it addresses not only technological issues but also issues related to organisational infrastructure and policies. The checklist provides a set of criteria for assessing digital repositories, which can be used as a guide to developing a preservation policy.

> For more information on trusted digital repositories, see Module 4. To obtain copies of the OAIS model and the TRAC checklist, see *Additional Resources*.

International Archival Descriptive Standards

In addition to records management and preservation standards, standards are also in place for the description of both paper-based and digital archives. Archival description is an essential component of good record keeping, and it is important when developing records management policies and procedures to bear in mind the archival functions that will be performed, including description, once those records that have enduring value have been set aside for ongoing preservation and use.

The International Council on Archives (ICA) has issued a range of internationally accepted archival descriptive standards, some of which are identified briefly below.

> See *Additional Resources* for information about how to obtain copies of the descriptive standards identified here.

ICA *ISAD(G)*

In 2000, the International Council on Archives issued *ISAD(G)* or the *General International Standard Archival Description.* The standard is intended to provide general guidance for the preparation of archival descriptions. *ISAD(G)* may be used alone or in conjunction with other national standards, or it may form the basis for the development of regional, local or institutional standards.

ICA *ISAAR(CPF)*

In 2004, the ICA issued *ISAAR(CPF)* or the *International Standard Archival Authority Record for Corporate Bodies, Persons, and Families, Second Edition.* This standard offers guidance for the preparation of authority records, in order to provide consistency in the identification of corporate bodies, individuals and families, when describing archival materials.

ICA *ISDF*

In 2008, the ICA released the first edition of *ISDF* or the *International Standard for Describing Functions.* The purpose of the standard is to support consistency in the identification of the functions performed by corporate bodies, so that even if functions are transferred from one body to another they can still be identified through consistent application of terminology. This standard is designed to work closely with *ISAAR(CPF)* in order to gather extended information about the work performed by records creators, whether they are corporate bodies, persons or families.

ICA *ISDIAH*

In 2008, the ICA issued the first edition of *ISDIAH* or the *International Standard for Describing Institutions with Archival Holdings.* This standard, which is intended to work in conjunction with *ISAD(G)* and *ISAAR(CPF),* is intended to capture and standardise information about the institution that holds archival materials, in order to support user access to archival holdings.

Archival Codes of Ethics

Aside from adhering to standards, records professionals have an obligation to adhere to professional standards of practice. The International Council on Archives first issued a code of ethics for archivists in 1996, which articulates the core standards of conduct for archives professionals. Several national professional associations have also issued codes of conduct guiding the work of archivists and records professionals in their jurisdictions.

See *Additional Resources* for information about how to obtain copies of the codes of ethics of different professional associations around the world.

Several of the principles articulated in ethics codes are of particular importance for archivists dealing with electronic records. For instance, of the ten requirements outlined in the ICA code of ethics, seven take on heightened meaning in the digital environment, where the authenticity and integrity of electronic records can be so easily impaired. These seven are duplicated below, with a commentary following in italic about the importance of the requirement in an electronic environment.

1 Archivists should protect the integrity of archival material and thus guarantee that it continues to be reliable evidence of the past. *Protecting integrity in the electronic environment requires effective management of records and the technology used to create them.*

2 Archivists should appraise, select and maintain archival material in its historical, legal and administrative context, thus retaining the principle of provenance, preserving and making evident the original relationships of documents.

Preserving the context of electronic records creation – including capturing metadata – is essential to demonstrating original relationships.

3 Archivists should protect the authenticity of documents during archival processing, preservation and use. Processing and preserving electronic records involves active intervention, and protecting authenticity is more difficult when processing electronic records than when processing paper-based records.

4 Archivists should ensure the continuing accessibility and intelligibility of archival materials. The ability to access and use electronic records depends on active intervention in the preservation of both the digital objects and the technologies used to create them.

