



General Guidelines for Implementing an Electronic Document and Records Management System

MARCH 2009

CONTENTS

1.	INTRODUCTION.....	3
2.	CONTEXT	4
3.	LEGISLATION AND STANDARDS	4
3.2.	Legislation.....	4
3.3.	Standards	5
4.	DEFINITIONS	5
4.1.	Author	5
4.2.	Container	5
4.3.	Creator	6
4.4.	Disposal	6
4.5.	Disposal Schedules	6
4.6.	Document	6
4.7.	Document Editing.....	6
4.8.	File Plan	7
4.9.	Hybrid System.....	7
4.10.	Metadata	8
4.11.	Record	8
4.12.	Records Management.....	8
4.13.	Record Types.....	8
4.14.	Redaction.....	9
4.15.	Reference Material.....	9
4.16.	Secure Remote Access	9
4.17.	Security	9
4.18.	Storage Devices.....	10
4.19.	TRIM Context (more commonly referred to as TRIM)	10
4.20.	Workflow	10
5.	ROLES AND RESPONSIBILITIES.....	10
5.1.	Roles.....	10
5.2.	Responsibilities	13
6.	FILE PLAN	13
6.1.	Overview.....	13
6.2.	Functional File Planning.....	14
6.3.	Operational Functions.....	15
6.4.	File Plan Guidance.....	16
7.	NAMING CONVENTIONS AND STANDARDS	17
7.1.	Naming Documents	17
7.2.	Building a Name.....	17
7.3.	Elements needed in a Document Name	17
7.4.	Elements Not Needed in a Name.....	18
7.5.	Practices to Adhere to in Naming Documents	18
7.6.	Practices to avoid in Naming Documents	18

8.	CREATING CONTAINERS	19
8.1.	Electronic Containers.....	19
8.2.	Manual Files.....	20
8.3.	Confidential Files	20
9.	SAVING DOCUMENTS AND RECORDS	21
9.1.	Why do we need to save documents and records?	21
9.2.	Revisions in Documents	21
9.3.	Status of Documents.....	22
9.4.	Deletion of Documents.....	22
9.5.	What not to file.....	22
9.6.	Ensuring Completeness.....	22
9.7.	Finalising Documents to become records	23
10.	E-MAILS.....	23
11.	MANAGING SECURITY AND ACCESS	24
12.	AUDIT TRAILS.....	26
13.	RECORDS MANGEMENT AND SCHEDULING	26
13.1.	Record Types.....	26
14.	METADATA.....	27
15.	SCANNING	28
16.	PRINTING	30
17.	STORAGE DEVICES OUTSIDE OF EDRM SYSYEMS	31
18.	DISPOSAL SCHEDULES	31
19.	TRANSITION PROCEDURES	31
19.1.	Introduction	31
19.2.	Papers currently held for filing.....	31
19.3.	Closure of existing paper files.....	32
19.4.	New File Classification	33

1. INTRODUCTION

The last decade has seen a massive expansion in electronic ways of working across the entire Northern Ireland public sector. Today, the majority of work carried out on behalf of Northern Ireland Civil Service (NICS) Departments, non-Departmental public bodies and other public sector organisations is carried out electronically.

This growth has seen public sector organisations employing a wide variety of electronic record creating systems. This in itself leads to problems when it comes to information sharing, providing accountability for decision making, or replying to information legislation requests.

In 2003 NICS, as part of the Common NICS Infrastructure Programme, launched the project which was to become known as RecordsNI. That introduced a single Electronic Document and Records Management System across the NI Government Departments. The successful implementation of the chosen product, the HP system known as TRIM, has led to a standardisation of electronic record keeping processes across NICS, improved sharing of information between staff, and 16,000 users accessing a single application to create the record of their respective Department's work. As of March 2009 almost five million documents have been created within TRIM.

The 'roll-out' of TRIM across NICS was overseen by an Inter-Departmental Working Group (IWG) made up by representatives from the NICS EDRM Central Project Team, Departmental Information Managers from NICS and staff from the Public Record Office of Northern Ireland. IWG was responsible for agreeing the finalised version of TRIM that rolled out to staff.

With the implementation phase complete the operation of TRIM has moved into the records and information management phase of the project. Together with TRIM and the launch of reform projects such as HRConnect and AccountNI all strengthening electronic working across NICS the issue of Information Assurance has become a central issue for Departments. As such, the IWG has been formalised as a central records and information management group tasked with taking forward electronic record-keeping across NICS.

The following guidance distilled from the experience of NICS during the TRIM implementation is intended as a best practice benchmark for all organisations that operate, or intend to operate, an Electronic Document and Records Management system (EDRM).

It is recognised that a number of Line of Business Applications and databases are in use across the NI public sector which are used to manage day-to-day business operations. Integration of these LBAs with TRIM was not undertaken as part of the EDRM Implementation Project.

A second piece of guidance to follow will deal specifically with these electronic record-keeping systems.

2. CONTEXT

Records are essential to the smooth operation of a public sector organisation in pursuit of its function. If records, whether paper or electronic, are not managed properly public sector organisations are left unable to carry out business, provide accountability for decision-making, or deal with information requests.

Lord Chancellor's Code of Practice on the Management of Records sets out what is expected of public sector organisations when they create and manage records in any format. The Code states that *'Records and information are the lifeblood of any organisation. They are the basis on which decisions are made, services provided and policies developed and communicated'*. The guidance below is intended to provide public sector organisations with best practice advice on how to prepare for, implement and manage an Electronic Document Record Management System.

3. LEGISLATION AND STANDARDS

3.1. Overview

There are a number of legislative drivers that necessitate the creation and management of records within all government departments and agencies. The sections below give details of the legislation that governs records management, as well as the standards, which provide the necessary framework for effective and efficient records management.

Please refer to the website/reference material listed for guidance on the relevant matter.

