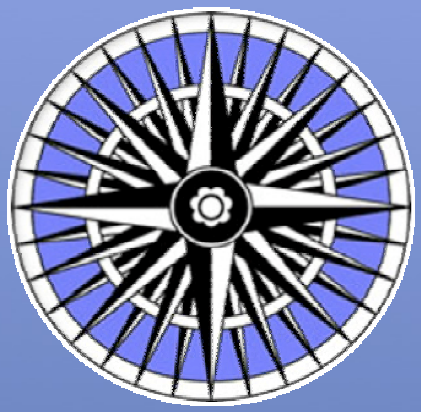
INTERNATIONAL RECORDS MANAGEMENT TRUST



Module 3

MANAGING THE CREATION, USE AND DISPOSAL OF ELECTRONIC RECORDS

Training in Electronic Records Management

MODULE 3

MANAGING THE CREATION USE AND DISPOSAL OF ELECTRONIC RECORDS

Training in Electronic Records Management

General Editor, Laura Millar

MODULE 3

MANAGING THE CREATION, USE AND DISPOSAL OF ELECTRONIC RECORDS

INTERNATIONAL RECORDS MANAGEMENT TRUST

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

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 3: Managing the Creation, Use and Disposal of Electronic Records

Authors

Elaine Goh
Shadrack Katuu
April Miller
Lori Podolsky Nordland
Peter Sebina

Author of Annex: E-Registry Systems in Singapore

Elaine Goh

Additional Contributor

Laura Millar

Reviewers

Andrew Griffin
Michael Hoyle
Segomotso Keakopa
Jim Suderman
Anne Thurston
Geoffrey Yeo

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

Just like physical records, electronic records need to be managed consistently. Effective management includes the following tasks:

- setting up classification structures (to aid in filing records)
- establishing retention and disposal rules (to determine how long to keep records and how to dispose of them)
- assigning access permissions or security rights (to clarify who may use records)
- determining whether a record is official (and so must be managed as part of a formal records management scheme) or transitory (and so should be removed from use as soon as it is no longer needed).

Unlike paper records, however, electronic records may be stored in various formats and on various media. For example, an electronic record may be saved as both a Word document and as a 'portable document format' or PDF (a format that allows documents to be saved and exchanged over the Internet without alteration). The Word document may then be stored in a centralised computer, while the PDF may be transferred to a memory stick or a personal digital assistant (PDA). The same record now exists in two different locations and in two different formats.

Another challenge with managing and using electronic records arises from the way in which they were created. Records created using instant messaging (IM), PDAs, Palm Pilots and electronic mail (email) can be difficult to capture and preserve in an electronic record-keeping repository. Unless the PDA, Palm Pilot or Blackberry is synchronised to communicate directly with the office desktop computer, and unless staff are diligent about downloading and transferring their messages from the remote device to the office computer, it can be difficult if not impossible for records managers to access and preserve those records.

Another difficulty with preserving and protecting electronic records is the way in which they are created: electronic mail, for example, can become like a conversation, with several messages building one on top of another. These 'threads,' as they are called, can become very long. How does a records manager capture the entire thread, when it includes multiple contributors or when the topic or subject of the original email is modified and a new subject emerges partway through the 'conversation'?

As discussed in Module 2, policies and procedures are important tools for managing electronic records. But policies need to be enforced and procedures need to be maintained in order to ensure the ongoing protection of records. Two of the most important procedures that can be taken to preserve and access electronic records is (1) establishing a strong classification scheme for all paper and electronic records,

including electronic mail and (2) capturing adequate metadata about the records as they are created and used.

This module examines several important issues involved in the management of electronic records in the office.

Unit 3.1 defines the concepts of classification and functional classification and then examines the benefits of developing effective functional classification schemes. It then considers the key steps involved in classification, including identifying different types of files, determining the complexity of the classification scheme and standardising information in the scheme.

Unit 3.2 covers a wide range of issues associated with managing electronic records in the office environment. Topics addressed include the following: understanding and applying naming conventions, using computer software to standardise the creation and naming of records and files, considering different methods for saving electronic documents, using different approaches to the collection of metadata (including collecting metadata manually, using computer systems to generate metadata, using forms to gather metadata and using other methods), managing records in shared computer drives, synchronising computers, managing electronic mail, managing paper and electronic records in a hybrid environment and establishing good housekeeping procedures for electronic records care.

Unit 3.3 examines the nature and importance of appraisal and then outlines five steps involved in carrying out effective appraisal and disposal actions, including: conducting research, determining the value of records, making an appraisal decision (including creating a retention and disposal schedule), implementing the decision and monitoring appraisal decisions.

Unit 3.4 looks at the concept of access and considers the importance of developing sound and effective access policies for electronic and paper records, particularly in the public sector. The unit includes a discussion of the importance of regulating and monitoring access, and it addresses the role and scope of access policies.

At the end of the module, a series of study questions is included that readers may wish to review in order to help them reflect on the topics discussed throughout the text. An annex to the module examines the development of an electronic registry (e-registry) system for the management of electronic mail messages; this case study from the National Archives of Singapore complements the information provided in Unit 3.2 and highlights some of the important issues to consider when establishing software systems to manage electronic records.

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

- Organising and Controlling Current Records
- Building Records Appraisal Systems
- Managing Records in Records Centres
- Managing Archives

Procedures Manuals

- Managing Current Records: A Procedures Manual
- Restructuring Current Records Systems: A Procedures Manual
- Managing Records Centres: A Procedures Manual
- Managing Archives: A Procedures Manual

Case Studies

- Candace Loewen, Canada, Appraisal of Common Administrative Records of the Human Resources Management Function of the Government of Canada
- Catherine Bailey, Canada, Macro-Appraisal: The Case Of Income Securities Program Branch
- Andrew Evborokhai, The Gambia, Development Of a Records Management Programme In The Gambia
- Victoria Lemieux, Jamaica, The University of the West Indies: Registry Filing Room Procedures Improvement Project: The Use of Total Quality Management in a Records Management Environment
- Cassandra Findlay, Australia, Development and Implementation of the Immigration Department's New International Traveller Movements System
- Gail Saunders and Elaine Toote, Bahamas, Records Management - Building or Adapting a Records Centre Facility: The Case of the Bahamas Records Centre
- Setareki Tale, Fiji, Improving Records Control and Storage in Papakura
- Ann Pederson, Australia, Management Case Study: Revising the Record Keeping Programme for the Widget Manufacturing Company
- Ann Pederson and Trudy Peterson, Australia/ USA, Archival Control: Case Studies

UNIT 3.1

DEVELOPING CLASSIFICATION SCHEMES

Classification is defined as the process of identifying and arranging records and archives in categories according to logically structured conventions, methods and procedural rules represented in a classification system. The task of classification is to identify different categories of business functions and activities, and the records generated as a result of the work performed, and group those records into logical units in order to facilitate access, storage and disposal. This unit defines both classification and functional classification and then examines the benefits of developing effective functional classification schemes. It then looks at key steps involved in classification, including identifying different types of files, determining the complexity of the classification scheme and standardising information in the scheme.

What Is Classification?

As defined by the International Council on Archives, a classification scheme is a hierarchical tool that can 'facilitate the capture, titling, retrieval, maintenance and disposal of records.' The classification scheme is one of the important foundations for any electronic or paper records management programme: it is the central tool used to describe, categorise and control records. The classification scheme should process series or groups of records efficiently and effectively so that retention and disposition rules can be applied consistently; when used in an electronic environment, a further goal is to allow for the comprehensive computerised search and retrieval of both the record and the metadata.

Classification enables the creation of a structured file plan so that everyone in the organisation can easily identify the one logical and unique physical or intellectual 'place' in which to file records. Classification organises records into mutually exclusive categories so that there can be no doubt about the appropriate place for an individual item. If records are filed logically, information can be retrieved by anyone at any time according to a consistent set of rules and guidelines.

Of course, no classification scheme is perfect, and any scheme will inevitably group together some items which relate to more than one subject area. The great advantage of managing electronic records is that a strong classification scheme can be supported by computerised indexing tools, allowing users to retrieve records not only based on their functional purpose but also by names, dates, keywords or types of document.

As people have started using computer technologies, they have become used to creating, managing, and filing their electronic documents themselves. Even though

well-structured file plans may exist for the organisation's paper records, office workers rarely adopt that plan for the management of their electronic files. Consequently, electronic documents are often created according to individual preferences, making it harder to find, use and manage them.

There are those who question the need for a structured file plan. They suggest that it should be possible to save all electronic documents in one computer storage device, since the computer program allows for sophisticated searches. One of the benefits of automation is the flexibility it provides for creating and revising records and for searching for and retrieving information easily and quickly. One of the difficulties, however, is that if an electronic record is not stored in a logical place, and if the terms used to search for it do not relate to actual words or phrases within or associated with the document, it is virtually impossible to find. Therefore, classification of records becomes even more important when dealing with electronic information.

As well, electronic records need to be organised in order to facilitate managing them as a group, rather than as discrete items. Scheduling, review, preservation and destruction decisions should be applied to records in one group in the same way at the same time. It is particularly important to ensure all records are managed in a consistent fashion in order to ensure the government adheres to records or access legislation; it is a serious breach of the law to find that a record that ought to have been kept has been destroyed or a record that should have been destroyed was kept in error. Managing records in the aggregate is the only efficient and effective way to ensure consistency. An electronic records management system that does not allow for the creation and maintenance of file and folder structures will not serve essential records management requirements well.

The reality is that most organisations will have to manage both electronic and hard copy records. It is therefore critical to have a classification system that functions perfectly in a hybrid environment: that is, a record-keeping environment containing both paper and electronic records. A classification scheme needs to support the storage and retrieval of records that will be created and kept in different physical locations: some on computer servers or storage devices, others in filing cabinets or storage boxes. An effective classification scheme will function efficiently in this hybrid environment.

It is not always possible simply to adopt an existing paper-based classification scheme for the management of electronic records, though a strong and functional file plan will form the basis for a solid new structure. Often, the use of computers changes the way people work: more people work together to create documents, they share information more widely, and their job responsibilities and boundaries change with the flexibility brought by electronic technologies. All these changes can be beneficial, but they can result in more complex records management requirements. A new or revised file scheme is often necessary in order to manage both manual and electronic records in a coordinated manner.

A well-structured classification scheme, whether for manual or electronic records, will

- suit the particular needs of the organisation it serves
- enable unique identifiers (titles and/or reference numbers or codes) to be assigned to each item that requires classification, in order to facilitate management and retrieval
- be fully documented so that all the rules and structures used to classify records are consistent
- will be flexible, to allow for changes in the nature of work and records over time
- will be reviewed and revised on an ongoing basis, in order to ensure it is always current and relevant.

Some of the important qualities of an effective classification system, whether for electronic or paper records, are outlined in Figure 1 below.

What Is Functional Classification?

Increasingly, as governments and businesses develop electronic filing systems, they are creating what could be called 'functional classification schemes.' A functional approach to filing provides the most logical and useful structure for the classification scheme, because defining functions means defining what the organisation does: its responsibilities and work. By organising records by function instead of by department or name or subject, file management becomes easier; file plans do not have to be changed regularly. For example, when filing by function, it does not matter if the name of the department or division changes over time, which makes classification by organisational structure so problematic. Similarly, alphabetical and numerical filing structures require extensive indexes and are out of date as soon as they are developed. A functional structure encourages users to think logically, about what tasks they perform and duties they fulfil.

To create a functional classification scheme, the first task is to identify the organisation's *functions* and *activities*. A function can be defined as a unit of business activity in an organisation or jurisdiction. Functions represent the major responsibilities that are managed by the organisation in order to fulfil its goals, and they are the high-level aggregates of the organisation's activities. Functions may be derived through legislation, policy or programme development, or they may represent a set of tasks or activities that result in goods or services that the organisation is expected to provide.

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

In effect, functions represent the broad responsibilities and work areas of the organisation: functions are what an organisation does. Activities are the means by which the organisation carries out its functions. A filing scheme based on functions

and activities ensures that records are managed in an arrangement that reflects the work that led to their generation. The functional approach links together records that relate to the same activities.

Figure 1: An Effective Classification System

An effective classification system will support business or organisational requirements.

- It will suit the organisation it serves and support decision making and the activities of the organisation.
- It will match users' needs.
- It will be cost effective.
- It will be properly resourced, with adequate equipment, funds or staff.
- It will not be dependent on outside resources for operational requirements.

A classification system will be easy to understand, use and maintain.

- It will be understood by records staff and users.
- It will be independent of human memory.
- It will use simple processes.
- It will inspire confidence in operators and users.

A classification system will be precise.

- It will minimise doubt about where to file records.
- It will allow the quick identification and retrieval of files.

A classification system will be complete and comprehensive.

- It will cover all the files that need to be included.
- It will be capable of including files that may be created in future.
- It will be flexible and allow for expansion, contraction or reorganisation.

A classification system will be backed up by a procedures manual and associated training materials.

- It will be clearly and comprehensively documented.
- Its scope and use will be explained in easy-to-follow steps.
- It will provide master copies of all forms, with completed examples.
- It will be supported by training programmes.
- It will be supported by professional advice or guidance.

A classification system will be easily computerised.

- It will be adaptable for use in electronic records management systems.

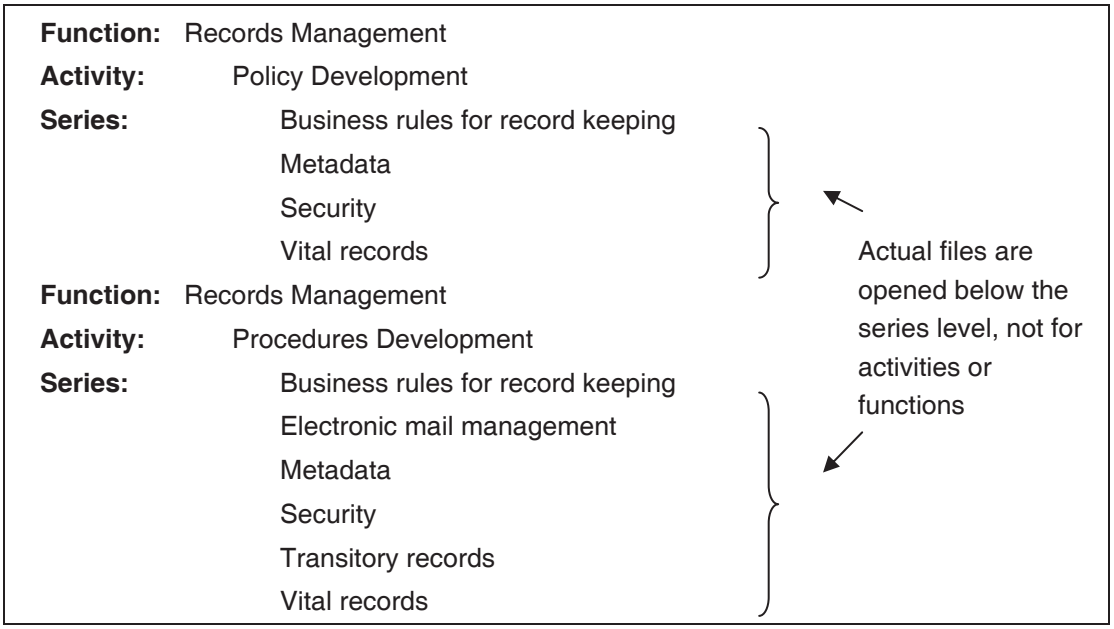
For example, consider the responsibilities of the agency in charge of records management for a ministry or department of government. The core function of that agency – the function it must perform in order to fulfil its mandate – is the management of the records of that ministry or department. To fulfil that function, the agency performs a number of activities, such as

- developing, implementing and enforcing policies, standards, guidelines and procedures
- developing and maintaining classification schemes and disposal schedules

- acquiring, developing and maintaining records management systems (including computer systems)
- preserving records and archives
- providing access to records and archives
- developing and maintaining security systems for records and information
- providing advice and guidance within government on records issues
- developing and delivering training and awareness programs on records issues.