5 Archivists should record, and be able to justify, their actions on archival material. Documenting all work done with electronic records, as part of the metadata captured about the records, is essential to ensuring archivists can justify and explain their actions.

6 Archivists should promote the widest possible access to archival material and provide an impartial service to all users. In an age of instant communications, promoting 'the widest possible access' can take on a new meaning, as archivists are faced with making archives available digitally as well as in original manual form.

7 Archivists should respect both access and privacy, and act within the boundaries of relevant legislation. Respecting privacy is a greater challenge in a digital environment, where widespread access to information is common and desirable and personal and organisational privacy is too easily breached.

Other Records-related Standards

Several other standards exist that relate to records management, archives management, electronic records and digital information. As part of the development of an effective and comprehensive records management programme, the records professional should review as many standards as possible, especially national standards that exist or are in development, to identify areas where information and records management might be affected. Records-related standards include, for example, protocols related to

- the conversion of media (such as paper to electronic or electronic to microform)
- the creation and management of metadata
- the creation of forms and documents (such as the use of templates or the markup of web documents)
- interoperability between different computer systems
- the legal admissibility of records (as evidence, for instance)
- performance measurement and quality control
- the permanence and durability of paper
- the quality and durability of storage equipment and facilities
- the retrieval of information and the provision of access and user services

- the security of information and records (against theft, damage, misuse or loss)
- standardisation of language and terminology
- technical specifications for computer software.

Applying Standards and Guidelines

When considering whether and how to apply records management or other standards or guidelines, the records professional needs first to conduct a risk analysis and determine which standards should be used and how extensive their adoption should be. In other words, the records manager needs to assess the current status of records operations, the risks associated with not implementing a standard and the costs and consequences associated with incorporating that standard into the organisation.

A thorough implementation of any standard, guideline or other requirement can be costly and time consuming. Minimal implementation will be less expensive, but in the end the value of the final product may be negligible. The implementation may end up being a waste of time if the standard or guideline does not do what it was designed to do. Each organisation needs to determine its key business requirements in relation to information and records management, and then it needs to plan the process of implementing a standard so that the tool chosen delivers the best results without overburdening the organisation or becoming excessively complicated.

In relation to ISO 15489, for example, the framework that is included in Part 1 of the standard can be used to provide the structure for organisational policies or business rules. At a practical level, policies based on standards and guidelines need to demonstrate a clear link between the standard, the business requirements and the work of the people in the organisation, so they can see a clear and direct link between the business requirements and the work they perform. Not everybody reads policy documents, of course, and so simple, explanatory documents, such as guides or leaflets, need to be available to help individuals understand in practical terms what they have to do to comply with the requirements.

Implementing standards and guidelines involves the same procedures as undertaking any other business project. A formal and structured approach is best, to ensure the implementation is thorough and the final results effective and sustainable. Actions to take include

- defining the aims and objectives of the project
- defining the project scope
- determining deliverables
- identifying project personnel
- establishing and maintaining communications
- ensuring quality control
- preparing project documentation
- establishing evaluation procedures
- managing necessary organisational change throughout the project.

See Module 2 for a discussion of the steps involved in developing and managing any records management project.

When implementing standards, the following issues need to be addressed in order to gain the greatest organisational and staff support for the effort.

- Everyone in the organisation needs to feel that he or she is a part of the standardisation process; the effort needs to be meaningful and the outcomes desirable.
- The standards chosen need to be appropriate to the organisation; 'one size does not fit all' and often standards need to be customised to suit the specific requirements of a jurisdiction or agency.
- Clear and compelling incentives – both positive and negative – need to be presented to demonstrate to management and staff that compliance with the standard is important. Positive incentives might include: supporting national or regional interests, increasing cooperation with other agencies; improving information flows; complying with funding requriements; or obtaining additional support for other programmes. Negative incentives might include: inability to obtain funding or support; greater exposure to lawsuits as a result of poor information management; exclusion from multi-lateral projects and initiatives; or failure to move forward (personally or as a group) with organisational or career growth.
- Everyone in the organisation needs to understand whether participation in and compliance with the development of the standard is voluntary or whether sanctions will apply if people do not participate.
- The organisation needs to commit adequate resources to the implementation of standards; a half-completed job is worse than not even attempting the standardisation in the first place.
- Once the standards are in place, the organisation will need to go through a transition period before everyone is comfortable with and complies with the new procedures and requirements. The organisation needs to support this transition with resources, training, mentoring and other support as required.