3.2. Legislation

The Copyrights, Designs and Patents Act 1988
www.cla.co.uk

Public Records Act (Northern Ireland) 1923
www.proni.gov.uk/

Freedom of Information Act 2000
www.opsi.gov.uk/Acts/acts2000/ukpga_20000036_en_1

Environmental Information Regulations 2004
www.informationcommissioner.gov.uk/eventual.aspx?id=36

Data Protection Act 1998
www.informationcommissioner.gov.uk/eventual.aspx?id=34

The Re-use of Public Sector Information Regulations 2005
www.opsi.gov.uk/si/si2005/20051515.htm

3.3. Standards

Northern Ireland Records Management Standard

<http://www.proni.gov.uk/>

ISO15489 Records Management Standard

www.iso.ch/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMB ER=319008&ICS1=1

ISO7799 Information Security Management System

<http://www.bsi-emea.com/InformationSecurity/Overview/index.xalter>

BS 10008:2008 Evidential weight and legal admissibility of electronic information

<http://www.bsigroup.com/en/Shop/PublicationDetail/?pid=00000000 0030172973>

Guidance on Electronic Records and Metadata

www.nationalarchives.gov.uk/electronicrecords/reqs2002/

3.4. Codes

Lord Chancellor's Code of Practice on the Management of Records on the Management of Records. Issued under the Freedom of Information Act 2000. (Currently under review.)

<http://www.justice.gov.uk/guidance/foi-code-of-practice-records.htm>

4. DEFINITIONS

4.1. Author

The person who creates a document. TRIM automatically captures this detail from a user's login details.

4.2. Container

An EDRM allows for the creation of electronic files into which a user can save their documents. Various terms are used to describe these files. In the NICS RecordsNI implementation the systems referred to these as Containers.

Containers, equivalent to Folders in a Windows environment, are opened within classes in the File Plan and hold all the documents and records relating to that activity. As in the paper environment where a centralised registry would hold files opened to contain paper, so too can an EDRM.

4.3. **Creator**

This is the person who creates a document or record into an EDRM. If you create a document and then save it you will be author and creator. However if you save a received email into TRIM, you will be the creator and the sender of the email will be the author. TRIM will automatically capture the creator details.

4.4. **Disposal**

The word disposal, when used by PRONI can mean any of the following:

- ▶ Destruction of records
- ▶ Records to be appraised (if paper, to be reviewed)
- ▶ Records transferred for permanent preservation at PRONI
- ▶ Transfer of the ownership of records
- ▶ Damage, alternation or rearrangement of records
- ▶ Separation from or disturbance to contextual information, software, hardware or other equipment on which records depend.

4.5. **Disposal Schedules**

An EDRM should have the capability to allow for the creation of disposal schedules determine the retention, destruction or transfer of records after a specified time period and should be managed centrally within an organisation, in conjunction with PRONI.

4.6. **Document**

The term “document” is used to describe any document created, edited and stored by an end user prior to being finalised as a “record”. Document could be an electronic record in any format such as e-mails, word documents, PowerPoint presentations, PDFs, TIFs, etc.

4.7. **Document Editing**

An EDRM will allow for the editing of electronic documents after they have been saved onto a file plan. The NICS EDRM system, TRIM, has functionality that enables users to create revisions, new versions or renditions of documents. These are described below:

Revisions

Any editing of a current document will automatically create a new revision of that document. TRIM provides the functionality to view the revision history of documents/records.

Versions

A version is created manually by the user and a new record is generated for the document. Therefore versions are different documents with the same title, whereas revisions are successive alterations to the same document.

Renditions

A rendition is part of the same document and is similar to a revision except that it is the document presented in another format, usually for accessing in a different way or for displaying different information. For example, instead of releasing a Word document as part of an FOI request you could release the rendered copy of the document (e.g. in a TIF format) possibly with sections redacted. The rendered copy would still be part of the original record

4.8. File Plan

A structured classification of records providing a full representation of the business of an organisation. The top levels of the file plan are referred to as 'classes' within which 'containers' are opened to hold documents and records relating to particular activities, tasks and transactions.

In a paper filing system this would be similar to looking at your File List, going to the relevant Filing Cabinet, selecting the relevant Drawer within that cabinet and identifying the relevant Paper Folder/File in which you need to access or file information.

4.9. Hybrid System

An EDRM can be configured to operate what is, in effect, a hybrid system. This will allow for the registration of electronic containers and documents, as well as holding cross referenced information about any physical paper files created. Therefore an EDRM will be able to accommodate:

- ▶ Electronic documents to be filed within the appropriate container in the File Plan.
- ▶ Electronic documents and an associated paper file (perhaps containing papers marked 'confidential') – in this situation, the electronic documents are filed directly into the File Plan as usual and the metadata on the container updated to indicate the relationship to a paper registered file.

- ▶ Finally, in some cases there will be no electronic documents for the container but only physical papers. In this case a registered paper file will be opened to store documents and a corresponding container in TRIM will be opened where the metadata indicates that a paper file exists.

To ensure effective tracking of ownership and physical location of a paper file it is essential that the appropriate referencing information, to include corresponding file references, should be added to the metadata describing the container. This will also allow for the appropriate disposal action to be applied to both the electronic and physical documents at the same time.

4.10. **Metadata**

This is information about documents or records. It is either automatically generated when a document is created or it may require the user to fill in some fields. For example the metadata for a word document might include title, author, date created etc.

4.11. **Record**

A record is evidence of a business transaction or decision. To create a record a user must first save a document into an EDRM. When the user has finished working on that document a further step needs to be taken to fully register it within the EDRM. This will then allow for disposal and retention actions to be applied to the document. In the paper world this would have been the same as putting a document into a registered file once all work had been completed.

The system used by NICS, TRIM, describes the action taken to create a record as 'finalising'. Once a document is finalised and becomes a record it can only be deleted from TRIM in accordance with the disposal schedule.

4.12. **Records Management**

Records Management is the field of management responsible for the efficient and systematic control of the creation, receipt, maintenance, use and disposal of records. It includes processes for capturing and maintaining evidence of and information about business activities and transactions in the form of records.

4.13. **Record Types**

Record Types are templates for the creation of an organisation's records. The Record Type dictates how records of that type will be numbered, titled, the default security etc.

4.14. Redaction

When dealing with requests for information under either the Freedom of Information Act or the Data Protection Act, it is important to note that in some cases, exemptions, which are contained in these Acts, may apply.

In practice, this could mean that portions of the information requested should not be revealed under the terms of the relevant Act and should be redacted (ie blanked out) to ensure that the person who requested the information cannot read them. Departmental Information Managers (DIMs) will be able to advise on when an exemption may apply. Information Management Branches (IMBs) will be able to provide guidance to staff on how redactions can be achieved, cross referenced and retained within TRIM.