Within each activity there will be a number of records series, which are related to the different records created to document each of the activities. For instance, records related to the activity of developing, implementing and enforcing policies and procedures' may include records related to policies and records related to procedures. So a series would be established to capture documentation about policies and standards, such as for metadata, records security, vital records management, business rules for filing and managing records and so on. Another series would be established to capture documentation about guidelines and procedures, which may relate to the same issues – records security, metadata and so on – or to other issues, such as managing electronic mail or disposing of transitory records. A chart illustrating these different levels of classification is shown in Figure 2 below.

Figure 2: Levels of Classification



The actual files within each series will be determined by the nature of the work itself. There may be draft and final policy documents, memos or emails confirming government approval of policies or opinions from others in the ministry or department about the issue.

The complexity of a classification scheme will depend on a wide range of factors, such as the following.

- The nature, size and complexity of the organisation: the agency will have more intricate records requirements if it is larger or if it carries out a wide range of different functions.
- The nature and complexity of the records: an organisation that creates, for instance, detailed interactive maps, graphical tools or other multimedia electronic records may need a more sophisticated classification scheme to file and find all the components of those records.
- The level of accountability and risk associated with the work of the organisation: an agency that needs quick and accurate access to critical records in an emergency, for instance, will need to develop more detailed and sophisticated classification schemes.
- The technology deployed: the more powerful the computer systems, the more effort should go into developing a sophisticated classification scheme to maximize the benefits of that technology.

This list is far from complete but illustrates some of the issues that can affect the complexity and detail of the classification scheme.

A functional classification scheme ensures that there is one logical place to file similar records: for example, all policy-related records associated with the security of records would be kept together as one discrete grouping, and all procedural records associated with security would be kept as another discrete grouping. Then retention periods can be applied to the series, rather than to individual documents, saving time and ensuring consistency. All policy records related to security may need to be kept for 30 years, but procedural records related to security may only need to be kept for 2 years.

As noted in the International Organization for Standardization records management standard (ISO 15489), classification is a 'powerful tool' that helps organisations work effectively, by

- ensuring records are named in a consistent manner over time
- assisting in the retrieval of all records relating to a particular function or activity
- determining security protection and access appropriate for sets of records
- allocating user permissions for access to, or action on, particular groups of records
- distributing responsibility for management of particular sets of records
- distributing records for action, and
- determining appropriate retention periods and disposition actions for records.[1]

---

[1] ISO 15489: 2001: *Information and Documentation – Records Management, Part 1: General,* p. 13. See *Additional Resources* for information on how to obtain a copy of the ISO standard.

Developing Classification Schemes

As noted, the complexity and size of an organisation can affect the level of detail included in a classification scheme. If, for example, an agency responsible for records management offers training as part of its duties, it will need to retain records related to designing and delivering training programmes. However, if training is not its primary purpose, records related to training (1) should not be very extensive and (2) likely will not be needed in the long term as central evidence of the functions of the agency. On the other hand, an agency entirely responsible for training as its central business function will create many more records related to the business of training, and a large number of those records may need to be kept as evidence for the long term.

It is wise not to make a classification scheme more complex than it needs to be: a well-structured functional classification system will be easily expandable, which means that additional categories can be added later, if and when the agency's responsibilities and records expand. It is best not to anticipate the future and create activities or series 'just in case' some particular task becomes part of the agency's responsibilities at some undetermined point in the future.

The goal of an effective classification scheme is to enhance usability of an access to records throughout the organisation. Therefore, it is essential to keep the users' needs and understanding in mind and not focus solely on the needs or preferences of records managers.

Figure 3 below is an extract of a fictitious classification scheme for a central government agency, showing the classification structure for managing records created in order to support the function of records management in the government.

Figure 3: Sample Government Records Classification Scheme (excerpts only)

FUNCTION: RECORDS MANAGEMENT

Description: The function of managing the organisation's official records throughout their life cycle, including managing the processes of creation and receipt, capture and organisation, storage and protection, use and disclosure, and destruction and preservation; the function also includes developing and implementing plans, systems, standards, training and communications to effectively accomplish the life cycle management of records.

Activity: Classification Development
Description: The activity of designing, developing, and implementing classification systems in order to organise records. Includes records related to developing classification schemes, controlled vocabularies, naming conventions, numbering schemes, indexes, taxonomies, thesauruses and other information control mechanisms.

Series: Functional Classification General
Files: Classification Policies
Records: draft and final policy documents, agendas, minutes, reports, communications

Series: Classification Procedures
Records: draft and final procedural documents, agendas, minutes, reports, communications

Series: Functional Records Classification Schemes
Files: Case Files by Name of Department
Records: draft and final classification schemes for each department, evaluations and feedback, requests for changes, approval records, reports, communications

Activity: Electronic Records Systems Administration
Description: The activity of implementing, maintaining, supporting and documenting the organisation's electronic records management system (ERMS). A separate series is created for each task involved in maintaining the system.

Series: Hardware and Equipment Maintenance
Files: Case Files by Name of Equipment or Hardware
Records: contracts or agreements, maintenance logs, requests for maintenance or repairs, tests, reports, communications

Series: Software Configuration
Files: Case Files by Name of Software
Records: contracts or agreements, configuration specifications, requests for programming changes, tests, reports, communications

Series: User Training and Support
Files: User Training
Records: training and testing materials, training service contracts, user evaluations and feedback, reports, communications

Files: User Support
Records: user updates and bulletins, guidance notes and advisory information, user feedback, communications

Activity: Marketing and Promotion
Description: The activity of promoting records management operations and the work of the records management unit within and outside of the organisation, including networking through participation in professional groups, raising awareness and disseminating information about the records management programme and maintaining relationships with stakeholders within and outside the organisation.

Series: Committee and Association Membership

Files: Case Files by Name of Organisation or Group

Records: invitations to conferences or workshops, speeches or presentations to professional associations or groups, membership information, committee records

Series: Awareness Raising and Information Dissemination

Files: Records Management Website

Records: draft and final copies of core web documents, policies and procedures about website contents and management

Files: Records Management Newsletter

Records: draft and final copies of newsletters, policies and procedures about newsletter contents and management

Files: Stakeholder Outreach

Records: invitations to seminars, workshops or public events, speeches or presentations to stakeholder groups, draft and final versions of information dissemination tools

Activity: Policies, Standards and Procedures Development

Description: The activity of establishing policies, procedures, standards and guidelines for effective records management throughout the organisation.

Series: Policies, Standards and Procedures

Files: Case Files for Different Policies (such as records management, metadata, security, email management, vital records management)

Records: draft and final copies of policy, procedures or standards documents, related policy and procedural records, records related to approvals and implementation of policies

Activity: Preservation

Description: The activity of establishing policies, procedures and approaches to ensuring the long-term preservation of information and records and protecting vital records in the event of an emergency or disaster.

Series: Disaster Planning and Emergency Response

Files: Disaster Planning and Emergency Response Policies

Records: draft and final copies of policies, related policy records, records related to approvals and implementation of policies

Files: Disaster Planning and Emergency Response Procedures

Records: draft and final copies of procedures, related procedural records, records related to approvals and implementation of procedures

Files: Disaster Planning and Emergency Response Training and Testing

Records: records related to testing scenarios, training exercises, evaluations, reports and recommendations for revisions to policies or procedures

Series: Electronic Records Preservation

Files: Electronic Records Preservation Policies

Records: draft and final copies of policies, related policy records, migration plans, digital preservation strategies, research related to longevity of digital components

Files: Electronic Records Preservation Procedures

Records: draft and final copies of procedures, testing and development records, related procedural records

The next unit outlines a wide range of actions that can be taken when managing electronic records in order to improve efficiency and protect the integrity and authenticity of the records.

UNIT 3.2

MANAGING ELECTRONIC RECORDS

There are four common ways of creating, using and storing documents in an electronic environment: in personal computers, where individuals control the creation and use of the records; in shared computer servers, where individuals control the creation of records but share those records with others in the organisation; in shared servers with centralised control, where all individuals adhere to established procedures for creating and managing records; and in shared servers using electronic document or records management software, where control over the creation and use of records is strongly regulated. Each of these approaches to creating and using electronic records can result in different methods for managing those documents, particularly for naming, filing and accessing records.

When there is little or no control over how electronic records are created and used, inconsistency can lead to difficulties finding and retrieving information. More control leads to more consistency, but it is important to ensure that the users' needs are well served; after all, they create documents in order to use them for their work, and they need easy and fast access to their office records.

This unit examines some of the ways in which electronic records can be managed in order to make information readily available to users and to ensure authentic and reliable electronic records are protected for the long term. Specific topics covered include: managing records in shared computer drives; understanding and applying naming conventions; using computer software to standardise the creation and naming of records and files; considering different methods for saving electronic documents; collecting metadata; using computer systems to generate metadata; using forms to gather metadata; considering other methods for gathering metadata; synchronising computers; managing electronic mail; managing records in a hybrid paper and electronic environment; and establishing good housekeeping procedures for electronic records care.

Managing Records in Shared Computer Drives

In most organisations, users have access to a series of networked computer drives, where they create, store and access corporate documents and share information through Intranet or Internet sites. Typically, an organisation maintains the following types of computer drives:

- a corporate-wide shared drive, containing documents relevant to the whole organisation

- a branch or divisional shared drive, containing documents relevant to a single organisational unit
- a personal drive containing documents relevant only to the individual.

Using shared network drives has many advantages. For example, staff can

- place documents on a shared drive and let people know it is there (called 'publish and point') rather than duplicate documents multiple times
- develop logical and useful filing structures for shared drives
- develop and adhere to common terminology
- establish control over the creation of folders within computer systems
- develop 'good housekeeping' practices for synchronising the creation, use and disposal of documents.

Of course, successful use of shared drives depends on the creation of and adherence to clear and usable policies for managing electronic documents. Some important issues to consider are outlined below.

Adopting a Publish and Point Approach

A 'publish and point' policy is a method of controlling the duplication of a document while it is being widely circulated. Instead of attaching the document to an email message, which sends each recipient an individual copy, a read-only version of the document is placed on a shared drive – in other words, it is published – and a pointer or shortcut is emailed to alert intended recipients. Recipients can then retrieve the document from the shared drive as required. A publish and point policy

- encourages a culture of sharing documents as organisational resources, rather than retaining them as individually owned items
- encourages users to think more carefully about the most appropriate method for distributing information
- reduces the number of working copies of records in individual folders.

A publish and point policy will tend to decrease the requirements for individual document storage, but it may increase the network traffic and may require more storage space in shared computer servers.

Establishing General Filing Structures

When a significant number of documents are stored on a shared network drive, a basic general filing structure should be established. If a division or branch (or a specific project) has developed its own filing structures, these structures should aim to conform to the principles of a general filing structure in order to prevent divergent practices and application.

End users should also be encouraged to use consistent filing structures in their own group and personal work spaces, not just when filing into shared drives. This consistency will help the organisation coordinate the creation, use and retention of working papers and final documents and will ease retrieval and access of information throughout the institution.

Configuring a Secure Record Drive

A secure record drive is a shared network drive which has been configured in such a way as to prevent the amendment or unauthorised deletion of documents on the drive. With such a mechanism in place, organisations are more likely to consider the electronic document to be the official corporate record, even though a paper copy may also exist. Any records considered official and final should be stored separately from transitory or non-official electronic documents, and the organisation should establish clear definitions about who has the right to add records to or delete records from the drive. When establishing a separate storage location for official records, consider the following suggestions.

- Before establishing a separate storage area, assess the risks involved with this approach and clearly identify the types of document which it may be acceptable to manage in this way. Remember that a secure drive does not provide the same level of security as a fully managed ERMS.
- Use a separate logical hard drive with read-only settings to prevent anyone from making changes to documents that have been saved to the drive.
- Ensure that users can read and create documents but that they cannot replace existing documents. with edited versions.
- Ensure appropriate backup and recovery procedures and maintain necessary levels of security at the operating system level.

Although separate storage areas can provide reasonable sound storage of documents in the short term, there will be challenges with migrating material to a full ERMS later. For instance, a Microsoft Windows directory structure does not easily provide document and folder level metadata that will support a structured migration to an ERMS. Although migration can be achieved, it may be a relatively expensive process. Research is critical before decisions are made and new systems implemented.

Understanding and Applying Naming Conventions

Standardising the way in which folders and documents are named can dramatically improve access to electronic records. Applying naming conventions results in

- better access to and retrieval of electronic documents
- improved sorting of documents into logical sequences by version number or date
- easier identification of documents in lists or directories
- better management of different versions of documents.

Essentially, naming conventions serve two related functions:

- Consistent naming of folders or documents brings related items together under a common label.
- Consistent naming also distinguishes similar items by naming each in a consistent, logical and predictable way.

Standardising Terms

Since every agency's core business is and ought to be different from the business of every other agency within a government, it is not possible to 'cut and paste' classification schemes from one unit to another. It is necessary to analyse each agency's duties and responsibilities and determine an appropriate classification scheme accordingly. However, most agencies carry out a similar range of administrative functions and activities, and administrative records series created in one agency are often similar to those in another agency. Consequently, it is possible to draw on existing resources, and to create standard terminologies, for classifying some types of records. A useful tool for improving consistency and streamlining the classification process is a functions thesaurus, which helps to standardise the terms used to refer to different functions and activities.