Formally implementing standards and requirements is one way to improve the operations of an organisation and, in the case of records management, increase its ability to manage its information resources effectively. But standards are not obligatory and their implementation can be incremental. Often, if an organisation can gain the support of its staff for improved operations and make change based on the spirit of standards rather than on intensive application of the specifics in them, great gains in efficiency, accountability and effectiveness can still be made.

The next unit examines a specific type of standard relevant to records and information – metadata – and discusses its central role in effective electronic records management.

UNIT 1.6

THE IMPORTANCE OF METADATA

The term 'metadata' has become popular in discussions about the management of electronic records. While the term has been defined in different ways for different situations, in essence the word 'metadata' means 'data about data.' The term 'metadata' refers to information about information; metadata provides the context for a piece of data or information so that the user of that information understands what he or she is using and how and why it came to be. Just as there are standards in place for electronic records management, as discussed in the previous unit, there are standards in existence for the creation and use of metadata.

Bibliographic information about a book or journal – such as the name of the author, the date of publication, the number of pages or the ISBN number – provides information about that book: the bibliographic information is metadata. Similarly, information about the size and dimensions of a three-dimensional object is metadata, and information about the contents and playing speed of a vinyl sound recording is metadata. They all provide contextual information about those items, allowing users to understand how to use and understand the materials.

This unit looks at the nature of metadata and explains its importance as a tool for preserving the authenticity and integrity of electronic records. The unit also examines some of the best-known metadata schema and standards in place for records management, including the Dublin Core Metadata Initiative; the National Archives of Australia Recordkeeping Metadata Standard; and a metadata standard for images developed by the National Information Standards Organization (NISO) and the Association for Information and Image Management (AIIM).

What Is Metadata?

Consider for a moment the following set of data:

100965 020359 031265 300989 060297

Is there any way to know what these numbers mean? They could refer to populations, budget estimates, or bank account numbers. They could even represent lottery ticket numbers. The only way to assign any meaning to the data is by linking the content to its structure and context, which means providing metadata.

Figure 11 provides some general examples of metadata as applied to pieces of information we see in the world every day.

Figure 11: Examples of Metadata

Information	Metadata	Comments
(965) 235-6522	Telephone number with area code	The metadata explains that the number shown is a telephone number and not, for example, a serial number or other type of code.
08/11/08	Date, showing day, month, and year	The metadata indicates not only that the numbers represent a date but also the order in which the information appears: without the metadata it would not be clear if the date is November 8, 2008 or August 11, 2008.
33	Revolutions per minute (RPM) for a vinyl sound recording	The metadata confirms that the recording should be played at 33 RPM, not 45 RPM or 78 RPM.
.ppt	PowerPoint slide software file	The metadata – the extension on the file name – confirms that the file is a PowerPoint file; it does not, however, indicate which version of PowerPoint software has been used. More metadata is required to clarify that information.
1987	Date of publication of a book	The metadata confirms the year of publication of a particular book title. Without the metadata the date alone is meaningless; however, the date information is not useful unless it is maintained alongside other bibliographic information about the book.
001 009 454	Canadian Social Insurance Number	The metadata confirms that a string of nine numbers, shown in groups of three, is a Canadian social insurance or identification number. However, a similar string of nine numbers could represent many other pieces of information, so the metadata provides critical contextual information.