4.15. Reference Material

Refers to information created by another department, branch or organisation and kept as a reference source.

4.16. Secure Remote Access

When Departmental networks are accessed from outside of the office e.g.: departmental laptop or departmental PC located in the home.

4.17. Security

During the planning for an EDRM implementation careful consideration should be given to what security mechanisms be built into any organisation's record creating platform.

An EDRM will allow for the creation of security functions that will restrict user access to areas of a file plan, to documents and containers, or set up an area of a file plan that will only be accessed by certain groups of staff.

In the NICS implementation the product chosen, TRIM, allowed for the application of security controls such as the creation of security levels, security caveats and access controls.

Security caveats place restrictions at document and container level which are used to restrict areas of the file plan to specific users with the appropriate permissions. Likewise, security levels ensure that records can only be accessed by users who have the same security level, or higher, than that allocated to the document itself, or the container where it is located.

Security levels and caveats can be applied to the file plan, and managed, by those users who have system administrator profiles. For fuller definition of user profiles see section 5, Roles and Responsibilities.

4.18. **Storage Devices**

A device capable of storing data. Some examples include USB Pen, CD, and Floppy Disks.

4.19. **TRIM Context (more commonly referred to as TRIM)**

TRIM Context is the EDRM product developed by Tower Software that has been chosen by the NICS. TRIM stands for Tower Records Information Management.

TRIM Desktop is the interface which general end users will use to manage their documents and records, and provides the ability to save, search for and retrieve information and manage emails.

4.20. **Workflow**

Automation of business processes, in whole or in part, during which documents, information or tasks are passed from one participant to another for action, according to a set of procedural rules.

5. **ROLES AND RESPONSIBILITIES**

5.1. **Roles**

When implementing an EDRM within an organisation thought should be given to what roles and responsibilities members of staff have when operating the chosen system. EDRMs will have a wide range of functionality that could give users access to all of the systems applications. However, from experience gained during the NICS implementation of TRIM, it is advisable that you should create several user profiles to meet your organisation's business needs. When a user logs onto TRIM, the action is carried out according to a specific user profile which will permit them to carry out tasks within the system according to the permissions related to that profile.

In the NICS implementation of RecordsNI it was decided that three profiles should be created. These were end user, power user and system administrator.

An individual's profile will be determined when their account is created, and amended as necessary by the System Administrator or relevant nominated individual.

The user profiles that were created during the TRIM implementation can be summarised as follows:

End User

The majority of staff in an organisation will fall under this profile. An end user will be able to:

- ▶ Open and read all documents and records to which they have access within the file plan;
- ▶ Create, save and edit documents in agreed areas of the file plan;
- ▶ Search for documents (and save these searches if required);
- ▶ Finalise documents as a corporate record.
- ▶ Request deletion of a document (nominated personnel will review all deletion requests to ensure that the request is appropriate or if it is necessary to retain it as a record).

Power User

It is essential that each business area within an organisation has a Power User. The authority of who takes on this role, specified as the Power User in this instance, will be at your organisation's discretion.

Power Users who have been identified within each business area will provide local user support (particularly in the early stages of the EDRMS rollout when members of staff are getting to grips with the system). It is recommended that Power Users should receive additional training to supplement the standard end user training in advance of any implementation. This will give them time to get used to the functionality of the EDRM, so that when the rest of staff 'go-live' the Power Users will be in a position to provide assistance. In addition to the functions of the end user, a Power User will be able to:

- ▶ Provide initial user support within the branch/office;
- ▶ Provide guidance on the use of the system, where to file documents etc;
- ▶ Create containers at a local level in specific areas of the file plan (initially this function will be carried out by Information Management Branch, but the plan is to roll out this function to branches once the system is embedded in each branch).
- ▶ As in the paper environment where a branch EO, or SO, took responsibility for managing the disposal process, so will the power user in the electronic environment.

System Administrator

There are 2 separate roles involved in the administration of TRIM EDRMS:

- ▶ day to day administration; and
- ▶ information management.

Day to Day Administration – activities associated with this role would typically include:

- ▶ location management (creation of locations, ie user accounts, resolution of 'ghost' locations, activation of temporary locations)
- ▶ Security implementation (assigning security levels and caveats to file plan and locations)
- ▶ Report running (creation and maintenance of reports).

Information Management – activities typically associated with this role would be:

- ▶ Configuration (configuration of systems options to reflect and organisational policies and any updates to these).
- ▶ File Plan management (creation and maintenance of all levels of the file plan)
- ▶ Monitoring of good naming conventions
- ▶ Security management (decisions on the creation and maintenance of caveats, security levels and user types)
- ▶ Record type management (creation and maintenance of record types).
- ▶ Disposal Scheduling Management.
- ▶ Management of document deletion (if appropriate).

Public Sector organisations will have the discretion to define the specific roles, taking account of resources, circumstances, needs and composition of their Organisation.

The number of administrators with full control over the system should be kept to an absolute minimum. Although the 2 roles indicated above may all have full control of the system, it is essential that the roles are assigned to different members of staff.

5.2. Responsibilities

It is the responsibility of every member of staff to ensure that the work they carry out on behalf of their organisation is correctly saved and maintained within the EDRM. Anyone responsible for a particular area of work, in which documents and records are generated, has a duty to create, name, and store them within the EDRM. This includes:

- ▶ creating documents and records as required, and saving them correctly within the EDRM to the appropriate area of the file plan (i.e. relevant container);
- ▶ naming documents and records properly to ensure they can be retrieved easily (in conjunction with naming convention guidance);
- ▶ managing emails properly within the EDRM;
- ▶ declaring documents as records (called finalising);
- ▶ ensuring record-keeping is up-to-date; and
- ▶ determining, from the outset, the protective marking of the document and, more importantly, the sensitivity of the document in line with any organisational protective marking scheme.

Information Management Branches can provide guidance on all aspects of records management and use of an EDRM. However it is the responsibility of individual branches to ensure that this guidance is adhered to at a local level and that staff are aware of their individual roles and responsibilities.