A functions thesaurus is an alphabetical list of preferred terms for use in a classification scheme or other records management tool. The terms are linked together by their different relationships, so that the user can review terms related to a particular function or activity and determine the best term to label it when categorising its records. Thus the thesaurus helps support standardisation and consistency by ensuring that the same terms are used when representing the same type of function or activity.

For example, an organisation involved with the development and delivery of workshops could refer to its work using words such as 'workshops,' 'training,' or 'education.' Which is the best term? What about other terms, such as 'schooling,' 'teaching,' 'guidance,' or 'instruction'? A thesaurus helps determine which term should be used in a particular instance and recommend against the use of other terms if they were not considered appropriate.

A thesaurus can also support the standardisation of terms representing common activities or types of records that may appear across the agency. The chart shown in Figure 4 below illustrates some of the common tasks performed in different offices and the different terms that could be used. Selecting one term and using it consistently has many benefits, including

- encouraging common use of language for similar work
- maximising the retrieval of information using search features in records management software
- supporting decisions about whether common types of records may or may not warrant similar retention periods.

The development of a thesaurus of terms is one way to standardise the use of names and terms. Below are some other suggestions for developing and using standard approaches to the creation of file names. Also included are some suggestions for how to create folder titles so that they are understandable and usable.

Figure 4: Selecting Terms for Business Functions and Activities

Function or Activity	Possible Terms	Issues to Consider
Providing advice and guidance	Advice Advisory services Advice and consultation Consultations Opinions	• Is providing advice a core function, in which case it will involve a wide range of activities, or is it a small part of a much larger set of duties and only happens from time to time? • Do the terms 'advice' and 'guidance' have specific meanings within the organisation that determine how they might be used and understood?
Developing and delivering training	Training Education Workshops Guidance Seminars Awareness raising	• Does the organisation offer formal education programmes, or does it offer in-house or informal training opportunities? Do the terms used clearly reflect what people do and why?
Providing outreach services	Outreach Promotion Marketing Advertising Awareness raising	• Is outreach intended to lead to awareness raising, to promote a product or service, to sell goods, or to achieve some other outcome? Which terms best represent the purpose of the work performed?

Creating File or Document Names

Creating understandable and logical document or file names is essential to easy and quick retrieval of records. At a minimum, all document names should include a title, a version number and a date. Other information that might be included in a file or document name are shown in the chart below, which is based on naming conventions used by the Government of Alberta, Canada: the chart shows the recommended order in which these elements should appear.

For more information about the Government of Alberta's naming conventions, see the government's Information Management Branch's official website at http://www.im.gov.ab.ca/.

Don't forget these tips when developing naming conventions.

- Remember that nothing comes before something (for example, when sorting records in an electronic filing system, the term 'Policy' would come before the phrase 'Policy Directives').
- Similarly, using zeros can ensure documents sort in proper numeric order so that they are displayed in order on the computer screen (for instance, 10 will come before 9 but 09 will come before 010).
- The following characters are usually not allowed in file names, because the symbols may also be used in computer commands or for other purposes:
    - forward slash [/]
    - backslash [\]
    - greater than sign [>]
    - less than sign [<]
    - asterisk [*]
    - question mark [?]
    - quotation mark ["]
    - pipe symbol [|]
    - colon [:]
    - semicolon [;]

Below is an example of poor usability in a pathway name. The name is so long, with so many levels, that it can be confusing to know precisely what is filed in the folder.

Staff reports\ Registry \ Surveys of Government Departments \ 1999 – 3RMG 13.11 \ Staff Survey 1999 – Analysis and Results Process – 3RMG 13.11.2 \ Survey Forms Returned

A better name would be

Staff reports – Survey 1999 – Survey Forms Returned

If retaining specific reference numbers is important, it is possible to add those to the metadata for the record, so that they can be searched and retrieved through the computer system. Figure 5 is an example of naming conventions used in one jurisdiction: the Government of Alberta, Canada.

Figure 5: Naming Conventions in the Government of Alberta[2]

Naming Elements	Example	Description of Need or Use
Title	Literature Reviews	The first three elements (title, version and date) are usually needed to facilitate searching for the document and the display of like documents in a logical order.
Version Number	V01	
Date (publication date, version date, or logical date relevant to the document)	2005_05_31	
Author or Creator	Jsmith	The middle elements (author, business unit and type) may be needed, depending on the business requirements. They can be helpful in identifying the controller of the document.
Business Unit/Program	Research	
Type (eg., report, memo, letter)	RPT	
File Extension	.doc	The last element (file extension) is provided by the application in which the document has been created and is always last. It is important to remember that this element should not be altered.

Sample short title: Literature Reviews V01 2005 05 21.doc
Sample long title: Literature Reviews V01 2005 05 31 Jsmith Research RPT.doc

Standard terms and forms of name should be used wherever it is sensible to do so. In particular, this can apply to the names of people or organisations, the names or projects and activities and logical document types. When choosing between the full spelling of a name and an acronym, it is important to be consistent; do not use the full name sometimes and the acronym at other time. For example,

- Choose between e-government and electronic government.
- Use accepted acronyms, such as DOH instead of Department of Home Affairs. Do not use Dept. of Home Affairs, D-home-affairs, or dept-h-a.
- Use standard terms for document types, such as agenda, letter, minutes, project report, memo and so on.
- If the author's name is captured in the metadata (and it should be) then it usually does not need to be repeated in the document title. If using personal names, decide whether to use forename then surname or surname then forename: Jason Smith or Smith Jason. Do not use the two orders interchangeably.
- When a date is necessary in the document or folder title, order the elements so that they display chronologically, for example in a YYYYMMDD pattern. Months spelled alphabetically do not file in chronological order.

[2] Source: Government of Alberta, *Naming Conventions for Electronic Records* (Service Alberta, August 2005), p.6.

Document titles should contain enough information to identify them if they become detached from the correct folder. A large number of documents entitled *2000-04 Minutes* is not helpful. Naming conventions should aim to strike the right balance between brevity (keeping titles short) and usability (providing useful information about the content). Also important is to ensure that the relationship between individual documents and the folders in which they are stored is maintained in a meaningful fashion within the record-keeping structure.

Controlling Versions of Documents

Consistent naming rules can link different versions of the same document, by including a version number as part of the title. This approach will also help to provide an audit trail for future tracking of document development but the success of this method depends on accurate and careful naming and tracking of versions. There is a danger of inconsistency if different users access and update different versions of a document without coordinating their efforts. As a result, different versions may exist throughout the organisation. Well-developed and robust procedures are important for control of document versions in a multi-user environment.

A first task is to establish procedures for when to call a document a new version or when to save it with the same title as the previous edition. Remember that what constitutes a substantive change depends on the business context of the work being performed. For instance, all versions of legislation under development may need to be kept, but only the final version of an administrative memo may be worth keeping.

A common method for version control numbering is to use the ordinal number (1, 2, 3, etc) for major version changes and the decimal number for minor changes, as in: ver. 0.5; ver. 1.0; or ver. 2.7. A version 1.0 normally denotes a first document version given wider circulation.

Using Computer Software to Standardise Records Creation

While computer software packages such as Microsoft Word advertise that they can capture metadata and apply file names and titles consistently, the reality is that the computerised features in such software are usually neither useful enough nor flexible enough to suit the specific needs of a particular organisation. For example, there is a feature in Microsoft software called ‘Document Properties’ that allows users to capture metadata about the document being created: the software will capture information such as author, title, keyword ‘tags’ and date. There are advantages to using a Document Properties feature, such as the following.

- Standard key metadata terms will accompany the document at all times.
- The history of the creation and use of the document will be documented over time.

However, there are also disadvantages, as shown below.

- Requiring staff to fill in Document Properties metadata leads to more work before records can be closed and filed.

- The metadata can be misleading, especially if document production is shared: for example, the *Author* field may take the last named editor even though several people have worked on the document.
- In practice, no one may bother to use or maintain the metadata gathered using Document Properties.

Controlling Dates

In Microsoft applications, it is possible to insert a generic date field, which can be updated automatically by the computer application each time the document is saved or opened. This feature is convenient when used carefully, but it will provide false information if it is used indiscriminately, particularly where different types of date are not clearly labelled and identified. The best course of action is to turn off the automatic date function and require staff members to insert date information manually.

Saving Electronic Documents

In order to provide ongoing access to records, it is important to define standard formats in which documents should be saved, particularly if many different software applications are in use or many people need to access and use records. It is always preferable to limit the number of formats used as much as possible, to reduce the difficulty of providing access or preserving records in the future. There are three basic options for saving documents, as outlined below.

- One choice is to standardise on an *exchange format,* when multiple application versions are in use. For example, you can use the Microsoft version of RTF, by saving all corporate documents in an .rtf format (which the application can be set to do automatically). These documents will be accessible by different application versions (e.g. MS Word 97 and MS Word 95) and by other word processors; for further modification or manipulation but some formatting information may be lost in certain circumstances.
- Another choice is to standardise on a *distribution format,* which is most appropriate once documents are finalised and the content will not change. For example, a PDF rendition of a document converts documents so that they can be read but not revised. However, it is necessary to have the appropriate Acrobat software for creating PDFs. This option is unlikely to be cost-effective in an organisation with a large number of direct users, and access to the documents is best provided through a centralised storage function, which may not be available in smaller organisations.

In order to determine the most appropriate method for saving or sharing documents, it is necessary not just to select the easiest or most accessible option but to research different approaches thoroughly.

Collecting Metadata

The concept of metadata was introduced in Module 1. This section discusses approaches to collecting metadata when creating and using electronic records in the office environment.

There are two options for collecting metadata. Both options may be relevant for different types of records and both may be used together, depending on the nature of the computer systems in place. Metadata can be captured automatically by computer systems or it can be gathered systematically by having the creators and users of records complete forms and templates. Metadata may also be added by records managers and archivists as records are transferred throughout the record-keeping system. In recent years, work has been underway to develop software that will capture metadata after the fact using what are called 'utility programs.' Generally, though, both manual and computerised approaches will be used to capture metadata.

Much of the technical metadata related to a digital resource is automatically captured, such as file format (such as 'doc' or 'pdf') or software application and version (such as Adobe 8) are captured automatically. Metadata that is entered by a user may include descriptive elements such as links to related documents, custodial history (changes in ownership of a document, particularly as a result of reorganisation of an institution) and title.

Metadata elements may also require modification by users if the software captures the information automatically. For instance, in most word processing applications, the title of the document is automatically captured by the computer program. In these instances, the first line of the document becomes the title, but this string of words may not be useful or meaningful. Consequently, the user will need to modify the title manually to something more appropriate.

Issues to Consider when Collecting Metadata

When developing a process for capturing metadata, it is important to consider the following issues.

- The greater the amount of metadata attached to a record, the higher the potential cost for storing and managing the metadata and the record.
- The poorer the quality of the metadata, the harder it is to manage, locate, retrieve and access electronic information.
- Entering complex metadata efficiently, accurately, and consistently can be costly, time consuming and error-prone, leading to inaccuracies and inconsistencies. Vigilance is required to ensure quality information is gathered.
- Manual capture of metadata can lead to variations, depending on the interpretations made by different people during the process. To avoid variations, it is important to
    - use naming conventions consistently
    - use metadata that are meaningful to the users and the organisation

- train staff thoroughly and monitor their work regularly
- focus on capturing metadata schema that is useful for the organisation's business processes and do not attempt to create elaborate systems if they are not required.

- Another difficult challenge with capturing metadata is getting staff members to comply with the process. Many users do not want to enter information into computer screens, considering it a poor use of their often very limited time. It is important to convince them that managing metadata effectively will help improve their business operations, maybe even saving them time in the long run.

Software Tools for Generating Metadata

Below is a brief overview of some of the software tools currently available to create or capture metadata from electronic files. Most of these tools use the metadata elements identified in the Dublin Core Metadata Initiative. This list is provided as an indication of the types of software available; readers are encouraged to research these and other tools in order to determine their suitability for the organisation. Note also that these tools should not be needed if the organisation has developed an effective electronic records management system that captures metadata when records are created. These tools are more useful for capturing metadata in records that have already been created but have not been stored in a formal ERMS system.

Metamaker

Metamaker is a tool designed to create Dublin Core compliant metadata. The tool allows the user to create metadata from scratch using a simple web form and save the information in different computer file formats. The tool also allows users to extract metadata from existing web pages or local html files. A list of frequently used terms is included in the tool to allow for standardized description of the information captured.

My Meta Maker

My Meta Maker is an online tool to create metadata for online (open access) publications, such as e-journals.

JHOVE

JHOVE was created by a non-profit organisation called JSTOR (which stands for Journal STORage), in partnership with the Harvard University Library. JHOVE (JSTOR/Harvard Object Validation Environment) – pronounced 'jove' – is a software program that will automatically identify the format of computer files; verify that the format extension and file are the same; and extract technical metadata from the file. By extracting and confirming this information JHOVE can validate the format of computer files, ensuring their integrity and authenticity.

DC-dot

DC-dot is a software program that automatically extracts and validates metadata from HTML resources and MS Office files. The metadata can then be edited using the form provided and converted to various other formats if required.

With the development of more sophisticated electronic records and document management systems, the capture of essential metadata is becoming easier, as the software applications automatically gather a great deal of important information automatically.

See Module 2 for more information on selecting and implementing electronic records management systems.

Synchronising Computers

With the increasing use of laptops, handheld computers and personal digital assistant devices (PDAs), it is common to find that documents have been duplicated in different computer locations. If procedures for synchronising computers are not established, important documents may be lost, potentially conflicting versions may be retained and confusion can result.

It is important, therefore, to establish procedures for managing different technologies, including

- maintaining a filing structure on a laptop that is consistent with the structure used on the desktop
- developing a disciplined approach to updating document versions
- nominating a single storage location for documents in development, to hold the primary version and later updates.

File synchronisation facilities such as Microsoft Windows Briefcase, which keeps track of changes to particular files, can help to control duplication, as long as the software is used properly. Windows is not designed to handle file conflicts easily, and it is not a substitute for effective procedures, particularly in cases where several members of a work team are working on the same documents.

A similar synchronisation facility is often used with Microsoft Outlook and Microsoft Exchange to synchronise folders between the email mailbox of a laptop and the user's primary network mailbox. Many people use this facility to create emails using the local laptop copy, and these emails are later uploaded to the main mailbox for dispatch. The synchronisation facility harmonises changes in both main and local mailbox versions. Potential difficulties can arise where two separate copies of a message – a local copy and a main copy – have been edited separately, resulting in conflicting versions. It is essential to establish procedures for uploading locally made changes to the main mailbox before editing or transmitting main mailbox versions of messages.