Metadata and Records Management

The term ‘metadata’ emerged out of the information management community many years ago. In the broadest sense, though, records managers and archivists have long been metadata experts. Records professionals have always maintained contextual information about information and records in a paper environment. For example, index cards, file covers, file registers and the headers and footers of paper documents all contain metadata. Records managers have developed computerised equivalents to fulfil a similar function, including computerised indexes, folder names in word processing software and file registers for electronic records.

Metadata is essential for using and preserving electronic records because it provides the background information necessary to understand how and when and by whom a particular set of data or a record was created, collected or received and how it is formatted. It can be impossible, especially when using computerised data, to understand the essential details of a record or file without access to that background information.

Many types of metadata are relevant to the management of electronic records, including 'record-keeping metadata,' 'systems operating metadata', 'descriptive metadata,' 'data management metadata' and 'access/location and retrieval metadata.' Of particular importance to records management is record-keeping metadata, which helps to

- identify records
- authenticate records
- administer terms and conditions of access and disposal
- restrict unauthorised use
- track and document the use of records including distribution, retrieval and delivery for authorised users
- capture structural and contextual information needed to preserve the record's meaning.

Also important to record keeping is descriptive metadata, which becomes very important once a record has been transferred to storage as an archival document and is used by people other than the employees within the creating agency. Metadata elements relevant to archival description include: author, writer, addressee, date of creation, provenance and the existence of finding aids.

Administrative and technical metadata elements may also be important for record keeping; these elements include information about when the record was created, when it was deposited into a digital storage system, who owns intellectual property rights, what format is it in, whether it has it been compressed (such as a digital photograph) and how and so on.

Metadata can be organised into several levels, ranging from a simple listing of basic information about available data to detailed documentation about an individual data set or a record. Given the abundance of metadata a computer system can create, it is important to think about how metadata can best be used for managing and preserving electronic records. For example, some valuable metadata to preserve about electronic records might identify the following:

- **context:** what is the provenance of the record?
- **content:** what is actually in the record?
- **use:** who sent, read, or received the record?
- **structure:** how was the electronic record created and designed?
- **terms and conditions:** how can or should electronic records be made available?

Each of these categories of metadata is described in more detail below.

Context

Contextual metadata identifies the provenance of the record (such as the person or system responsible for creating the record) and provides information that supports the use of the record as evidence of a transaction. Examples of contextual metadata include: the organisation, unit or other entity responsible for authorising or requiring the transaction; the name of the person or system responsible for actually initiating the

transaction; the name of the person or system receiving the results of the transaction; the time the transaction began and ended; the type of transaction (its functional context); and information about any other transactions that are part of the same business activity.

Content

Content metadata identifies the actual information within the record. Keywords may be captured to identify the names of subjects or events or people involved with or mentioned in the record and other information about the actual substance of the record.

Use

Metadata about use is captured in order to document any significant ways in which the record was used following its creation. Typically, use metadata identifies how the record was used once it was created: how was it viewed, copied, edited, filed, indexed, classified and sent. The metadata also identifies when these actions took place and who carried them out. This type of metadata can often be gleaned from the computer system's audit trail, which is the computer record showing who has accessed the system and what operations were performed in a given period of time.

Audit trails are useful for maintaining security and for recovering lost information. Most accounting systems and database management systems include an audit trail feature. In addition, a range of audit trail software products are available to help administrators in an organisation monitor the use of network resources.

Structure

Structural metadata consists of information about the design of the data or record. For example, structural metadata maintains information about the different components of a report, such as the title, section headings, subsection headings, text, annexes and so on. If structural information about the design of the report is lost, the logical flow of ideas in the report could be destroyed. Further, the table of contents and index to the report could be incorrect, thus making information difficult to locate.

Some examples of structural metadata include the following.