6. FILE PLAN

6.1. Overview

During an EDRM implementation, as was the case for NICS, the single most important stage should be the development of the organisational file plan. NICS took a functional approach to file management that reflected activities and transactions rather than an organisational structure. The reason is that the names of branches and divisions are subject to change, whereas underlying business functions remain relatively constant. The amount of effort and skill required to develop a functional file plan should not be underestimated. If the project is to succeed it will require a significant commitment from all staff within an organisation from senior management to those working in business areas to establish a system relevant to your business needs.

Development of the lower levels of a file plan depends on a good level of understanding of business processes within the organisation. It is essential that you include staff in the development process, e.g. when PRONI carried out its own TRIM implementation a series of business process workshops were held with staff to map out the functions of the

various business areas within the organisation. This had the benefit of involving staff in the implementation, it also provided a sense of local ownership and input, and gave staff the sight of a file plan thus familiarising them with the concepts prior to 'go-live'.

A functional file plan is a living document, which requires continued development, review and ongoing monitoring, e.g. after a period of use a check of the PRONI implementation found that there had been a 25% increase in the number of containers created since the 'go live' date, thus confirming that a file plan is a continuously developing project which will require ongoing monitoring and controls.

The experience of NICS supports the theory that it is essential to the success of an implementation to have a tested and proven functional file plan in place in advance of the actual implementation of the EDRM.

6.2. Functional File Planning

What is it?

The approach taken by NICS when forming the file plan looked at the way Departments approached their work, e.g. in PRONI this was carried out in a series of business process workshops that looked at the functions, activities and transactions that formed the organisation's work. These workshops were held between staff in business units and those tasked with developing their Departmental file plans, and looked at how the business unit carried out its functions, activities and transactions.

What are business functions, activities and transactions?

- ▶ A function is what an organisation carries out to achieve its goals and strategic aims
- ▶ An activity is how the organisation carries out those functions
- ▶ A transaction is the individual task that comprises the activity

The function of an organisation forms the top level of a functional file plan; the activity forms the second level and the transaction the third. It is strongly recommended that when an organisation is carrying out an analysis of its functions that it holds to the function/activity/transaction formula. Experience has taught that a file plan that has three top levels reflecting the function/activity/transaction formula with a level beneath for the containers is much easier to manage.

When carrying out a business process analysis it is recommended to keep the following questions in mind:

- ▶ What are your organisation's functions? (i.e. what do you do)
- ▶ What activities do you carry out to fulfill those functions? (i.e. how do you do it)
- ▶ What information do you receive to carry out the activity?
- ▶ What information do you produce from the activity?
- ▶ To whom do you provide that information?
- ▶ What records do you need to keep?
- ▶ What records do you generate that other business areas need to keep?
- ▶ What is the best way of organizing this information?

As mentioned previously NICS took a functional approach to implementing the RecordsNI file plan. Following business process mapping it was deduced that the work of NICS could be broken down into seven main 'Corporate' functions synonymous to all Departments. These functions covered the general management activities and internal administration processes which keep NICS Departments running and support the business programmes and services.

To promote consistency of approach the decision was taken that it should be mandatory for Departments to implement the top level of the file plan and highly desirable to hold to the second and third levels. The seven main functions which form the top level of the NICS corporate file plan are:

- ▶ Accommodation & Services
- ▶ Audit & Accountability
- ▶ Financial Management
- ▶ Human Resource Management
- ▶ Information & Communication
- ▶ Strategic Management
- ▶ Technology & Telecommunications

6.3. Operational Functions

During the NICS implementation it became clear that the top seven levels of the file plan would not cover all areas of work carried out by an organisation as diverse as NICS. To address this it was agreed that 'operational' functions specific to Departments would also be added to the file plan. In this context 'operational' is used to describe those business functions that are not generally found in other Departments but fall uniquely within a particular Department's remit.

When PRONI was carrying out its own business process analysis it was found that the work carried out specific to the organisation should be categorised as 'Managing Archives & Records'. When PRONI's file plan was finalised it contained the seven top level Corporate functions as well as the new function.

Once an organisation has completed a version of its functional file plan it should be quality assured by staff from PRONI before it is mapped to the EDRM.

6.4. File Plan Guidance

Coding of File plan

To ensure consistency throughout the Northern Ireland Civil Service Departments an alpha-numeric coding system was adopted for the corporate file plan. The alpha prefix should consist of 2 letters as follows:

- AS/ – Accommodation & Services
- AA/ – Audit & Accountability
- FM/ – Financial Management
- HR/ – Human Resources Management
- IC/ – Information & Communication
- SM/ – Strategic Management
- TT/ – Technology and Telecommunications

The following coding system should be adopted – alpha/numeric – for example:

IC/007/005/ INFORMATION & COMMUNICATION – Records Management – EDRM Project

MA/001/001/ MANAGING ARCHIVES & RECORDS/ (example of an operational code and function)

Operational functions should adopt a similar Alpha/Numeric/ coding system but Information Managers should ensure that all alpha codes do not overlap with the corporate indicators. Quality Assurance of file plans by PRONI should include comprehensive information on file coding.

The record number applied should reference the year – for example: 06/0003727. EDRM will condense the year number so that all 4 digits are applied but only the last 2 are shown. By adding the year to the record number information managers will be able to quickly search by year for all records created in a container, groups of containers or throughout the file plan.

7. NAMING CONVENTIONS AND STANDARDS

7.1. Naming Documents

Meaningful naming of documents is essential. Poorly named documents cannot be easily retrieved and will cause confusion. Therefore staff must give greater care and attention than ever before to the naming of documents.

For those staff with responsibility for the creation and naming of containers, the same principles will apply.

7.2. Building a Name

Names must be concise and meaningful. They must be descriptive of the content of the document.

7.3. Elements needed in a Document Name

The following naming convention is likely to be able to describe a document uniquely and, therefore, make it easier to find in any search. There are five elements to consider but not all elements will be appropriate for every document. However, a document name is more likely to be unique if more elements are used.

The five elements are:

Recipient Name – The name of the person, group or organisation to whom the document is to be sent. For example, the addressee of a letter or memo or a branch, directorate or organisation to whom a report is to be issued.

Recipient Address – The location of the recipient. For example, the street address, building name, town or city where the recipient is located. The choice of which to use will be determined in conjunction with the recipient's name.

Subject Matter – The topic of the document (ie what it refers to). For example, for minutes and memos it would be the heading, or for reports it would be the title, or for an agenda or minutes of a meeting it would be the title of the group meeting e.g. Departmental Board.