Managing Electronic Mail

Electronic mail (email) messages should always be treated as potential corporate records of the organisation. More and more departmental business is conducted by email, replacing the conventional memo and, increasingly, the formal letter. To manage email effectively, it is necessary to establish policies and procedures for

- clarifying which emails should be kept
- managing messages within the email system
- managing emails in shared drive folders when necessary
- managing the composition of emails and the exchange of emails (as threads develop)
- helping individuals to manage their own mailbox.

Valuable records can be lost if email is not managed effectively, but it can be difficult to establish firm control over email creation and use. Since email is not a record series but is instead a mechanism for the transmission of information, an electronic mail system cannot be scheduled in its entirety; individual decisions have to be made about which emails to keep and which to destroy. As well, retention of messages depends on their content and context, and both content and context differ depending on whether the message has been sent or received, how an email thread develops and who is responsible for what part of the communication process.

Therefore, email policies are essential to guiding users about which types of email messages should be kept in the short- , medium- and long term. Policies should cover

- whether and when messages sent and messages received should be retained
- how to manage email threads
- whether and when drafts of emails should be retained
- who will have access to different types of emails.

In addition, organisational policies should emphasise

- the fact that any email message relating to departmental business may be considered an official record
- the importance of taking care with language used when composing emails
- the importance of protecting personal privacy when communicating via email
- the importance of avoiding any inappropriate content in email messages.

In an organisation that does not have a computerised ERMS system in place, there are three main approaches to managing email records:

- by adopting a ‘print-to-paper’ policy
- by managing emails within the email system itself
- by saving messages to a shared drive.

Adopting a Print to Paper Policy

An organisation may adopt a policy of printing all emails and filing them in the paper filing system. There are drawbacks to this approach. For example, documents are often not actually printed and placed on a paper file, because this task is seen as increasingly burdensome by the end user at the desktop. As well, it may not be possible to print all the metadata that exist within the email system. On the other hand, the electronic version of the document may not be consistently managed either, and emails may be stored in a variety of locations and under different names, with no guarantee of accuracy and therefore with limited access.

Managing Emails within the Email System

Retaining emails within the organisation's email system is sometimes the easiest way to preserve them, since the person responsible – the office worker at the desktop – does not need to undertake many actions beyond just creating, sending, receiving and/or filing the message. However, if the user is storing emails in personal folders, then access is limited to that person only, or his or her designate, and so the record is out of the reach of the organisation as a whole. On the other hand, if messages are stored in a work team space or shared folder, access is improved but controls over naming conventions are critical. If emails are kept in public folders, then security issues need to be addressed as some messages may contain confidential information.

The advantage of managing messages within the email system is that all metadata relevant to the record is captured and preserved, and the messages are kept within a familiar environment, making it easier for staff to comply with filing requirements. There are disadvantages, however. For instance, email messages in an email system are not integrated with other relevant documents; as a result, parallel filing structures will develop, making it hard to find information and avoid duplication. Still, managing emails within the existing email system is a good interim solution, since staff can develop filing practices that will be useful in the future, if the organisation develops an ERMS system.

Saving Emails to a Shared Drive

Saving messages to a shared drive helps bring together all documents and messages relevant to a theme or activity in the same folder, which significantly improves corporate access to the organisation's records. This approach is close to the way in which email messages would be managed in an ERMS system. Unfortunately, the process of manually saving emails into a shared drive is often cumbersome and staff members are not always willing to comply. It is also important to clarify who is responsible for saving emails, since many messages are circulated widely within an organisation but only one or two people may have official responsibility for the business tasks associated with the message.

When saving emails into a shared drive, they can be saved in various formats. An .msg format is convenient within the Microsoft Outlook environment, but it is a proprietary format and therefore it may be more difficult to migrate documents to other systems later, if the commercial software is not available. An .rtf format is a

fairly standard exchange format, which will embed any attachments within the message body, but saving .rtf files takes more disk space and so can become more costly to maintain. Saving emails in .html format is not recommended; as mentioned earlier, the syntax used for .html may contain proprietary elements, and access the information might be limited if commercial software is not available.

When establishing procedures to save emails on a shared drive, it is important to decide whether to save attachments with the message or separately. There are differing opinions on the question but the general approach is to save the message and the attachments together when any significant information related to the topic is contained in the message itself. If the message is just a container for the attachment however – such as a message written to forward a report with the text 'here it is,' – then it is recommended that the attachment be saved and the email itself destroyed.

When saving email messages outside of the email system, transmission data, showing fields such as date of sending and receipt, recipients, subject title, should always be saved with the message text. However, as with printing to paper, some other metadata may very well be lost. As well, encryption tools should not be used when saving messages to a shared corporate drive, or access will be hindered.

Managing Records in a Hybrid Environment

As has been noted in this training programme, many organisations will continue to create both paper and electronic records as a normal part of their daily activities. Managing this hybrid record-keeping environment is normal and expected; it is unlikely that a purely electronic records framework will be found anywhere in the world in the near future. In order to coordinate the management of both paper and electronic records in a hybrid environment, the following few suggestions should be considered. Some of these have been raised elsewhere in this training programme but it is worth expanding on them here.

Linking Electronic and Paper Filing Systems

A shared network drive can usually be configured to reflect the paper filing structure so that electronic documents are stored in a manner comparable to their paper counterparts. This approach may be achievable by building a hierarchical 'folder within a folder' structure using Microsoft Windows, to simulate the structure of a paper file plan. As you investigate how to link electronic and paper filing systems, consider the following points.

- There is little point in building a paper-based structure in electronic folder form if the structure does not work well in the paper environment. Often, the implementation of an ERMS forces an organisation to rethink its paper filing systems, but even before an ERMS is contemplated it is worth looking closely at existing filing systems before copying them.
- Alphabetical folder titles are generally more usable in the electronic environment than numerical schemes. Using both letters and numbers together will produce very long folder titles.

- Paper filing systems tend to use long names. In a Microsoft Windows environment some of the file directory information might not be seen on the computer screen, making it difficult to identify and access records. As well, the longer the folder or file name, the more chance that it will exceed the limit allowed in a software application, making the document essentially unusable.
- If paper and electronic filing systems are coordinated, it is important to establish clear directions about who can create paper or electronic folders and who is responsible for ensuring that both the paper and electronic systems remain coordinated. Allowing everyone to create their own folders and files will eventually result in a break down of the systems.

Scanning Paper Records

It is sometimes desirable to scan paper records and retain the electronic copies as part of the electronic record-keeping system. Many issues need to be considered when developing a scanning programme, not the least of which is ensuring the quality, authenticity, and integrity of the record in electronic form. But first, the organisation needs to decide why it wants to scan records and preserve them digitally. Is the goal to save storage space? To save money? To provide improved access to information? The reasons for digitisation will determine what will be digitised and how. The following questions need to be answered when planning a digitisation initiative.

- Is the goal to save space? If so, the organisation should first ensure it has implemented an effective records management programme, one that moves records through the life cycle and destroys or transfers records regularly.
- Is the goal to provide improved access? If so, the organisation should ensure that the records to be digitised are worthy of long-term retention; if they are only going to be kept another few years, the cost of scanning will likely far outweigh any storage costs incurred. The organisation may also want to make any scanned text searchable by including optical character recognition (OCR) as part of the scanning process.
- Whether the purpose is to save space or improve access, the organisation must determine how the scanned records need to be 'profiled' so that they can be found. What naming convention will be used? What other data for accessing the records will be needed? How much of this data can be captured automatically and how much will have to be input manually?
- Are there any legal concerns associated with replacing paper records with electronic ones? The organisation needs to be able to confirm the authenticity and integrity of the scanned copies, and there may be legitimate reasons for retaining the originals instead of or as well as providing electronic versions.
- Are the paper-based originals suitable for scanning? If the quality of the electronic product is not high enough, the original may need to be retained for evidential or information purposes. It is important to test the scanning process before committing to widespread scanning projects, in case some records are not suitable and must be retained in their original form.

- What format should the electronic copies be kept in? If the integrity of the copies is to be maintained, they could be saved as PDF files or other unchangeable formats. But if the organisation wishes to use, alter or manipulate the records, then it may want to save them in a word processing format that allows changes. However, the organisation then needs to assess the implications for the authenticity and integrity of the original evidence.
- How long should electronic and paper copies be retained? Once a record is scanned, the organisation needs to clarify if the original will be destroyed immediately or if it will be kept for a certain time, if not permanently. The organisation will also have to determine which version will be considered the official record, if both are to be retained. Legal restrictions on the destruction of records must be identified so that the organisation does not breach any laws in the process of digitising records.
- How will the electronic record be made accessible? There is an increased risk of violating privacy and confidentiality when making any records available electronically, and the organisation needs to assess the privacy concerns and the access procedures to be used before deciding if it is appropriate to scan certain records in order to make them more widely available in an online environment.

If a scanning programme is established, the organisation needs to establish policies and procedures for how it will be managed. These policies and procedures should confirm that the organisation is complying with legislative and other requirements to ensure that the digitisation process results in authentic and trustworthy documents. Quality control and regular monitoring of the scanning programme is important to confirm that the process is operating as it should. The organisation may need to create a certification process, wherein certificates are scanned along with the originals confirming the technical specifications followed and attesting to the fact that the procedures are up to expected standards.

Good Records Housekeeping

Consistent and ongoing management of both shared and personal drives, and paper filing systems, is essential to maintaining the long-term viability of records. Staff members should be trained to review their records periodically and remove any non-official materials along with unnecessary duplications; ideally, they should be encouraged not to capture non-official materials in the record-keeping system in the first place. This housekeeping work is external to the application of formal retention and disposal schedules and so becomes an individual responsibility. The goal should be to reduce unneeded duplication of records while still ensuring good access to information for business purposes.

Procedures should be established to clean up unnecessary duplicates, working copies that are no longer required and documents with no continuing value. Staff should be reminded regularly to review their filing systems, their local drives, personal work spaces and other paper or electronic work areas and reduce as much clutter as

possible. They should also be reminded regularly not to use their local or personal drives for the long-term storage of official corporate documents.

The next unit examines issues involved with appraising and disposing of electronic records and outlines the steps involved in establishing and implementing a formal appraisal programme. The unit also addresses the creation of retention and disposal schedules for both electronic and paper records.

UNIT 3.3

APPRAISING AND DISPOSING OF ELECTRONIC RECORDS

The appraisal and disposal of electronic records is essential to the sustainability of a quality ERM programme. Preserving valuable records and destroying obsolete ones ensures that only necessary records are retained and saves the organisation time and money. While the focus in this unit is on the appraisal of electronic records, the purpose of appraisal remains the same for all records no matter their medium. Appraisal involves determining what records exist or will be created; who creates them and why; how they relate to the organisation's business functions; and how, when and by whom they are used, and then deciding which records have enduring value and which can be removed once their immediate usefulness is at an end.

This unit examines the nature and importance of appraisal and then outlines five steps involved in carrying out effective appraisal and disposal actions. The discussion focuses on an appraisal exercise for a specific body of electronic records, but the steps should also be used when carrying out appraisal in order to develop a retention and disposal schedule. After the steps involved in appraisal are examined, the unit includes information about how to develop a retention and disposal schedule, which should govern the ongoing management of records and their disposal, either as archives or as candidates for destruction.

When to Appraise?

Traditionally, paper records were appraised long after they had been created, used and stored. Indeed, it was common to wait 30 to 50 years or more after records were created before deciding whether or not to retain them permanently. Fortunately, paper-based records are 'neglect tolerant' and can, within reason, withstand the environmental dangers associated with storage, such as fluctuating temperature and humidity, damage from dust or vermin and excessive light levels, for limited periods.

Electronic records are unlikely to survive neglect, and it is not possible to wait decades before deciding what to keep and what to destroy. The technology used to create the records may become obsolete in one or two years, if not sooner, and so it is imperative that decisions be made about which electronic records should be kept at the time they are created, if not before.

Ideally, therefore, appraisal and disposal activities should be built into the normal practice of records management, becoming as routine a procedure as possible. Non-systematic appraisal work – perhaps done in response to poorly planned office moves

or the last-minute rescue of records from garbage bins – will interfere with the quality of the appraisal and will, therefore, hinder the work of preserving quality records. The success of appraisal of electronic records depends on the active involvement of records professionals. As noted above, a records retention and disposal schedule should be created as a central tool in managing the ongoing disposal of electronic or paper records. However, it is often necessary to carry out a one-time appraisal exercise for a select group of records or for all the records in the organisation, either to clear up a backlog of records or to lay the groundwork for the creation of a formal electronic records management programme.

Appraising records for enduring value is a complex process, and many different archival appraisal theories exist around the world. In general, however, it is agreed that, in an electronic environment, micro-appraisal of individual folders and documents is no longer a reasonable approach. There are simply too many records and the risk of loss is too great to allow the time required to carry out such minute analysis. Instead, the best method for appraisal of records – both paper and electronic – in a modern office environment is a macro-appraisal approach, based on an analysis of the functions and activities of the creating agency, a process called 'functional appraisal.'

Functional appraisal involves assessing the enduring value of records by determining the functions of the body to be documented, identifying who created records in order to carry out those functions and then selecting the records that provide the most complete and concise documentation of those functions. Functional appraisal is currently considered the best way to appraise large volumes of records, no matter the medium in which they were created, in a way that minimises potential bias and encourages the preservation of those records that provide the most complete and concise picture of significant organisational functions.

Appraisal as a Risk Management Activity

If records creators and archival institutions had all the time, money, employees and space in the universe, then no records would ever need to be destroyed. However this is not the reality, and so archival institutions, in collaboration with record creators, need to make rational and informed decisions about what to keep and what to remove. How can records professionals implement this type of risk management in an informed, effective and accountable manner?

The greatest risk electronic records face is the risk of being altered, manipulated, overwritten or destroyed, resulting in an inauthentic and unreliable record or, worse, no record at all. This risk is compounded by the prohibitive cost of maintaining all the technology and expertise needed to retain electronic records in their original form. The changes in computers and information systems happen far too quickly to allow organisations the luxury of keeping 'old' computers just so they can access electronic records in their original configuration, especially when a large percentage of those records are not worth preserving for the long term.

Who is Responsible for Appraisal?

Developing clearly defined responsibilities for appraisal and disposal activities is essential to ensuring successful records management, no matter the form of the records. Traditionally, appraisal and disposal activities were divided, with the records manager determining the time frame for semi-active retention and the archivist determining the final disposal. Now, in the electronic records environment, it is practical for the records manager, archivist, information technology specialist and records creator to work as a team, in order to bring a range of expertise to the process of deciding which records need to be kept and which can be destroyed.