- *File identification,* indicating which parts of the computer file are the text of the report itself ('report.doc'), a graphic image ('image.gif') and a spreadsheet (spreadsheet.xls). Metadata should capture each file name and the file location where it is stored.
- *File encoding,* indicating whether and how files have been coded: specific information would relate to modality (eg text, numeric, graphic, sound, video, etc); data encoding standards (ASCII, EBCDIC); method of compression (JPEG, MPEG); and method of encryption (the algorithms used to encrypt the record's content).
- *File rendering,* identifying how the record was created, including information about software applications, operating systems, the hardware used and any standards used. This information is essential to reconstituting a file later, since

using the data may depend on having access to specific hardware or software or following particular standards.

- *Source,* identifying the origin of the record or the relevant circumstances that led to the capture of the data. Source information to capture includes the type of computer system in which the record was created and the instruments used to capture the record. If the record is a sound recording, for instance, then source information might identify the recording equipment used, including the manufacturer, model number or other information about the instrument, as well as information about the date, time and place the recording was made.

Terms and Conditions

Terms and conditions metadata identifies restrictions imposed on access to and use of the data. Terms and conditions metadata also documents any requirements for disposal of the information. Examples of such metadata include information about conditions of use, restrictions on access, reproduction rights and permissions, disposal schedules or destruction conditions.

Developing Metadata Schema

A metadata schema is a list of metadata elements, accompanied by information that identifies the name of each element and provides rules and guidelines for how to capture and describe each element. A metadata scheme, or taxonomy, provides a formal structure that users can follow when determining what information about a record they need to capture and how that information should be recorded.

Existing Metadata Standards

Before developing a list of metadata elements for a particular organisation, the best first step a records professional can take is to review existing metadata standards and consider using or adapting these. A number of detailed metadata standards and schemas have been developed over the years that are worth reviewing. Some are very detailed and designed for large and complex organisations, but they provide valuable information that can be modified for the specific needs of the institution.

Below is a description of three metadata standards that are particularly relevant for electronic records management; each of these standards are freely available through the Internet. They include the Dublin Core Metadata Initiative; the National Archives of Australia Recordkeeping Metadata Standard; and a metadata standard for images developed by the National Information Standards Organization (NISO) and the Association for Information and Image Management (AIIM).

These examples are included to demonstrate the nature of metadata and to provide an overview of the different types of metadata elements that might be useful when capturing information about electronic records. Each metadata schema

- defines the metadata element
- provides the structure of the metadata
- sets out how the metadata is to be applied to the record.

It is not necessary to use any one of these standards exclusively or to use every element included in the metadata structure. It is often necessary to expand or change metadata elements to suit the needs of a particular institution. However, many international and national requirements for record keeping may be based on the use of different metadata standards, and users are urged to research the topic of metadata carefully before determining which metadata elements are most useful or relevant in their own situation.

Since research into metadata is constantly underway, readers are encouraged to review these and other sources regularly to make best use of the most up-to-date information available.

See *Additional Resources* for a list of publications and other tools related to these and other metadata standards.

Dublin Core Metadata Initiative

The Dublin Core Metadata Initiative (DCMI) began in 1995 at a workshop held in Dublin, Ohio, to discuss the development of information standards and the creation of specialised terminology for capturing data about data, or metadata. Over time, the informal group of researchers that held the first workshop evolved into a more formal organisation, which now operates on the basis of a set of formal principles and with clearly identified roles and responsibilities. Drawing on the expertise of professionals from librarianship, computer science, text encoding, the museum community, and other related fields, the organisation has developed metadata standards for creating, filing and sharing information, particularly in a web-based environment.

The Dublin Core metadata standard is a set of elements designed to describe a range of networked information resources. The 'simple' Dublin core standard comprises fifteen elements; an additional 'qualified' Dublin Core includes three additional elements (audience, provenance and rights holder) as well as refinements to the core elements.

Dublin Core is a generic metadata standard that is intended to work with other records and information standards; it was adopted by the International Organization for Standardization (ISO) in 2003 as ISO standard 15836, *Information and Documentation – The Dublin Core Metadata Element Set.*

Figure 12 below outlines the fifteen core elements of the Dublin Core metadata standard.