Period Dates – The dates relevant to the document (ie what period it covers). For example, the date may relate to the subject matter e.g. the date the meeting took place, or the period covered by a report, e.g. a calendar year or a specific to and from date range.

Document Type – The format of the document (ie what style the document is prepared in). For example, the document may be in the form of a letter, memo, minute, report, submission etc.

7.4. Elements Not Needed in a Name

The following information is not required in a name as it is normally automatically associated with the document:

- ◆ Author
- ◆ Date created
- ◆ Department ie DHSSPS
- ◆ Container name

However, if the content of the document requires you to identify Department, date, or author in order to describe it properly, then these elements should be included in the name.

7.5. Practices to Adhere to in Naming Documents

DO:

- ▶ name your document so that the name is meaningful to others
- ▶ remove all instances of “FW”, “RE” from email titles
- ▶ if using a dash “ - “, include a space immediately before and immediately after the dash to enable proper searching within TRIM.

7.6. Practices to avoid in Naming Documents

DON'T:

- ▶ identify electronic file format information – for example e-mail, Word document, Excel, etc
- ▶ include the date the document was created as this is automatically captured
- ▶ use generic names like ‘Latest Version’; ‘Lecture’
- ▶ base names on your ownership of the record, e.g. ‘Jenny’s documents’
- ▶ use the words ‘Miscellaneous’ or ‘General’, as these encourage poor filing practice
- ▶ compress two or more words into one word, e.g. ‘CorpSer’ or ‘RecordMan’. Always separate words with spaces and type out in full
- ▶ automatically accept the e-mail subject as a name – it is likely that you will have to rename emails with an appropriate title
- ▶ best practice would suggest that users should refrain from using the following characters in a name: \ / > < * ? “ ; : _ However there may be occasions when it is necessary to use such characters in the titling of documents. Users should ensure that appropriate spacing between characters, etc is considered in such cases

Examples of Bad Practice	Examples of Good Practice
<ul style="list-style-type: none"> ◆ Untitled ◆ General docs ◆ Jenny's work ◆ Excel spreadsheets ◆ Mtg mins ◆ Recommendations for new services in the Picture Library ◆ Presentation on EDRM 	<ul style="list-style-type: none"> ◆ Archive Centre Proposal ◆ Audit Committee – Risk Management Review ◆ Highlight Report – Dec 2004 ◆ Costings 1st Quarter 2006 ◆ Management Committee Minutes – Jan 2005 ◆ Picture Library – new services – recommendations ◆ Electronic Document and Records Management – Benefits Presentation – Departmental Board

Departments will also need to agree local naming conventions with business areas, following best practice guidelines. This may be necessary where the work of a business area is such that this needs reflected in the naming of the document.

E.g. FOI Requests – the document could be titled ‘Requester Name’ – ‘Topic’ or ‘FOI Case number’ – ‘Requester name’

It doesn't matter which method a Department adopts. However it is important that IMBs agree local naming conventions with branches, and that the agreed convention is documented and monitored for compliance over time. A separate record type may also be necessary.

8. CREATING CONTAINERS

8.1. Electronic Containers

There is a need to retain central control over the file plan and the creation of containers within it to ensure they are correctly named and positioned in the appropriate area of the file plan. Control of classifications (i.e. the top levels of the file plan) will be the responsibility of an organisation's Information Management Unit, if it has one, or within the Corporate Services division, if not.

During the initial stages of any EDRM roll out an Information Management Unit will have responsibility for creating containers within

the file plan. This follows the model in the paper world where Departmental registries would issue registered files upon request.

Once an EDRM has been implemented responsibility for container creation can be devolved to those staff that have the appropriate user profile, such as power user.

For records management purposes, a container in an EDRM should hold a maximum number of documents.

In NICS when TRIM was rolled out this figure was set at 300 documents. This figure can be adjusted to suit an organisation's business need. When the maximum limit is reached TRIM automatically closes the container. A continuation container is created by using a 'rule' within the TRIM permissions. TRIM automatically captures the "Part" number in the name of the new container. TRIM will need configured to provide these functions.

Disposal Schedules will be generally allocated at Classification Level, so careful consideration needs to be given to the location of containers as they will inherit the disposal classification's disposal actions.

8.2. Manual Files

It is recognised that, in some instances, there will still be a need to create manual files to accommodate certain types of information, e.g. confidential papers, legally signed documents, some financial documents, records required in hard copy form and publications which it may not be possible to scan due to copyright issues. The unique reference for such files will be created within the EDRM. A similar process to that outlined at 7.1.2 above will apply. However, the EDRM should allow for it to be recorded that a paper file exists and where that file is located. This will then allow a new manual file to be created, using with the appropriate code and title.

8.3. Confidential Files

A public sector organisation may need to create files in the course of their business that have higher levels of confidentiality than ordinary records.

In this instance existing policies, if they exist, should be adhered to and consulted.

When the NICS implementation was taking place the existing policies governing confidential files were applied. This process is described below:

The NICS Public Service Network has security clearance to store information up to and including 'Restricted' classification. Therefore, records that were deemed to need a protective marking of Confidential or above continued to be retained on new manual files. The existence of these paper files was cross-referenced within the relevant TRIM container. All other records relating to the same activity should be stored in a container in TRIM.

Public sector organisations can seek further guidance on Protective Marking Classifications and related policies from PRONI.

9. SAVING DOCUMENTS AND RECORDS

9.1. Why do we need to save documents and records?

It is important to save documents and records as evidence of Departmental business activity and to ensure business continuity. Everything, including e-mails, and all other information that are evidence of a business transaction or decision, should be saved into EDRM.

Saving documents and records within an EDRM also helps to promote a culture of information sharing, making it easier to work and access information quickly. Any information that is not filed within the EDRM cannot be shared or retrieved by other users. For this reason, all information that is required for business/record or audit trail purposes should be stored directly into the EDRM once created.

A document will be finalised as a record within the EDRM when it is completed and is evidence of a business activity. As a document, the creator (and other contributors if required) can edit and update the information contained within. A record secures the content so that it cannot be edited or deleted.

An EDRM should contain the facility to finalise a record:

In TRIM the user will right click and select 'electronic' and then select 'final'. A user may also select to tick the check box 'finalise on saving'. This is the equivalent of placing a paper on a registered file in the old system. Documents should be 'finalised' as soon as is viably possible.