- The records creator brings knowledge of the day-to-day use of records and their importance to the organisation's business.
- The information technology specialist can advise on changes to electronic systems and best practices in IT operations.
- The records manager supports the ongoing evidential and informational needs of the organisation and can balance the user's needs for records against the resources available in order to make solid judgements about records retention.
- Archivists have the long-term management of the records in mind and are responsible for ensuring authentic and reliable records remain accessible over the long term.
- Lawyers, auditors, compliance specialists and other subject experts can also contribute important insights during the process of appraisal.

These stakeholders – along with any other appropriate representatives of the organisation – should be involved in any appraisal exercise, and their different responsibilities and areas of authority should be clearly defined and formalised in appraisal policies. The archivist may be the primary appraisal specialist, but he or she should draw on the expertise of others in the organisation throughout the process.

Documenting Appraisal and Disposal

No matter who undertakes appraisal and disposal work, documenting all decisions and actions is essential to ensure the organisation remains answerable for its actions and to guarantee that detailed information is available about all work performed. Documentation provides audit trails for important decisions, which render governments accountable to the citizens they serve. As well, future records professionals may need to revisit appraisal decisions, and documentation is essential to reconstruct the reasoning and logic used in making disposal decisions.

Documentation of appraisal and disposal actions can also be valuable for other purposes, such as the creation of archival descriptions and finding aids, and the development or revisions of records classification schemes. Documentation also provides analysis and information related to the authenticity and preservation of electronic records that may be critical for their long-term care.

To clarify the different types of documentation that may be created, special mention is made throughout the rest of this unit of the different types of documentation that can be generated as part of an accountable and transparent appraisal process.

Appraisal Step 1: Conducting Research

Any appraisal decision must be based on solid information and research. A critical first step is to gather and analyse as much information as possible about the records' context of creation and use, as well as information about the records themselves. Information about the juridical, organisational and procedural contexts of the records can be gathered by referring to materials such as procedure manuals, mission statements, business process rules, annual reports, websites, legislation, and other publications. Information about the technological context of electronic records is also critical for good appraisal decisions. It may be easier to gather information about the electronic records when they are still 'live' in the system, as system manuals and user guides are more likely to be available from the record creators.

The appraiser may also gather information by interviewing staff members who create and use the electronic records as part of their work. Interviews would help to identify what tasks people perform, the extent of their responsibility and authority, the kind of records they create and use and the relative value they place on different types of documentation. When conducting interviews, it is a good practice to use a predefined interview protocol so that information can be gathered in a consistent manner, allowing for easy comparison among the different responses received. This comparison helps identify areas where issues or concerns are similar and can also highlight areas of contradiction. During research, additional information can be gathered by examining the records within the electronic system itself, and by witnessing and recording the interaction of office workers with the electronic systems used to create and hold records.

Information about the technological context of the electronic records is also required. A technical analysis involves identifying the elements or components making up the records and the hardware and software environment, documenting the way in which the records are organised and assessing how records are stored and for how long. As well as providing useful information for appraisal, the technical analysis also lays the foundation for the development of the technical documentation that will be needed later, to understand what threats affected the records and what security was in place to protect them from those threats, and support wider access to and use of the records.

Documentation from Step 1

Following is the key documentation resulting from the research conducted in Step 1.

- A compilation of all contextual information gathered from the records creator and from outside sources.
- A technical analysis.
- Notes, transcriptions or audio / video recordings of interviews with staff.

Appraisal Step 2: Determining Value

The appraisal team uses the information and research gathered in Step 1 to determine the value of the records throughout the life cycle: in the active, semi-active and inactive phases, in order to determine how long the records should be retained. Once the value of the records is assessed, those precise retention periods can be assigned and a retention and disposal schedule can be developed, using the records classification scheme as the basis.

Assessing the Business and Accountability Value of Electronic Records

In assessing the value of records to determine their retention for business and accountability purposes, the appraisal team may ask questions such as:

- Why and how does the records creator use the electronic records?
- How long does the records creator need the records in order to conduct business?
- What legal requirements must the record creator meet with regard to the protection or use of electronic records?
- Might the records be needed for audit, quality control or other evaluation purposes? If so, for how long might such needs continue?

The answers to these questions will come from a careful analysis of the organisation's legal, financial and business requirements as well as a review of the organisation's current information needs.

Determining retention periods for business purposes is relatively easy: they should be kept accessible for as long as the creator or user reasonably needs them. It is worth noting, however, that many users are reluctant to accept that their records can ever be destroyed, believing that they will 'always' need access to them. A difficult but important task is to assign a reasonable period for retention and convince staff members that this is appropriate.

Determining retention periods for accountability purposes is a more complex process, and decisions will vary from one organisation to another. Research into the legal and juridical environment of the organisation will be critical.

Assessing the Archival Value of Electronic Records

Besides meeting the legal or operational needs of the organisation, a decision needs to be made about whether records need to be preserved for posterity. Questions to ask include

- Are the electronic records valuable enough to society to have enduring value?
- What will be the final disposition action for electronic records? Will archives be sent to an archival institution for preservation or preserved internally using the organisation's own facilities and resources? How will obsolete records be destroyed?

These are the same appraisal questions that should be asked when assessing the value of traditional manual or paper-based records. The challenge with electronic records

preservation is ensuring the technological capacity is available to carry out the decisions and protect the records for the long term.

Determining Authenticity and Integrity

The appraisal of electronic records must include an assessment of their present authenticity and an analysis of whether and how they can be preserved with their authenticity intact. Electronic records are more easily altered, manipulated and overwritten than records on traditional media, and therefore their integrity may be compromised. The integrity of electronic records is most at risk when they are transmitted between people, organisations or software systems.

A presumption of authenticity can be made by examining the elements of electronic records, their associated metadata, and their contextual environment: how, when and why they were created and used. The electronic records themselves should contain all the elements they need in order to be relied upon as evidence within the juridical and organisational environment. For instance, an email with no information about who sent the message, who received it or when it was transmitted has lost its authenticity. Important though the information may be, the record is unlikely to be accepted as evidence in court and cannot be relied on to prove or disprove any action or claim. The need to ensure authenticity is one of the reasons capturing metadata is so important to preserving valuable electronic records.

Similarly, many legal requirements exist for creating and issuing deeds for the sale and transfer of land. If an electronically generated land deed did not contain the date of sale or the precise location of the land in question, could the record be relied upon as fact? Additionally, if the format of the land deed did not conform to juridical requirements – for instance, if it could not be proved that the document was an official record generated by the Land Office – could one confirm that the record was indeed issued by the proper authority?

Risks to the identity and integrity of the electronic record (and therefore, its authenticity) occur when the required elements are not included in the record or are lost during creation, use or storage. An electronic records system that does not capture adequate metadata and other important components of the electronic record will put the authenticity of the records at risk and will not allow the records in the system to stand as reliable evidence of the agency's work.

If, however, all the required elements of the record exist, the archivist may then make a strong presumption of authenticity. Therefore, identifying the required elements of the electronic record and discovering how they are expressed in the electronic system is critical when assessing the authenticity of the electronic records.

The European Commission's *Model Requirements for the Management of Electronic Records* (*MoReq2*), the *Victorian Electronic Records Strategy (VERS)*, the UK National Archives' *Requirements for Electronic Records Management Systems* specification, and the *International Research on Permanent Authentic Records in Electronic Systems (InterPARES)*, among others, have identified and defined requirements to determine the authenticity and safeguard the integrity of electronic

records. Readers will want to consult the resources identified at the end of this module for more information.

> See Module 4 and the *Additional Resources* tool for more information about electronic records research projects underway today.

Assessing Electronic Records Systems

A high presumption of integrity for electronic records can be made if certain conditions exist in the system used to create and house the records, including clearly defined and fully implemented procedures for

- controlling access to records
- preventing the loss or corruption of records
- preventing media deterioration or technological obsolescence
- carrying out regular audits of the electronic system.

When assessing the context of the electronic records system, the appraisal team should attempt to answer the following questions.

- How is access to the system controlled? Who has or had access and what level of access did they have?
- Does the electronic records system use passwords and other means to control access?
- What are the file formats used? Are the file formats still compatible with the current technological environment or do records exist in file formats that are obsolete or unsupported?
- What storage media are used, where is the storage media located and is this location secure?
- Have the electronic records been transmitted from another agency or outside organisation, and how?
- Has there been any other break or change in the chain of custody? How and why?
- Have the records been migrated into a new hardware or software environment? When and how?
- Are the records inactive and, if so, how long have they been so?

The answers to these questions will help the archivist assess the organisational and technological context surrounding the records and help reveal whether the records can be considered authentic and reliable.

Determining the Feasibility of Preservation

When considering the archival value of electronic records, another question the appraisal team must consider is whether it is feasible to preserve the records for the long term. Preservation is expensive and time consuming, and it is an ongoing responsibility – as technologies change, preservation approaches must also change.

To determine the feasibility of preserving electronic records, the appraisal team can use the information about the technological context of the electronic records that was gathered in Step 1 to analyse the current hardware and software environment. During a technical analysis, the archivist must examine how the records are created in the computer and how they are saved.

Once this research is completed, the archivist must then determine whether the organisation – either the creating agency or the archival institution – has the ability to preserve the electronic records. Questions to ask include

- Does the organisation have the financial resources needed?
- Does the organisation have the appropriate technical equipment?
- Does the organisation have the technical expertise and knowledge?
- Is the organisation committed to maintaining these records indefinitely?

To gather this information, the appraisal team may need to compile information from budget and equipment personnel and conduct interviews with upper management.

If it is deemed to be too difficult or costly to preserve the electronic records properly, a decision may be made not to transfer the records to an organisational electronic records storage facility or to the archival institution. If these electronic records are deemed to have enduring value, other steps must then be taken to preserve them, such as exporting them to print or to a specifically designed report format. However, the value of the electronic records for legal, organisational, financial or informational purposes may be so high that it is necessary to invest in the equipment and services required to ensure long-term preservation.

Documentation from Step 2

Following is the key documentation resulting from the research conducted in Step 2.

- A technical analysis detailing the components of the electronic records and the controls needed to ensure that electronic records will not be tampered with or otherwise altered. The technical analysis also includes analysis of the formats of the records and identifies possible preservation and / or access formats.
- A list of the types of hardware and software needed to access and view the electronic records.
- Information about the archival institution's ability to preserve electronic records, such as annual work budgets, staff profiles, equipment lists, information from upper management and similar documentation.

Appraisal Step 3: Making an Appraisal Decision

After assessing the value of the electronic records being appraised, at the point when they are being considered for transfer a decision needs to be made either to preserve the records or destroy them. The options are as follows:

1 If the records are no longer found to have enduring value, they will be destroyed.

2 If the records are found to have enduring value, if it is reasonable to assume that they are authentic and if long-term preservation is feasible, the records will be preserved.

3 If the records are found to have enduring value, but there is some question of whether or not they are authentic, or if preserving the records will require extraordinary efforts or expenditures, the appraisal decision must be made through a case-by-case analysis.

In the last situation, the archivist may determine that it is appropriate not to preserve the records, given the resources required to ensure their protection. On the other hand, the archivist may determine that the records should be retained because, for example, legislation requires that the records be preserved for the long term. Protecting the records may be necessary, even though the actual preservation mechanisms are not yet in place.

In addition to making the final appraisal decision, the archivist must specifically identify, in writing, which electronic records and other components in the electronic system (such as metadata profiles or other information) must be transferred along with the records, and which electronic records and other components must be disposed of. It is imperative that those components needed in order to implement disposal be clearly identified. (Disposal is examined below in Step 4.) The same authorisation is required if the records are to be destroyed.

Creating a Retention and Disposal Schedule

A valuable tool for records management is the records retention and disposal schedule, which identifies how long records within different series should be retained and whether they should ultimately be kept for their enduring value or destroyed as obsolete. The retention and disposal schedule is a central document in any records management programme, whether for paper or electronic records. It is generated out of the process of appraisal and draws on the information provided in a classification scheme.

Disposal schedules have four functions.

1 They identify all the records of an agency, irrespective of medium and format, including those created in the private offices of ministers or senior officials, as well as confidential and secret records created elsewhere.

2 They document decisions about the length of time records need to be retained because of their continuing utility to the creating agency (retention periods).

3 They document decisions about the appropriate disposal action to be taken at the end of retention periods (such as destruction or retention as archives).

4 They confirm that disposal actions have been authorised by appropriate agencies.

The core of a retention schedule is the date or time period for retention. This information triggers the ultimate disposal of the records. For example, the retention rule for a series of electronic payment vouchers might indicate a destruction date of six years after the end of the fiscal year in which the payment voucher was issued. This metadata should break down into different elements:

1 The retention trigger, which might be the end of the fiscal year in which the voucher was set aside. The retention trigger is the date that the system uses to begin 'counting down' to the end of the retention period.

2 The retention period, which in this case might be six years. The retention period is the amount of time before the final disposal action.

3 The final disposal action, either to retain records permanently or destroy them: in this case the disposal action might be to destroy the records.

These three metadata elements would be required in order to execute the retention and disposal rule.

In electronic records systems, retention and disposal metadata can be applied to a whole series of records by linking retention information to the classification scheme. This functionality is one reason archivists and other records professionals need to be involved in early in the development of electronic records systems, so that they can support the development of classification schemes and retention and disposal metadata before records are created within the system, saving time and effort and improving the management of and access to records.

Some retention triggers do not always work for all records in an electronic records environment. For example, trigger dates that are defined by chronological time and expressed as a date within the year (e.g. 31 December 2007) are easily implemented into electronic systems because they can reference the time/date clock function of most computer systems. However retention triggers not defined by chronological time, such as those defined by events, can be more difficult to implement. For example, event triggers such as 'end of project,' 'after application acceptance,' or 'after termination of lease' cannot always be calculated or entered automatically. Instead, someone has to manually enter the information in the metadata profile of the record.

Additionally, a record may be created in the electronic system before the exact date of the event trigger is known. For example, electronic records created for a construction project might be scheduled for disposal ten years after the end of the project. When the records are initially set aside in the electronic system, the records creator may not know precisely when the construction project will end, making it impossible to computerise the retention process. In such instances, event triggers should be monitored by a responsible party outside the electronic environment to ensure that the

retention and disposal metadata is complete and that the electronic system can execute the disposal command using accurate metadata.

For computer systems that do not have records retention and disposal functions, the archivist or records manager will need to create procedures for the scheduled disposition of records. Using the electronic payment voucher introduced above as an example, the business processes for disposing of those documents would generally proceed as follows:

1 The series of electronic payment vouchers are assigned a retention period of six years after the fiscal year in which the vouchers were issued. They are deemed to have no enduring value after that retention period has expired.

2 Six years later, the records manager identifies the payment vouchers that were set aside six years before.

3 Once the records have been identified, the records manager confirms that that correct records have been identified and oversees their destruction through complete deletion from the system.