Figure 12: Dublin Core – Fifteen Core Elements

No.	Element	Description
1	**Contributor**	An entity responsible for making contributions to the content of the resource
2	**Coverage**	The extent or scope of the content of the resource
3	**Creator**	An entity primarily responsible for making the content of the resource
4	**Date**	A date of an event in the life cycle of the resource
5	**Description**	An account of the content of the resource
6	**Format**	The physical or digital manifestation of the resource
7	**Identifier**	An unambiguous reference to the resource within a give context
8	**Language**	A language of the intellectual content of the resource
9	**Publisher**	An entity responsible for making the resource available
10	**Relation**	A reference to a related resource
11	**Rights**	Information about rights held in and over the resource
12	**Source**	A reference to a resource from which the present resource is derived
13	**Subject**	A topic of the content of the resource
14	**Title**	A name given to the resource
15	**Type**	The nature or genre of the content of the resource

National Archives of Australia

In 1999, the Records Continuum Research Group at Monash University joined with the National Archives of Australia to create the metadata schema *Recordkeeping Metadata Standard for Commonwealth Agencies*. In 2008, the National Archives of Australia (NAA) introduced a completely revised version of this standard, which expanded the complexity of the model and allowed for the description of up to five separate entities: record, agent, business, mandate and relationship.

The standard defines an entity as any person, place, event, object, or concept about which information should be maintained. In this instance, the NAA has identified five possible entities about which information might be captured:

1 the record itself (the record)
2 the corporation, organisation or individual responsible for performing a business activity (the agent)
3 a business function or activity assigned to an organisation or its employees (the business)
4 the business requirements leading to the creation of a record (the mandate)
5 any association between two or more entities that has relevance for record keeping (the relationship).

This standard encompasses both records management and archival needs by providing intellectual control of records in order to provide access while ensuring records are well managed from their initial creation to their final disposal. The standard allows record creators and records managers to

- identify unique records
- authenticate records
- document and preserve records (capturing their content, context and structure)
- administer conditions of access and disposal
- facilitate the interoperability of systems through consistency in records creation and management
- enable and support the use of classification restrictions and security
- assist in the creation of finding aids and other tools to allow for identification of valuable resources.

The Australian metadata standard recommends capturing information about up to 25 elements, as listed in Figure 13 below.

Figure 13: National Archives of Australia Metadata Standard

No.	Element	Description
1	Category	The category of the entity being described (such as series for records or work group for agents)
2	Identifier	A unique identification number or name
3	Name	The name or title of the entity
4	Date	Start and end dates of the entity
5	Description	A narrative description of the entity
6	Related Entity	Identification of any related entities
7	Change History	Changes to an entity's metadata values
8	Jurisdiction	The jurisdiction within which the entity operates
9	Security Classification	Security status or sensitivity of the entity
10	Security Caveat	Additional warning or guidance about security or confidentiality issues
11	Permissions	Identification of security requirements or permissions for access
12	Rights	Other access or rights requirements
13	Contact	Information about how to contact an agent
14	Position	The name of the current position held by an agent
15	Language	Language of the record
16	Coverage	The jurisdiction, time or geographic space covered by the entity.
17	Keyword	The subject(s) documented by the record

Figure 13: National Archives of Australia Metadata Standard (cont.)

No.	Element	Description
18	Disposal	Current disposal authorities and actions for the record
19	Format	Information about the actual format of the record
20	Extent	Physical dimensions, size or duration of the record
21	Medium	Physical carrier of the record, particularly manual records
22	Integrity Check	A method for determining whether the record has changed in transmission or storage
23	Location	Current location of the record, physically or in a computer system
24	Document Form	The recognised form of the record, such as agenda, diary, form or memorandum
25	Precedence	The current time sensitiveness of a record, such as how quickly it needs to be acknowledged

NISO/AIIM Metadata Standard

In 2002, the National Information Standards Organization (NISO) and the Association for Information and Image Management (AIIM) published a metadata standard for the management of still digital images: the goal was to create a tool to allow the creators, users and keepers of digital photographs to preserve and exchange digital image files without losing any technical or informational quality.