9.2. Revisions in Documents

When documents evolve/develop over a period of time a large number of revisions will accrue. A number of these revisions would be considered minor e.g. formatting, grammatical edits etc and should be removed at appropriate stages in the document's life. Only those revisions that are essential to the final outcome of the document should be retained when the document is "finalised" to become a record.

9.3. Status of Documents

All documents must be saved within the EDRM irrespective of their status. .

9.4. Deletion of Documents

Deletion of documents can only be requested through nominated staff, such as Power Users, Administrators or those staff in an Information Management branch who have been given the task of deleting documents.

9.5. What not to file

While it is important to ensure all important information is retained, there are some instances where information does not need to be retained, for example if it is not business related or is a duplication of a document already in the system.

9.6. Ensuring Completeness

Any public sector organisation needs to be able to provide a complete and verifiable record of its business activities and therefore needs to be able to demonstrate a complete event or transaction from start to finish and all important stages in between. The following are some examples of complete records:

Example 1 – Complete records of a meeting might include:

- ◆ the agenda, minutes, any papers tabled at the meeting and circulation lists.

Example 2 – Complete records of project work might include:

- ◆ Authorisation for events or transactions, including emails, minutes and documents requiring signature;
- ◆ Records that demonstrate how decisions were arrived at, including reports, minutes and advice;
- ◆ Business cases, progress reports, risk analysis, plans and specifications.

Example 3 – Complete records of a report would include:

- ◆ The final report, important stages in its drafting, working papers relating to it, sent in support of, or as evidence that targets have been met.

9.7. Finalising Documents to become records

On an ongoing basis, end users when they have finished editing and updating documents must ensure that they finalise these to become a record within an EDRM. This is the equivalent of placing information on a registered file. Documents should be 'finalised' as soon as is viably possible.

It should be emphasised in the strongest possible terms that end users must finalise their documents.

10. E-MAILS

With the massive expansion in electronic ways of working the use of e-mail has become central to the operation of every public sector organisation. An EDRM will allow for the saving of emails and these should be treated as records of your organisation's business.

If your organisation has existing e-mail policies users should refer to these when dealing with their Outlook inboxes.

NICS realised that a potential problem could arise where users preferred to use Outlook to store their emails rather than TRIM. The approach taken to deal with emails is described below:

Users were instructed to save all relevant emails within TRIM as soon as possible after being received. If the emails were of no business importance they were to be deleted.

To ensure that users did not use Outlook as a storage area, instead of TRIM, a three month rule has been implemented across NICS. This meant that e-mails which have not been saved into TRIM and which remain within the native email application will be automatically deleted from inboxes and associated folders, sent items and deleted items after 3 months.

For those emails that are evidence of a decision or a business transaction and therefore need to be retained as a corporate record, the following guidelines apply:

- ◆ sent emails, whether internal or external, the sender should save the email in the appropriate part of the file plan;
- ◆ external emails received by one person, the recipient should save the email;
- ◆ external messages received by more than one person, the individual with responsibility for the area of work relating to the message should save (assuming they are one of the

recipients). Where this is not clear it may be necessary to liaise with other recipients.

- ◆ conversation strings (where an email 'conversation' is ongoing between a number of individuals), wait until the dialogue has finished or has settled at a reasonable point before saving into TRIM and name appropriately.

Saved emails will often need to be renamed to something meaningful – you do not have to accept the name in the subject field. However it is good practice to copy the original email name or subject line into the document notes field. This will aid retrieval via searching at a later date.

Titling of Emails should also be considered in conjunction with the guidance on naming conventions contained in section 7 above. The name does not need to duplicate information already identified with the email (such as sender, date sent, recipient, date received etc) as these will be automatically generated by EDRM and should not include automatically generated 'FW' or 'RE'.

Where attachments are received with an email, the email message and attachment should be saved together. The name of the attachment should be left unchanged (regardless of naming conventions) as it will be referenced in the main body of the email message.

Sending Attachments

Once all members of staff in the business area are using the EDRM, there should in most instances be no need to send attachments internally to staff. Only a link to the document within EDRM needs to be sent. This will cut down on the size of emails being sent around the Department(s) and therefore reduce the volume of network traffic.

When emails are being sent to recipients outside your organisation attachments will always need to be used.

11. MANAGING SECURITY AND ACCESS

Good information management practice suggests that all information within a file plans should be open and available to all colleagues within that organisation. However restrictions may need to be applied to certain classifications and classes of records for business, confidentiality or legislative reasons.

During the planning for an EDRM implementation careful consideration should be given to the specific security requirements that will need to be bedded into your file plan and then mapped onto the system.

It is recognised that organisations will manage security and access issues in line with their business requirements.

The culture change of giving open access and sharing information will be significant for all public sector organisations. The advantages of this approach will be to enable greater searching capability for FOI and other information requests. It will also facilitate more effective business practices, through the availability of information to colleagues, etc.

The EDRM product chosen by NICS allowed for the creation of security protocols described below

To enable cross-Departmental access across the NICS EDRM network the NICS Managed Service Provider, in agreement with IWG, allowed the creation of NICS Exceptions User profile. This profile gives unfettered access across the TRIM network. To reduce risk a limited number of users, 30 out of 16,500 users, were given this profile.

There are 3 components to TRIM Context's security system:

- ◆ security levels
- ◆ security caveats
- ◆ access control.

Security levels and caveats will be configured and used by the Systems Administrator. Security levels and caveats should be kept to a minimum. Access control can be used both by Systems Administrators and end users.

Security Levels

Security levels represent one of the three components of the TRIM security system. They enable Systems Administrators to control access to the documents and records stored in TRIM. Systems Administrators can apply them to the records (documents), the locations (users) and the classification (file plan).

Security Caveats

Caveats work by selecting certain classifications within the File Plan: containers, users and individual documents that require specific restrictions to be applied – i.e. budgeting information – when the rest of Finance classification is open to all staff.

Access Control

When saving a document, by default it will be available to everyone in the Department (unless other security restrictions have been applied). However the creator of a document has the ability to select document access controls. The creator may wish to place document access controls (at any stage) temporarily while editing and drafting a document prior to opening access to everyone. At this level the creator is able to specify the relevant individual(s) who have access to the documents. Good practice would recommend keeping documents as accessible as possible at all times.