Types of Retention and Disposal Schedules

A general retention and disposal schedule is one that applies to categories of records common throughout all or most agencies of a government or business. Such schedules will cover a large proportion of the records generated by individual agencies. The records concerned will be mainly administrative or housekeeping records, that is, records related to general administrative activities common to all organisations within the larger government or business, such as financial management, facilities and equipment, human resources and payroll.

A specific retention and disposal schedule identifies the retention and disposal criteria for records created to support a specific business function. Examples might include environmental management, health care, manufacturing or another core responsibility of the organisation.

Figure 6 provides a sample records retention and disposal schedule, illustrating retention periods for certain records. The example used relates to the office of the Director of a non-profit organisation. The types of records created in a small agency such as this are similar to records created in the offices of managers and small business owners. Figure 7 shows a sample retention schedules for a larger government office; government retention schedules are often more complex than those for smaller organisations but the basic information conveyed is the same.

Figure 6: Sample Retention and Disposal Schedule from a Non-Profit Organisation

Extract from the Office of the Executive Director of a Non-Profit Organisation

Definition of Codes:

A = active	s = documents to be replaced when superseded
S = semi-active	+ = documents to be kept for that many years after the file is closed
D = disposition	a = archival records
P = personal information	o = obsolete records to be destroyed
V = vital record	

FILES	A	S	D	P	V
Annual Report records					
draft versions	1		o		
final version	2	6	a		
Board of Directors' records					
agendas	2	6	a		✓
member lists	2	6	a	✓	
memoranda	2	6	a		
minutes	2	6	a		✓
policies	2	6	a		✓
policy correspondence	2	6	a		
procedural correspondence	2	6	o		
Project files					
applications for funding	1+	6	a	✓	
contracts	1+	6	a		✓
contract correspondence	1+	6	a		
financial correspondence	1+	6	o		
funding records	1+	6	a		
Conference attendance					
correspondence	2	6	a		
registration information	2		o		
speeches	2	6	a		
travel arrangements	2		o		
working notes	2		o		

FILES	A	S	D	P	V
Financial records					
interim accounts	**2**	**6**	**a**		✓
annual accounts	**2**	**6**	**a**		✓
auditing information	**2**	**6**	**a**		✓
draft budgets and accounts	**2**	**6**	**o**		
financial reports	**2**	**6**	**a**		
tax returns	**2**	**6**	**a**		
Insurance information					
claims correspondence	**2**	**6**	**a**		
insurance policies	**2**	**6**	**a**		✓
legal information	**2**	**6**	**a**		
sales information	**s**		**o**		
Payroll records					
government requirements	**2**	**6**	**a**		
payroll policies	**2**	**6**	**a**		
payroll statements	**2**	**6**	**o**		
Personnel records					
individual employee file	**2+**	**6**	**a**	✓	
job descriptions	**2**	**6**	**a**		
employment applications	**2**		**o**	✓	
vacation information	**2**	**6**	**o**	✓	
Professional associations					
committee records	**2**	**6**	**a**		
general correspondence	**2**	**6**	**a**		
membership information	**s**		**o**	✓	
procedural documents	**s**		**o**		

Figure 7: Sample Retention and Disposal Schedule from a Central Government

Extract from a Government Office, for Management of Records Related to the Records Management Function

RETENTION AND DISPOSAL AUTHORITY: RECORDS MANAGEMENT FUNCTION

This authority governs the retention and disposal of records relating to general records management issues and functions not identified in other records management-related retention and disposal authorities. This authority includes the general includes general records management standards, procedures and guidelines.

Definition of Codes:

A = active
S = semi-active
D = disposition
P = personal information
V = vital record
s = documents to be replaced when superseded
+ = documents to be kept for that many years after the file is closed
a = archival records
o = obsolete records to be destroyed

Records Series	A	S	D	Personal	Vital
Policies, standards and procedures	s	5+	a	no	no
General communications	current year + 2	0	o	no	no
Vital records management	s	0	a	no	yes
Records preservation procedures	current year + 2	0	o	no	no
Records management requests for information or access	s	0	o	no	no
Records management strategic plans	s	5+	o	no	no
Emergency response / business continuity plans	s	5+	o	no	yes
Training and orientation	s	0	o	no	no
Retention and disposal schedules	s	5+	a	no	no

Documentation from Step 3

Following is the key documentation resulting from the research conducted in Step 3.

- An appraisal report should detail the appraisal methodology and the criteria used. Also the evidence supporting the archivist's presumption of authenticity; the feasibility of preservation; and the lists of records series that have and have

not been selected for preservation. The report should conclude with a recommendation that the records be preserved or destroyed.

- If necessary, a formal agreement detailing the terms and conditions of disposal. (This documentation may not be necessary if there is an organisational policy or by-law that sets out the general terms of transfer.) The agreement includes the identification of persons responsible for implementing the decision; the timing and frequency of disposal activities; the analysis of native formats and identification of possible preservation and / or access formats as determined in the technical analysis; and other procedural information.
- If appropriate, a records retention and disposal schedule, including a technical analysis of the computer requirements for maintaining, preserving and disposing of records.

Appraisal Step 4: Implementing the Decision

All of the work performed as part of Steps 1, 2 and 3 will aid the person responsible for implementing the disposal decisions, which is best carried out for series of records, not for individual folders or files. Implementation involves two actions: destroying unwanted records and preserving valuable records.

Destroying Records

If records have been appraised as having no long-term enduring value, then they may be destroyed at the end of their life. For paper records, destruction means to physically destroy the record, by shredding, burning or otherwise obliterating the records' medium. For electronic records, destruction can be much more complex. It is not simply enough to erase the records from a computer directory. It may also be necessary to identify and destroy the components and metadata associated with the electronic record. Technical expertise may be required to ensure this destruction is carried out. It is also necessary to maintain an audit trail of the destruction process.

While the technology available in different organisations will vary, the general principle of destruction remains the same: every attempt should be made to ensure that data cannot be recovered by reasonable efforts. The security or sensitivity of the information should be used to determine what constitutes 'reasonable.' The only exception is the documentation generated by the destruction process itself; that documentation – which should include a description of the records destroyed and the means by which they were destroyed – should be retained as evidence of the act of destruction.

The usual steps involved in destroying electronic records are as listed below.

1 Identify records that have no enduring value.

2 Confirm that the records are going to be destroyed or otherwise disposed of according to the formal agreement between the preserver and the records creator.

3 If the records are to be destroyed, destroy them completely.

4 Analyse the steps taken to ensure compliance with all requirements.

5 Complete the destruction report and submit it to the appropriate authorities within the organisation.

Transferring Records

If records are appraised as having long-term enduring value, then the records will be transferred to the chosen archival facility, whether that is a separate archival institution or a permanent storage facility within the organisation. The appraisal research and technical analysis conducted in Step 2 and the formal agreement on the terms and conditions of transfer in Step 3 will indicate how the records should be transferred into the custody of the archival institution and in which format(s).

The assessment of preservation requirements conducted in Step 2 will provide valuable information about how the records need to be prepared for transfer. It is a good practice to transfer electronic records in both their original, native format and, if necessary, as a reformatted version (a copy). Keep in mind that the technical analysis may have identified the need for two reformatted versions: one for long-term preservation and another for access purposes.

The process of reformatting electronic records for the purpose of transfer must be fully documented in a transfer report. The transfer report should also include the following information:

- a list of the electronic records selected for transfer
- information about the electronic records' native format(s)
- a description of the preservation and / or access formats used
- information about how the electronic records were copied and reformatted.

This information will be critical for carrying out later work with the records, such as arranging and describing archives, preserving files and providing access to records. The archives must maintain the record of what was done to the records, if and how they were altered and what elements or components made up the electronic records before they were transferred.

In general, the steps in the transfer process are as follows.

1 Identify records that have enduring value and will be transferred to the archival institution.

2 Determine the format in which those records will be transferred: options include the native format, another preservation format or an access format.

3 Copy and, if necessary, reformat the records to be transferred.

4 Prepare transfer documentation, including a detailed list of records to be transferred; information about file formats used; and any technical documentation needed to support access and preservation.

5 Transfer records and documentation to archival custody.

6 Confirm the successful transfer of records.

7 Delete the records from the source system.

As can be seen, the process of transferring records alone involves complex technological support, which is why the records professional must work with a team of experts, including information technology specialists, in order to achieve effective records care in an electronic environment.

Documentation from Step 4

Following is the key documentation resulting from the research conducted in Step 4.

- Destruction report.
- Transfer report.

Appraisal Step 5: Monitoring Appraisal Decisions

As should be clear throughout this unit, it is vitally important that archivists and other records professionals be involved in the development and implementation of electronic records systems as well as in the appraisal of electronic records. Appraised records should be monitored for the following situations.

- Unexpected changes in business processes can affect how electronic records are used by action officers.
- Minor changes in the software and hardware environment made after the system has been implemented may affect authenticity or alter preservation options.
- Major changes to the software and hardware environment may place records at risk of loss or damage.

In addition, it is not possible to demonstrate the authenticity of records or assess the potential for preservation before the records have been created. Consequently, monitoring operations may lead not only to small changes in appraisal documentation, but also, sometimes, to more significant changes in the overall appraisal decision.

Documentation from Step 5

Following is the key documentation resulting from the research conducted in Step 5.

- Amendments or additions to any of the documentation generated in Steps 1 to 4, such as the appraisal report, technical analysis, terms and conditons of transfer, records retention and disposal schedule or other reports.
- If needed, documentation that provides a rationalisation for a new appraisal, such as when major changes to the technological environment have rendered the prior appraisal work inaccurate. This documentation would form the background for new appraisal reports.

The next unit examines the steps involved in developing and implementing access policies in an electronic record-keeping environment, in order to provide quality access to information and records, particularly within the public sector.

UNIT 3.4

DEVELOPING ACCESS POLICIES IN AN ELECTRONIC ENVIRONMENT

Access to government information is seen as a right in many countries in the world today, but this has not always been the case. Access to government records and to the information they contain used to be seen as a privilege for public servants and the executive arm of government. Members of parliament and the public relied on the government to inform them of decisions and actions; only those involved in the process of governing had direct access to the records they created and used. In the 1970s and 1980s, however, increased concern for democracy and human rights led to calls for accountability and transparency, and governments around the world began to enact legislation allowing the public to access government information more widely.

'Access to information' or 'freedom of information' legislation allowed the public much greater access to records than they had ever had before. People did not have to wait until records attained archival status before they could see them. In other words, members of the public could seek access to records even while those records were needed for the daily administration of the creating agency. The challenge for records professionals is finding a way to provide public access while still ensuring organisations can carry out their daily business without interruption. Records professionals also have to address growing concerns for privacy, in order to ensure that personal and confidential information is not inappropriately disclosed whenever public records are made available.

This unit examines the concept of access and the importance of developing sound and effective access policies for electronic as well as paper records, particularly in the public sector. While the unit focuses on providing access in an environment governed by formal access and privacy legislation, the principles of providing access and respecting privacy should be the same regardless of the nature of legislative frameworks in the jurisdiction in question. The unit also examines issues related to who should access which records and under what circumstances. It includes a discussion of the importance of regulating and monitoring access, and it addresses the role and scope of access policies. Even though the emphasis in this training programme is on the management of electronic records, the principles of access and privacy should apply to the establishment of access policies and procedures regardless of the form of record.

The Concept of Access

The international standard for records management, ISO 15489-1: 2001, defines access as the 'right, opportunity, means of finding, using, or retrieving information.' According to this definition, access can be a right or an opportunity, depending on the circumstances.

The right to access to information is usually derived from constitutional guarantees pledging a government's desire and commitment to provide citizens with access to official records. The right is normally implemented through an enabling legislation in the form of freedom of information, privacy, and national archival laws. Access is also an opportunity. Access to records and information allows members of the public, as well as public servants, the judiciary, the executive and the legislature the opportunity to learn about issues emerging from the governance process.

In order for information to be used, it has to be located, but at the same time, personal, confidential or sensitive information needs to be protected so that people's individual rights to privacy are not violated. Protection is also needed in order not to circulate information that legitimately ought to be withheld. Of particular concern may be the protection of

- intellectual property and commercial property rights
- financial information
- information important to state security
- legal and professional privileges.

The right to access information becomes enforceable when legislative and regulatory frameworks are in place in a country or region. Freedom of information, privacy laws, national archive and records laws and other laws govern the scope of access and privacy, meaning that the task of providing access will be managed differently in different jurisdictions.

The Relationship between Access and Records

Access to information frequently means, in reality, access to records. Without documentary resources, public bodies cannot answer questions or provide information for the public. Since many access laws establish time limits on the provision of information, finding information is critical to complying with access legislation. Even without such legislation, finding information in order to provide information to the public is and should be a central responsibility of any government or publicly accountable organisation. Therefore, effective records management is an essential tool for ensuring that agencies can find the right information at the right time, with minimal expense.

Access to the records of government is particularly important – more perhaps than the records of a private organisation – because they can contain so much information directly relevant to the rights and needs of citizens and the public. Consider this list of public records, shown in Figure 8 below, which identifies some of the types of records created by governments in order to provide vital services and support to people:

Figure 8: Types of Public Records

- birth records
- national identity records
- immigration and citizenship records
- election registration records
- medical records
- land allocation and ownership records
- residential and property records
- vehicle licensing records
- driving licence applications
- employment records
- social security records
- pension fund records
- police records
- court records
- vital records
- business records
- accounting records

Public records such as these provide both information and evidence. The information provided in these and other government records informs citizens of all transactions performed in their name. Information in records also enables public officials to take action, to fulfil their obligations and perform their duties. The evidence in these and other records provides proof of, for example, individual rights, public commitments, government obligations, personal ownership and the right to citizenship. The records document how, and how well, government is operating and whether it is acting in an accountable and responsible fashion.

As discussed earlier in this training programme, in order to serve as both information and evidence, records must be authentic, reliable and trustworthy; they need to be protected against unauthorised change or destruction and they need to remain accessible and usable for as long as the public needs them. In the electronic records environment, providing access is dependent on ensuring the records are well managed from the time they are created, if not before.

Everyone can benefit from access to records; having valuable information at hand allows people to carry out their daily work, to confirm their rights and responsibilities, to buy and sell property and other items, to vote in elections, to provide and receive services, to provide informed consent to procedures or actions, to defend themselves in a court of law, to conduct research or to pass on information about themselves to their children or grandchildren.

Access-related Legislation

Despite the great benefits of access to information, it is important to respect the reasonable privacy rights of individuals and organisations when deciding what information to release and what information should be kept from the public eye. Regulating access to records, therefore, is necessary in order to protect some information from unauthorised access and disclosure. In order to manage the process of providing access, many jurisdictions establish regulations, laws and policies related to information, records, access and privacy. Some of the different types of legislation that may be enacted are described briefly below.