The data dictionary created as part of the standard includes an extensive list of technical data elements specifically relevant to managing digital images. Therefore, this metadata tool is much more specific to the management of a particular type of record than the Dublin Core or Australian standards discussed above. In fact, the NISO/AIIM standard includes some 150 metadata elements capturing such technical information as size of the digital image file, compression, digital camera model, exposure time, light source and shutter speed.

Given the specificity of these elements, they have not been reproduced here. Interested readers can find more information about this standard at the end of this module. It is important, however, to know that such detailed and explicit standards exist for various types of digital information.

The capture of metadata about electronic records is one of the most important tasks involved with preserving digital information as reliable and authentic evidence. This unit has examined some of the metadata standards in place for use by records professionals; readers are encouraged to review these different standards closely before deciding how to adapt them for use in their own organisations.

STUDY QUESTIONS

The following questions are designed to encourage readers of this module to examine some of the issues raised in more detail and to consider how the general information presented here applies to the specific environment in which these records professionals are working.

1 Name at least three benefits and three drawbacks to the use of electronic information technologies. Are any of these benefits or drawbacks relevant in the context of your specific organisation? How?

2 What is meant by the term 'technological dependence'?

3 Give at least two examples of how technology in your organisation has become obsolete.

4 Identify and explain the three steps that computers perform.

5 What is a computer system?

6 Name as many parts as you can that make up a computer system.

7 Define the concept of digital security and explain why it is important for the protection of records as evidence.

8 Give at least two examples of different information systems in use in your organisation.

9 Describe the relationship of these systems to the mandates of the business units that use them.

10 What record metadata are collected in these two systems in your organisation? Do you believe the metadata collected provide sufficient information about the content, structure and context of records to make sure the records are understandable now and in the future?

11 Define the three attributes of a record.

12 Identify at least three different formats in which electronic records are created.

13 What is the difference between data, information and records?

14 Explain the three characteristics of an authentic electronic record.

15 Explain the concept of information architecture.

16 Research the information technology infrastructures in your organisation. What processes are in place to provide consistent power supplies? What is the bandwidth used and is it adequate for current information and communications needs? What technical support services exist in the organisation? How often are backups made of computer data and records, and how are those backups produced and stored?

17 Identify at least three laws or regulations that affect record keeping in your organisation. When is the last time those laws were reviewed or revised?

18 What audits are conducted in your organisation? Why? How often?

19 Review your organisation's mandate statement or mission statement. Identify at least three ways that good record keeping would enhance the completion of that mission or mandate.

20 What are standards? Why are record-keeping standards important?

21 What does the phrase 'functional requirements for record keeping' mean?

22 Name three record-keeping functions that can be controlled by the application of records management standards.

23 What is the purpose of the OAIS model?

24 What is the role of archival codes of ethics in protecting electronic records? Are there archival codes of ethics in place in your jurisdiction (country or region)?

25 Define metadata. Why is metadata management important to electronic record keeping?

26 Explain the meaning of the following phrases: ‘contextual metadata,’ ‘content metadata,’ ‘use metadata,’ ‘structural metadata’ and ‘terms and conditions metadata.’

27 What is the purpose of the Dublin Core Metadata Initiative?

28 Define the five entities identified by the National Archives of Australia about which metadata can be captured.

29 What is the purpose of the NISO/AIIM metadata standard? How is it different from other records-related metadata standards?

30 Does your organisation capture metadata? For what types of information objects (books, artifacts, archival materials, current records)? How?

31 Based on the information provided in this module, what actions would you take next to improve the electronic record-keeping environment in your organisation?

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

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

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

Produced with funding from the UK Department for International Development