12. AUDIT TRAILS

An EDRM will have functionality that allows for the auditing of actions carried out within the system. It is recommended that all of the EDRM product features are enabled from the start of implementation across your organisation. This will provide a full audit trail of all actions that happen to a document once it has been captured.

13. RECORDS MANGEMENT AND SCHEDULING

13.1. Record Types

An EDRM should be implemented with at least two basic Record Types, these being document and container

The Record Type contains important indexing information about a document, referred to as metadata (see below). It is essential that record types are managed appropriately and conform to relevant metadata standards.

Record Types are the basic building blocks or templates for your records. Through them you can control what your records will be called and what information they will contain.

The purpose of Record Types is for you to define the "shape" of a record series to meet your needs, or to reflect the records you manage.

Record Types ideally should be used to represent the ownership of information.

For the basic record types – the majority of metadata elements must be captured automatically. This will facilitate end users who do not want to fill in endless properties every time they try to save something into EDRM.

The following metadata elements should be included when creating a document and must be linked. The following list contains a selection of some of the most common requisite metadata element:

- ◆ Identifier System ID (mandatory)
- ◆ Title (mandatory) – usually entered as free text¹
- ◆ Creator (mandatory)²
- ◆ Date Created (mandatory) or Acquired (mandatory for e-mail)

¹ Only the title and sometimes ²Creator in this list would need to be entered manually – everything else can be automatically captured by EDRM

- ◆ Date Declared or Registered (mandatory)
- ◆ Addressee (mandatory for e-mail)
- ◆ Disposal (mandatory)
- ◆ Type (mandatory where applicable) – name of record type
- ◆ Physical Location (mandatory where applicable)
- ◆ Rights Protective marking (mandatory where applicable)

Additional metadata requirements are contained in the e-Government Metadata Standard and ISO 23081-1:2006 Metadata for records – principles, and preservation metadata standards, such as PREMIS, which all public sector organisations should take into consideration, especially when developing additional record types for business requirements.

The metadata associated with documents remain in the container, even if a document is deleted, until the container is closed and appropriate disposal actions are applied by information managers. This means a ‘marker’ will be left in place of the document – but it will only indicate the indexing information contained in the usual properties, like the title and date etc. This metadata information will be useful to information managers when applying disposal actions and will only be destroyed/retained at that stage.

14. METADATA

Metadata provides accurate and authentic contextual information about documents and must not be deleted from containers (even by system administrators) that have been identified for permanent preservation or to be appraised by PRONI. Metadata for these containers will be managed (including retention or eventual destruction) as part of the agreed disposal scheduling process and by formal appraisal reports which will be completed with PRONI.

If containers have been identified for destruction after a set period of time in an agreed disposal schedule – documents (and associated metadata) can be sent to a ‘temporary holding area’ for final destruction (regular reports should be kept for possible review by PRONI). Any finalised records (and associated metadata) in these containers must not be deleted (even by systems administrators) for legal and auditing reasons, and will be managed as part of the agreed disposal process.

Metadata can be captured via the EDM's record types – 2 standard record types were established during the NICS implementation, i.e. container and document. It is recommended that as many metadata elements as possible are captured automatically by EDM.

Although public sector organisations will have the flexibility to capture specific metadata elements according to business needs (in different business related record types), they must also comply with any metadata standards set by Government requirements and PRONI.

Metadata also exists about the file plan, users, auditing and security permissions etc – this information requires careful management and documentation over time. Any restructuring or change in ownership that affects the 'class' levels of the file plan will affect disposal arrangements and must be agreed in advance with PRONI (via reports, disposal schedules or appraisal reports).

15. SCANNING

Increasingly, information is now received by public sector organisations electronically, but there is still a need to manage hard copies which are received.

As standard practice, staff should request an electronic copy of a document, where it is available, either as a download or an email attachment, from the sender. This should then be stored in the appropriate container within the EDRM.

Where an electronic version is not available, the paper version should where possible be scanned. (Users should be aware of copyright or other legislative considerations before scanning a document.)

It is recommended that organisations use Multi-Function Copiers [MFCs] (e.g. combined scanner, printer and photocopier) particularly when replacing existing equipment. The use of MFCs provides a cost effective approach to the provision of copying facilities. .

Departments should conduct a risk analysis prior to recognising any scanned documents as the record. This analysis should consider the pros and cons on the use of scanned documents, taking account of specific business requirements. In some cases the analysis may need to filter down to business area level, particularly in instances where there are legal or financial issues/consequences in the day to day business.

When deciding what information needs to be scanned and saved within an EDRM the following guidance will apply:

- ▶ Paper that contains information that should be shared with other staff needs to be scanned and saved;
- ▶ Some documents or records are only legally binding if preserved in paper form. In all such cases, the paper version must not be destroyed until legal advice on its use is sought. Users may wish to make a scan of such documents and records if they wish to circulate

them electronically, but the paper original must still be safely retained and the paper version, rather than the scanned version, will still be regarded as the legal version. The TRIM version should be referenced to indicate that the recognised 'record' is the manual copy, and to show its location.

- ▶ Not every piece of paper can be scanned, such as large documents or records or bound documents/ books etc. In these cases it may be useful to scan and save the first few pages and place a note within EDRM to indicate where the entire physical document resides.

The following Principles should be applied when considering the scanning of documents.

Principle 1: Physical documents that form a record of a public sector organisation's activities should be captured electronically within the EDRM system, if it is cost effective, physically practical, and within the constraints set out in this section.

Principle 2: Copyright legislation and the terms of agreements relating to documents should be considered before scanning takes place.

Principle 3: Where an original source document is scanned, the source document should be destroyed unless there is an essential reason why it must be retained.

Principle 4: Procedures should be in place to ensure that the scanned image is an accurate and complete copy of the original source document and is finalised when stored in TRIM.

Principle 5: All staff will take responsibility for complying with scanning policies and procedures.

Public sector organisations should be aware of the existence of the standard, BS10008, which sets out the legal admissibility of electronic and scanned documents. The standard updates the existing guidance to cover what a public sector needs to do to ensure the legal admissibility of its scanned and electronic documents and whether or not these documents would be accepted by a court of law. To ensure the admissibility, information needs to be managed by a secure system throughout its lifetime (which can be for many years). Where doubt can be placed on the information, the evidential weight may well be reduced, potentially harming the legal case. The guidance ensures that any electronic information required as evidence of a business transaction is afforded the maximum evidential weight. The process is based on the specification of requirements for planning, implementing, operating, monitoring and improving the organization's information management systems.