Constitutional Guarantees

Normally, a country's national constitution guarantees citizens access to government-held information, including records. Constitutional guarantees do not identify in detail the types of information that may or may not be made available, and they do not specify the institutions that will provide that access. Instead, constitutional guarantees present a basis for creating more specific laws and policies about access to information.

National Archives Laws

National archives laws usually serve two purposes. First, they establish the institution called the national archival repository or national archives. Second, they provide a framework on which citizens can gain direct access to those records that have been preserved for their archival value.

Traditionally, archival legislation created in a paper-based records environment normally declared that records were identified as archival through the process of appraisal; usually, such records were not moved to archival custody until the transfer date assigned in appraisal reports or retention and disposal schedules, which may be 20 or 30 years or more after the record was closed and removed from active use in the business area.

With the advent of access legislation, some archival laws have had to be changed to address the importance of providing access to records even while they are still in daily use. Thus the focus of archival legislation has turned from a historical, cultural role for an archival institution to an administrative role, as the agency responsible for providing quality records management throughout the public service. New and revised archival legislation can govern

- the creation of records, including determining access conditions from the time records are created
- the maintenance of records, to ensure access continues as records move through the life cycle
- the disposal of records, to ensure that those records worthy of permanent preservation are protected and accessible as archives.

National Security Laws

Access to records can also be restricted in order to protect national security, as identified in national security laws. These laws often provide broad exclusions preventing access to certain classes or groups of records, such as information related to the military, international affairs and defence, customs and immigration, border control, communications infrastructures and so on.

Public Service Laws

Public service laws regulate the conduct and operation of the public service. Some of these laws have clauses forbidding public servants from disclosing official records and information without appropriate permission.

Freedom of Information / Access to Information

Under most freedom of information laws, access to records is a right which everyone is free to exercise. Through these laws, citizens can seek direct access to the records of a government agency. Usually, access laws prescribe time limits within which access to records must be provided: sometimes the time frame is as short as 30 or 60 days from the date the request was received.

There are certain exemptions and exclusions to the right to access, however. Examples of records that might not be freely available include

- information obtained in confidence
- information about ongoing law enforcement or investigations
- information that, if released, might compromise the safety of individuals or the economic interests of the jurisdiction
- advice provided to government agencies if that advice has not otherwise been made public
- information about testing or audits if those tests or audits have not been completed.

Privacy Laws

Privacy laws protect and regulate access to records involving specific individuals. Such laws are usually based on the following two principles.

- Individuals have a right to limit any access to, use of or dissemination of information directly related to them.
- Individuals have a right to inspect and correct any information about them found in organisational records.

However, access to these records may be provided if the information is needed for law enforcement, to conduct audits, to investigate fraud or other offences or if it is officially requested by a court of law.

Public Access in an Electronic Environment

Providing public access to and protecting the privacy of information in electronic records can be more challenging than providing access to information in traditional paper records. The value of records changes over time, and public interest in different subjects rises and falls depending on political, social or other imperatives. As well, finding and retrieving electronic records can take place quickly – if adequate records management controls are in place – but at the same time it is more difficult to ensure that electronic records are not at risk of inappropriate disclosure, unwanted duplication or inadvertent destruction.

The following are some of the issues that might need to be considered in order to provide public access to records in an electronic framework.

- How will access be affected by any changes in the technologies used to create, manage and store electronic records?

- When providing access to electronic records, how will the organisation distinguish between multiple copies of or versions of one 'record'? Will it decide that one version should be considered the appropriate record for public disclosure, or give access to all versions?
- What hardware and software will be needed to provide access to electronic records, and will new systems or approaches be required to provide public access as distinguished from organisation-wide access to electronic information?
- How will the organisation protect the authenticity of electronic records when providing access? Will records be 'certified' as traditional paper records often are?
- Will the organisation charge for access to electronic records? What about charges for providing print copies of records?
- Will the organisation allow the public to file access requests electronically? What records will be required to document and track such access requests?
- Will the organisation establish an online repository of already public information, including records that have been released through previous access requests, in order to provide a proactive approach to access instead of a reactive one? What costs would be associated with establishing and maintaining such a resource?

For guidance on providing access within the institution to its official records, see the Annex for a case study about access issues in Singapore.

Developing Access Policies

Even though it is increasingly accepted that citizens or the public in general have a right of access to official records, it is necessary to develop specific policies that regulate access to information. Any policies related to access need to be established within the legislative framework outlined above. The primary purpose of access policies is to articulate who can have access to which records, when and how. But access policies also help an organisation enhance its accountability, promote transparency and nurture public trust.

Before developing an access policy an organisation should undertake three specific tasks.

1 Identify the regulatory framework affecting access and privacy, including identifying all the laws and regulations (as described above) that may have a bearing on any decisions about providing access to information.

2 Conduct a records survey and/or business process analysis, to identify all the records created by the agency and identify those that need to be managed in order to ensure appropriate access is provided.

3 Carry out a risk assessment to determine the dangers of inadvertently providing or denying access to information that ought to be managed differently.

As a result of these three steps, the organisation should be able to identify and assess different risks, establish procedures for managing the access process and assign responsibilities for further action.

Identifying Risks

The organisation should be able to

- identify legally enforceable rights to or restrictions on access
- identify the risks associated with providing access, including the danger of invading personal privacy or violating commercial confidentiality
- identify the risks associated with preventing access
- link the risks identified to specific classes or groups of records and build access conditions or restrictions into specific classification schemes.

Managing Access

The organisation should then be able to

- identify ways to mitigate the risks identified
- identify ways to measure the success of access services
- identify the resources required to carry out access controls and procedures.

Assigning Responsibility

Finally, the organisation should

- assign responsibility for the management of access protocols within the business unit or agency
- document all policies and procedures so that an accountable access framework is established for the business unit
- train and orient all appropriate personnel in the business area so they are aware of their roles and responsibilities for providing access and protecting privacy.

Key Components of an Access Policy

All access policies should include the following components:

- statements outlining the objectives, purpose and scope of the policy
- information about related laws, regulations or policies that may affect access provisions in the organisation or business area
- statement of how the organisation intends to respond to those laws and regulations
- identification of who is responsible for overseeing the overall implementation of the policy and/or fulfilling the detailed requirements of the policy
- an explanation of the sanctions in place for non-compliance with the policy

The policy may also include reference to the resources needed to execute the policy successfully. A sample access policy is shown in Figure 9 below.

Figure 9: Sample Public Access Policy

Purpose

This policy provides people with the opportunity to access certain categories of public records created by [the government] without having to submit a formal application under the Access to Information and Protection of Privacy Act (ATIPOP Act).

Explain the purpose of the policy in as much detail as needed.

This policy shall be administered according to the following principles:

- Protection of personal privacy: public records containing personal or protected information shall not be disclosed except in accordance with the ATIPOP Act.
- *[The government]* will respond to routine access requests within a reasonable time, according to the guidelines established in the ATIPOP Act.
- *[The government]* shall be entitled to charge fees for the reproduction and delivery of records, as authorised by policies and as per the guidelines established in the ATIPOP Act.

Purpose

The purpose of this policy is to make certain records routinely accessible to the public, in order to facilitate access for those people requesting information and in order to support the intention of the ATIPOP Act to support openness and accountability in government.

Scope

- This policy covers records in all formats, created in the course of [the government's] business, including records in electronic, video, audio or other formats.
- This policy does not apply to information subject to exemptions under the ATIPOP Act.
- This policy does not apply to archives that were subject to access restrictions before the ATIPOP Act came into effect on 1 July 2003.
- This policy does not apply to information that is subject to solicitor-client privilege.

Outline the purpose and scope of the policy.

Policy Guidelines

Once a request for access to a particular record or set of records has been received, it shall be forwarded to the appropriate personnel within the agency, who shall review the request and determine whether the records requested may be released according to the policy. If the policy does not apply to the request, the requester shall be referred to the ATIPOP Act office. If the policy applies to the request, the records shall be provided to the applicant within a reasonable period, according to the requirements set out in the ATIPOP Act.

Responsibility

Application of the policy is the responsibility of the ATIPOP Act office, which may designate individuals in government offices or in the National Archives to administer the policy on a daily basis and respond to individual requests for information.

Identify the offices ultimately responsible for ensuring the policy is followed.

Monitoring

The access procedures established under this policy shall be reviewed and evaluated on an annual basis by the ATIPOP Act office.

Definitions

Records: Documents regardless of form or medium created, received, maintained and used by an organisation (public or private) or an individual in pursuance of legal obligations or in the transaction of business, of which it forms a part or provides evidence.

Add key definitions so that all readers understand the full scope of issues addressed in the policy.

Records management: That area of general administrative management concerned with achieving economy and efficiency in the creation, maintenance, use and disposal of the records of an organisation throughout their entire life cycle and in making the information they contain available in support of the business of that organisation. *Include a formal review date.*

Add any references or associated materials so readers and users can access all related resources.

References

Access to Information and Protection of Privacy Act

National Copyright Law

[*The government's*] Archives Policy

Associated materials

[The government's] Access and Privacy Guidelines

Review date

To be reviewed by senior management on or before July 12, 2009.

Include a formal review date.

Implementing Access Policies

Once access policies are established the organisation should review all documents created to ensure they are comprehensive and accurate, and then the organisation might consider testing the policy against actual or fictitious access requests to see if any policy-related concerns emerge. For the actual implementation of access policies to succeed, the following will need to be done.

- Ensure senior management support and commitment are in place for the new policy and for the consequent changes in the organisation's operations.
- Ensure all personnel directly involved in administering access policies and procedures have been given formal responsibility for that work, through revisions to job descriptions if necessary.
- Provide immediate and ongoing education and training for all affected personnel, including producing and disseminating procedural manuals and guides to support implementation.
- Meet regularly with all affected personnel to assess performance and address any concerns or questions.
- Monitor and evaluate the access programme regularly and make changes and improvements whenever necessary to achieve the best outcomes possible.

Any policy should be reviewed regularly, but it is especially important to review access policies when they involve electronic records or information. Since the technologies used to create records changes so rapidly, it is important to consider whether technological changes affect the nature or scope of the records covered by access policies or the ways in which the policies can be applied. Careful and regular review will ensure any organisation can then ensure it is always complying with both the letter and spirit of access legislation, ensuring the public's right to information is always protected.

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 Define classification. What are the differences between functional classification and other approaches to the organisation of files and records?

2 Explain the three main levels of functional classification. Give two examples of how the different levels reflect work performed in an organisation or business.

3 Explain at least three qualities of an effective functional classification system and name three benefits and three limintations of functional classification.

4 Describe the different categories of files that might be found in a typical organisation.

5 What is a functional thesaurus and why is using a functional thesaurus useful when developing classification schemes?

6 What is meant by the phrase 'naming conventions'? Why are naming conventions useful in the management of electronic records?

7 Identify at least three procedures that can be followed when naming records and files in order to improve consistency and increase retrievability of record.

8 Explain how organisations can control the creation and use of different versions of documents.

9 What are some advantages and disadvantages of relying on computer software to standardise and control records creation and naming?

10 Explain the three basic options for saving electronic documents.

11 What is metadata? Why should metadata be gathered when creating and using electronic records?

12 Describe at least two software tools that exist to generate metadata. What are the benefits and drawbacks to using software tools to capture metadata?

13 What are the advantages of using shared network drives? What are the advantages of using personal drives?

14 Explain the concept of 'publish and point.' When is it useful to establish a publish and point policy for electronic records management?

15 Identify two issues associated with managing sensitive information on shared computer drives.

16 Identify and explain at least three policies that should be established to support effective email management.

17 Define the concept of 'hybrid' record keeping. Name two benefits and two drawbacks to maintaining records in a hybrid environment.

18 Name three issues to consider when deciding whether or not to scan paper records and save them electronically.

19 Why is it necessary to appraise records? Is appraisal more important for the management of electronic records than for paper records? Why or why not?

20 Which representatives of an organisation should participate in the appraisal of records? What are their different roles?

21 Define the steps involved in appraisal and explain the importance of each step.

22 Outline the core documentation that should be generated from each step in the appraisal process.

23 What is a retention and disposal schedule? Why is it important to create such a schedule as part of the appraisal process?

24 What is the principle behind access to information legislation?

25 Identify at least three different types of legislation that can affect people's right to access information or to have their personal information protected.

26 How have electronic technologies changed the ability of people to access public information and records? What issues need to be considered in order to provide access to records in an electronic environment?

27 Identify the key components of an access policy and the major steps involved in implementing an access policy.

ANNEX

Establishing a Trusted Record-keeping System: Implementing an E-Registry System at the National Archives of Singapore

Electronic mail (email) is increasingly popular not only as a means of communicating within and outside an organisation but also as a tool for documenting decisions and actions.[3] In Singapore, for instance, a government initiative undertaken in 2005 to engage citizens on national policy issues resulted in more than 5,000 separate emails from the public providing feedback on the issues raised.

For more on this story, see the Singapore government website at http://www.igov.gov.sg/NR/rdonlyres/C586E52F-176A-44B6-B21E-2DB7E4FA45D1/11228/2005ReportonSporeeGov.pdf

With the proliferation of emails and with decentralisation of the records management functions in some ministries, however, there is an urgent need to address the proper management of emails, in order to ensure they are protected as evidence of business transactions and government decisions. Some government agencies have adopted a 'print and file' approach in managing emails, but one of the dangers of this approach is that many emails may not be filed if action officers do not take the time. And with the regular rotation of policy officers within ministries, it is easy to lose track of who has taken what action with filing and information management. There is also an inherent danger that action officers may mistakenly think that the term 'archiving' – meaning saving data on a central server – is the same as 'archiving' records for their ongoing preservation as authentic and reliable evidence.

As a custodian of public records for the nation of Singapore, the National Archives of Singapore (NAS) is mandated by the National Heritage Board (1993) to 'conduct a records management programme for the efficient creation, utilisation, maintenance, retention, preservation and disposal of public records' and 'to advise public offices concerning standards and procedures pertaining to the management of public records.'

[3] The author of this annex is Elaine Goh.

For more information about the mandate of the National Archives of Singapore, see Section 17(2) of the National Heritage Board Act (1993), available online at http://statutes.agc.gov.sg/.

To meet its legislative responsibility, NAS recognises the need to develop a practical and trusted record-keeping system to manage the filing, registration, retrieval and preservation of emails and attachments throughout a record's life cycle. The NAS worked with two private software vendors – SQL View Pte Ltd and Kodak (Singapore) Pte Ltd – to develop an electronic registry (e-registry) system to store and maintain electronic records, which has been operating successfully at NAS and in several other government agencies since April 2006. The system has also served as a practical model to train record managers and IT personnel in the public sector on good recordkeeping practices in an electronic environment.

To learn more about the background to electronic mail management at NAS, see the case study by Pitt Kuan Wah, *Preserving Electronic Records at the National Archives of Singapore: A Balancing Archival Act and a Shared Responsibility,* in volume 1 of the MPSR case studies.

The case study presented here aims to illustrate the record-keeping functionalities of the e-registry system and highlight some of the lessons learned as the system was developed and implemented.

Capturing Records

Determining the type of record to be filed in a recordkeeping system and who to file the record is primarily a policy issue. NAS has developed email guidelines for government agencies specifying the type of records that should be filed. For example, records that document activities, transactions and decision-making process, such as instructions, procedures, reports and approvals, should be filed. Matters that are transitory and ephemeral need not be filed.

It is common for the writers of emails to send the messages out to multiple recipients either for action or for information. The office then needs to make a decision about who should be responsible for filing the record. NAS email guidelines stipulate that the officer with primary responsibility for the action should e-file the record. For example, the secretary in charge of a committee would be deemed the official record holder and would file all emails and other records related to the work of the committee.

Another issue with record capture is to determine how to integrate the e-registry system with other applications that are also generating records. Since the Singapore Government Email System (SGEMS) is currently based on a Lotus Notes platform, the e-registry system also needs to be integrated with Lotus Notes. The system might have to be compatible with any other email system used to support SGEMS, and it must also accommodate other standard office applications such as word processing documents, spreadsheets and PowerPoint.

The e-registry system developed by NAS and its industry partners has four basic methods for filing electronically generated email records, including registering paper-based records so they can be tracked in the system. In each of these methods, the system has the capacity to maintain links between the email and its attachments, preserving the identity and integrity of the record as a whole.

Method 1: E-file Directly

E-registry includes a 'save' utility tool that allows users to click on a button and receive an automatic prompt from the system asking them to e-file either the email and the attachments together, the email message itself or just the attachment itself. This inclusion of a selection for filing meets one of the mandatory requirements of the US Department of Defence (DoD) standard, which states that users must have the option of filing emails and attachments together as one record or as separate records.

For more on the US Department of Defence standard DoD 5015.02, see the discussion in Module 1.

Method 2: E-file from Application Systems

Users can also directly e-file the record from the software used to create it, such as word processing software or PowerPoint software, moving the record directly from that software into the e-registry.

Method 3: Drag and Drop

Users can apply a 'drag and drop' method to move records generated from standard application software and save it into an e-registry folder, which is located on their PC desktop.

Method 4: File via a Web-based Interface

The e-registry is accessible via an organisation's Intranet, which means that users can also file the record generated from application systems via a web-based interface.

Registering Paper Records

For incoming paper correspondence or other records that are not scanned and e-filed and profiled in the system, action officers or registry staff can register the paper record by entering the details of the record profile into the system. The paper record

can then be filed with other paper records, and users can identify its location by searching in the e-registry.

Technical Conversion

At the time the record is created, the email is converted into an image file. NAS decided to use the software product DjVu, which NAS determined was a suitable file format for converting the email. Any attachments would be filed in their native format.

During the pilot test of the system, users at NAS discovered that when the email was converted to PDF using Adobe Distiller Version 6, part of the email message became corrupted, damaging the identity and integrity of the record. A decision was made to adopt DjVu as a file format to convert email records in the e-registry system. Even before the implementation of the e-registry, NAS had also adopted DjVu as a file format for digitising textual records for online finding aids. Examples of digitised records include government speeches and press releases.

> The file format specifications given by DjVu are freely available; details can be obtained from the company's official website by following the link http://djvu.org/.

When records are filed, a record number is automatically generated for both the filed email record and each of its corresponding attachments. The numbering structure is constructed as follows.

- The document number AQ-001-21-183A is a number automatically registered by the system.
- That number – AQ-001-21-183A – is linked to the file classification scheme:
  - AQ-001-21 refers to the file reference number (based on the file classification scheme which users can access based on their job function and responsibility)
  - 183 is the 183th record filed in the electronic folder
  - A refers to the first attachment.

Should there more than one attachment, the system will sequentially assign another letter, such as B, C and so on.

Creating a Record Profile

In most electronic records management systems, the act of profiling a record occurs when the action officer e-files the record. Creating a record profile helps to ensure the reliability of records, since the profile contributes to the overall completeness of the record and institutes documentary control over the creation of the record.

A record profile also verifies the authenticity of a record since it documents information about when the record was transmitted and received. In the NAS e-registry, some of the fields in the record profile are automatically generated by the system while others (such as the file reference number) must be completed by the action officer filing the record.

Below is a list of the fields in the record profile; all of these fields are mandatory with the exception of 'keywords.'

- **Document Subject:** denotes the subject of the email or the file name of the electronic record which is automatically generated from the application software. The action officer has the option to change the contents into a meaningful subject to facilitate future search and retrieval.
- **File Reference:** users can select a list of file frequency accessed files (based on the filing pattern of the respective user) or by selecting the appropriate file from a list of file references.
- **Action Officer:** name of the officer who e-files the record. The system automatically detects and captures the name of the action officer based on the user ID of the officer who logs in the system before he or she can file the record. However, if the person who e-files the record is not involved in the business activity that creates and generates the record – as in the case of registry staff who assist action officers to e-file emails – the registry staff is expected to change the name of the action officer.
- **Designation:** system automatically detects and captures the designation of the action officer based on his/her designated role in the institution's organisational chart.
- **Keywords:** this field can be optional and allows the user to provide a brief description of the content of the record.
- **Document Date:** system automatically detects the date of the record.
- **Registered by:** name of officer who e-files the record.
- **Date and Time of Registration:** these two fields are automatically detected by the system.

Note that the last two elements – registered by and date and time of registration are completed when the user e-files the record from the office application system; they are not used when creating a profile for an email to be filed.

Establishing a Classification Scheme and Retention Schedule

The NAS e-registry has the capacity to support a hierarchical classification scheme. NAS uses up to three levels of subject headings – primary, secondary and tertiary – for its file classification scheme. This approach is in keeping with the *MoReq* requirements for the management of electronic records, which states that ERMS systems must be able to support hierarchical classification schemes extending at least three levels.

For more on *MoReq,* see Module 1.

The metadata captured in the file classification scheme include fields relating to the date the file was created, the date the file was closed and the previous file reference. This information helps NAS maintain the archival integrity of the file by ensuring it can be related to other files relating to the same subject matter.

The file classification scheme in the system is integrated with the NAS retention schedule, with information included in the classification scheme related to the retention period for the file and the schedule for disposal. This ability to document retention information in the e-registry allows NAS to appraise records at the record creation stage. As a result, agencies that have implemented the system can transfer records of archival value to NAS custody on a regular basis and not wait for records to 'age' before deciding whether to transfer them.

NAS is in the process of working with its industry partners to develop an electronic archiving module to complement the e-registry system, which will fit into the life cycle model of creating, maintaining and preserving e-records. This module will allow government offices to submit the metadata for the records to NAS for appraisal, import the approved retention schedule into their file classification scheme and transfer metadata and records of value to custody in the national archives. NAS will then copy the records onto microfilm while preserving the metadata in electronic format, facilitating search and retrieval in the future.

Searching for and Retrieving Records

The e-registry supports the search, retrieval and display of records through a variety of interfaces. Users can search for records by file title, file reference number, record profile or content. Regardless of the search interface selected by users, the system allows users to access all related records within a file or electronic folder, provided that the user is granted permission to view the records.

Users can also identify records by browsing recently accessed files or reviewing the hierarchical structure of the file classification scheme. Because all related records within the same file can be accessed, action officers receive a holistic perspective, seeing all related records relating to the same business activity.

Implementing Access Controls

The system controls access to records on a file or electronic folder level. Access permission is linked to the action officer's designated responsibility and role in the organisation. NAS also recognises, though, that collaborative work groups cut across various divisions and involve many personnel within an institution; these work groups create and receive a range of records that might be used outside of a traditional hierarchical business framework.

The e-registry system recognises the dynamic nature of this collaborative work environment and also allows access privileges to be assigned to different work groups. For example, during the development of an exhibition gallery, a project team included staff from various divisions within the National Archives; everyone involved in the project was allowed access to the records related to the project.

In the event that the action officer accidentally files the record into a wrong folder, he or she can mark the records for deletion. But access controls restrict the officer from deleting the record immediately; instead, approval has to be obtained from a more senior official (or their immediate supervisor) and that approval must be sent to the e-registry system administrator, who can then delete the record. The system also includes a number of audit trails. Identifying which action officers e-file and delete records, which officers have viewed, copied and retrieved which records, which officers have edited record profiles; and which officers have created, edited or deleted folders. The officer's name and position are both tracked as part of the audit trail.

Lessons Learned

The following important lessons were learned during the implementation of the e-registry system.

The Importance of Records Management Education

The e-registry system was developed as a partnership between a public institution and private vendors. In the course of developing the infrastructure, NAS staff needed to communicate with the vendors about the functional requirements of the system, so that the vendors would develop an infrastructure that complies with the functional requirements of record keeping.

Because records professionals and IT personnel use different terminology or, more importantly, use the same terms to mean different things, there were a number of instances of miscommunication during the project. For instance, the concept of 'file,' 'record,' and 'archives' was defined differently by records professionals and IT professionals.

In addition, the vendors had to be familiar with the organisation's business processes, such as the way in which government agencies submitted their records to NAS for appraisal. Fortunately, this challenge also presented an excellent forum for archivists to educate those in the information management and information technology fields, and raised awareness of the importance of quality records management. In the end, the product was a viable and effective e-registry system that meets important record-keeping requirements.

The Potential for Restructuring Business Processes

The development of the e-registry system provided an opportunity for NAS staff to improve existing file classification schemes to accommodate the mandate and functions of the institution more effectively. Previously, the NAS file classification scheme had been based on a numeric and year system. One disadvantage to that approach was that the file numbering system was not meaningful to users.

For instance, the file number 99/100, which referred to the file titled Acquisition of Archival Records: Policies and Procedures, indicated that it was the one hundredth (100) file created during the year 1999 (99). Unfortunately, the numbers do not reveal any information about the business functions or operations of NAS.

The revised file classification scheme now reflects the business activities of NAS. For instance, the file reference GR-000 is meaningful: GR denotes Government Records, and 000 refers to matters relating to policies and procedures. The numbers 000 are always used to refer to policies and procedures, allowing staff to see logical patterns and help them become more familiar with filing practices.

The process of developing the e-registry system also prompted NAS to review its records appraisal and transfer process for electronic records. In order to ensure that there is an integrated approach in the life cycle management and preservation of records, NAS has been working closely with the software vendor to develop a module to facilitate the appraisal and transfer of records generated from its electronic records management system into permanent custody within the archival institution.

Some of the other government agencies in Singapore that have implemented an electronic records management system have also taken the opportunity to examine their records processes and business functions more closely. For instance, some agencies have changed their procedures with regard to scanning backlogged paper records and others have imposed strict cut-off periods for including records in the new system.

The Importance of Communication

The development of the e-registry system served as a useful training tool for NAS staff to stress the importance of record keeping, to promote good records management practices and to increase human capacity for records management throughout government. During briefing sessions about the e-registry system, the feedback received provided NAS and its industry partners with opportunities to improve on the functionalities of the system.

For instance, some users expressed concern that they may have inadvertently e-filed the same email in the same electronic folder multiple times. As a result of this suggestion, NAS and the software developers created a mechanism that allows the system to detect the potential for double-filed emails within the same electronic folder before the records are actually filed.

Briefing sessions with government agencies also enabled NAS to understand the concerns of record users in implementing the system and this was an important avenue for NAS as user support for the system is an essential component of the successful implementation of any electronic records management system. NAS has compiled a list of frequently asked questions raised about the system and distributes this information to government agencies through the Intranet. At the same time, regular communication with agencies allow NAS to understand the recordkeeping practices of agencies and their evolving business functions which enabled NAS to formulate strategies for better management, appraisal and preservation of government records.

The Importance of Automatic Metadata Capture

During the pilot test of an earlier version of the e-registry system, users complained that they had to key too much information into too many metadata fields; they argued that some fields should be completed automatically by the system. At the same time, NAS was conscious not to overload the e-registry system with too many metadata fields, thus hindering the performance of the system. The goal was to make the software as user friendly as possible, so that action officers would be more receptive and would participate actively.

As a result, a number of drop-down lists have been incorporated into the system to facilitate entering the record profile. The software developers have also developed an 'intelligent filer' system, which could automate the process of entering a record profile by replicating the common information generated by that particular user and then asking the user to amend any information.

The Importance of Addressing the Changing Business Environment

As of 2008, the Singapore government is involved with the implementation of a Standard ICT Operating Environment (SOEasy) for the public sector, which involves streamlining and consolidating information and communication services into a standard office environment. As part of this process, the SGEMS will be moved from Lotus Notes into Microsoft Exchange. NAS has worked closely with its industry partner to ensure that e-registry is compatible with Microsoft Exchange. At the same time, the software vendor has embarked on a research project to facilitate the filing of email records from mobile devices such as cellular telephones and text messaging devices since the government anticipates that public officers will be increasingly mobile and will create e-records from mobile devices.

> The announcement about establishing SOEasy for the Singapore public sector is available at http://www.ida.gov.sg/News%20and%20Events/20080228151049.aspx?getPagetype=20.

The Importance of Defining a Preservation Strategy

Email records that are of archival value would be transferred onto microfilm in NAS for long-term preservation. While it may be argued that the e-record would lose its dynamic nature once it is preserved onto microfilm, NAS still considers this an acceptable preservation strategy, since fixing and preserving the content of the record through microfilm would not lose the intrinsic evidential qualities of the email and is also a cost-effective way to reduce technological dependency.

Conclusion

In conclusion, the implementation of an e-registry for the government of Singapore has given the government a robust infrastructure to capture emails as a corporate

intellectual asset. The system also allows people across functional groups to share information and records, while ensuring that valuable records are protected through the implementation of access controls. Because the NAS worked closely with the software vendor, the end result is a system that meets record keeping requirements and also ensures that users will accept and use the system as a regular part of their business process.

NAS has absorbed the development costs of the system, while the vendor is required to provide enhancements to the system on a continuous basis as part of research and development. This collaboration benefits government agencies, which do not need to incur development costs but instead only have to pay for user licences and the cost of installing hardware and software.

Moreover, agencies across government have also worked closely with NAS to learn how to implement the system, providing NAS with a welcome opportunity to promote better awareness on the importance of records management as part of the accountability framework of the Singapore government.

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