Furthermore, the standard specifies the requirements for the implementation and operation of electronic information management systems, and to the electronic transfer of information from one computer system to another,

addressing issues relating to the authenticity and integrity of the electronic information.

16. PRINTING

Users of an EDRM should, where possible and/or appropriate, avoid printing hard-copy versions of electronic documents and records. Rather, users should be encouraged to read and review documents electronically.

However, it is recognised that from time-to-time it may become necessary for users of EDRMs to print electronic documents and/or records (including emails).

Documents contained within an EDRM should only be printed in instances when:

- ◆ papers are required for internal meetings when it is inappropriate for all participants to view on-screen;
- ◆ papers are required for external meetings – e.g. with external partners or members of the public; and
- ◆ documents need to be distributed to external sources – e.g. sent in hard copy form to a member of the public in response to an FOI request.
- ◆ when the size or nature of the document makes it impractical to view, consider or work on its content on screen

To maintain adequate version control, all printed versions of the electronic document should be clearly marked as a copy. .

Once a document has been printed, the individual working with the printed copy should decide whether or not any amendments and/or additional notes should be placed on record, for example comments on a policy document. If no amendments or notes are necessary then any unnecessary printed copies should be destroyed.

However, in situations where changes and or notes are necessary, then the individual should ensure that such amendments are recorded in the EDRMS as part of the full contextual record of events. Options available may include:

- ◆ scanning the printed copy with amendments indicated and registering this newly created image as a rendition within the EDRM with a marker to the original electronic document; and
- ◆ reviewing the agreed amendments and/or notes and creating a new electronic version of the original document or record incorporating such changes.

17. STORAGE DEVICES OUTSIDE OF EDRM SYSTEMS

The EDRM should be the standard repository for the storing of corporate information across a public sector organisation.

However, it may be necessary for business reasons information can be temporarily copied onto a temporary storage device, such as a USB Pen Drive.

In NICS, the use of temporary storage devices is a Departmental matter and governed by current Departmental ISU policies. If your organisation does not have a policy covering the use of external storage devices guidance can be sought from PRONI.

18. DISPOSAL SCHEDULES

Experience of the NICS implementation has taught that it essential that disposal and retention requirements are considered alongside file plan requirements during the planning phase of any EDRM implementation.

An EDRM will have functionality that will allow for the creation of disposal schedules. The actual building of disposal schedules is a relatively straightforward action only requiring training in the actual functionality itself.

However, the application of roles and responsibilities regarding disposal and retention in the and the operation of disposal and retention is much more complicated and resource intensive.

PRONI, in conjunction with NICS Departments, is currently involved in a project to address disposal and retention requirements within TRIM. Guidance will be posted on the PRONI website upon completion of this project.

19. TRANSITION PROCEDURES

19.1. Introduction

The introduction of the EDRM will mean a change in the current file registry system. From the EDRM agreed “go live” date, the existing file classification within the relevant business area will close and a new classification system based on the approved File Plan will be introduced. It is recognised that Departments operate their file registry systems in different ways and that Departments will need to consider this on an individual basis. Please see guidance below.

19.2. Papers currently held for filing

To aid the closure of existing files and to aid compliance with Freedom of Information it is essential that staff ensure that any papers currently being held and pertaining to registered files are filed immediately.

No documents produced or received after the “go-live” date will be filed in existing paper files.

19.3. Closure of existing paper files

Procedures need to be put in place by public sector organisations to facilitate the closure of all existing paper files.

Closing sheets need to be inserted on files and the closure recorded on the relevant index card.

Any new information will be stored in the corresponding container in the EDRM.

If, after referring to the EDRM Guidelines, it is identified that a paper file will still be required, a new file will be opened using the new File Plan structure and cross-referenced in the EDRM to any old files to ensure continuity of access.

Consideration needs to be given to introducing a system or process to distinguish any necessary new files from the previous file system, e.g. change of file colour or other suitable process.

In order to facilitate closure action, it is recommended that files should not be removed from a registry or storage facilities during this period. However, systems should be implemented to allow staff access to files for reference purposes during this period within the registry/storage environment. If it is absolutely necessary to remove the file a record should be maintained to record the removal (date, assignee, etc). These files should be returned to registry/storage as soon as possible but essentially within 3 working days. Staff should monitor return of files, and follow up where necessary.

On closure all files with a classification of Confidential or above will be returned to the originator to be held securely and reviewed at an appropriate time after EDRM implementation.

All files with markings of Restricted and below will be held in Registry/storage until six months after EDRM implementation. At this time it is recommended that files will be reviewed and, depending on business needs, may be sent to long term storage.

All papers should be filed immediately. However, it is essential that staff ensure that an additional check is made soon after implementation to ensure any further outstanding papers produced prior to the go live date are filed properly.

19.4. New File Classification

From the 'go live' date a new file classification system will be used. This will be the same system for both electronic containers and paper files. All electronic documents will be filed in containers in TRIM.

The levels of the file plan will form the title of the containers and will be similar as in the format of the example below:

Function/	Sub-function/	Activity/	Task
Human Resource Management/	Pay/	Overtime/	Overtime claims

A revised Alpha/Numeric system to identify and code containers will also be established. These will be automatically generated by TRIM.

The majority of records produced will be electronic (including e-mails) and will be saved directly to the EDRM.

Paper files will only be required in exceptional circumstances.

Confidential documents received in hard copy will be held in paper files. In these instances a marker/reference will be inserted on the EDRM indicating that relevant documents are held on a paper file and detailing the location. The title of the paper file will mirror that of the equivalent container within the EDRM. A marker will be placed to show that a paper file is also in existence and will be cross-referenced.

Initially, Information Management Branches, or those tasked with information management within a public sector organisation, will create new electronic containers at the storage level of the file plan, but it is anticipated that this will be delegated to Power User level at branch/office level.

If a new paper (hybrid) file is also required, a marker for this should be set on the EDRM and a link sent to Registry/EDRM Administrator who will open the paper file and inform the branch representative when the task is completed.