

## **EDRM Tender Appendix A**

### **Description of current system**

#### **1. EDRM DESCRIPTION**

- 1.1 TNA's current EDRM solution is Objective ECM version 8.3.3. It is the only document management in use, and so it is considered the sole authoritative repository of TNA corporate information.
- 1.2 All metadata including document names and dates is held in a Microsoft SQL Server database, and documents are held separately in a Windows filing system.
- 1.3 The EDRM is hosted in-house on a secure network. Users are unable to access the EDRM from outside this network. Most access is therefore on-site, but users may also access the system remotely using designated laptops and logging into the network through a secure session.
- 1.4 The EDRM is maintained by a server administrator who is a full time member of TNA staff. There are two members of staff who serve as administrators, with full access to all information and functions, and who enforce information management policy. There is additionally one or more super users in each TNA department, around thirty in all, who have elevated access to disposition functions and carry these out in addition to their substantive roles.
- 1.5 Users access the EDRM via client software installed on their devices. They may also browse the file plan via Windows Explorer and carry out common actions such as saving and editing documents.
- 1.6 Users log on to the EDRM via single sign on (SSO) with Active Directory, but roles and permissions are granted via group management within Objective.
- 1.7 Email is hosted in-house on Microsoft Exchange 2013, and accessed by users mainly via Outlook 2010, but also via Blackberry and iPad.
- 1.8 TNA currently uses Windows 7 desktops, laptops and thin clients with Office 2010 and Internet Explorer 11. A small number of users also have portable devices i.e. a Blackberry or iPad but are unable to access the EDRM from these.
- 1.9 Within twelve months, it is anticipated most users will use Windows 10 desktops or touchscreen laptop devices with Office 2016, Internet Explorer 'Edge' and alternative browsers such as Google Chrome and Firefox. A browser-based Office suite may also be available as an option to users.

#### **2. USAGE STATISTICS**

- 2.1 TNA uses its EDRM for its corporate information. Archival records held by TNA under the Public Records Act are stored and managed in a separate system and are not subject to this tender.
- 2.2 **Number of users:** Currently 540 active and licenced users. The system holds a metadata record of 2400 past and present users. There are approximately another 80 staff members who do not have access to the system because they do not have regular access to a computer, although they do have access to the intranet and shared drives.
- 2.3 **Volume and number of documents:**

The table below shows the number and volume of documents held in the system and the amount of growth.

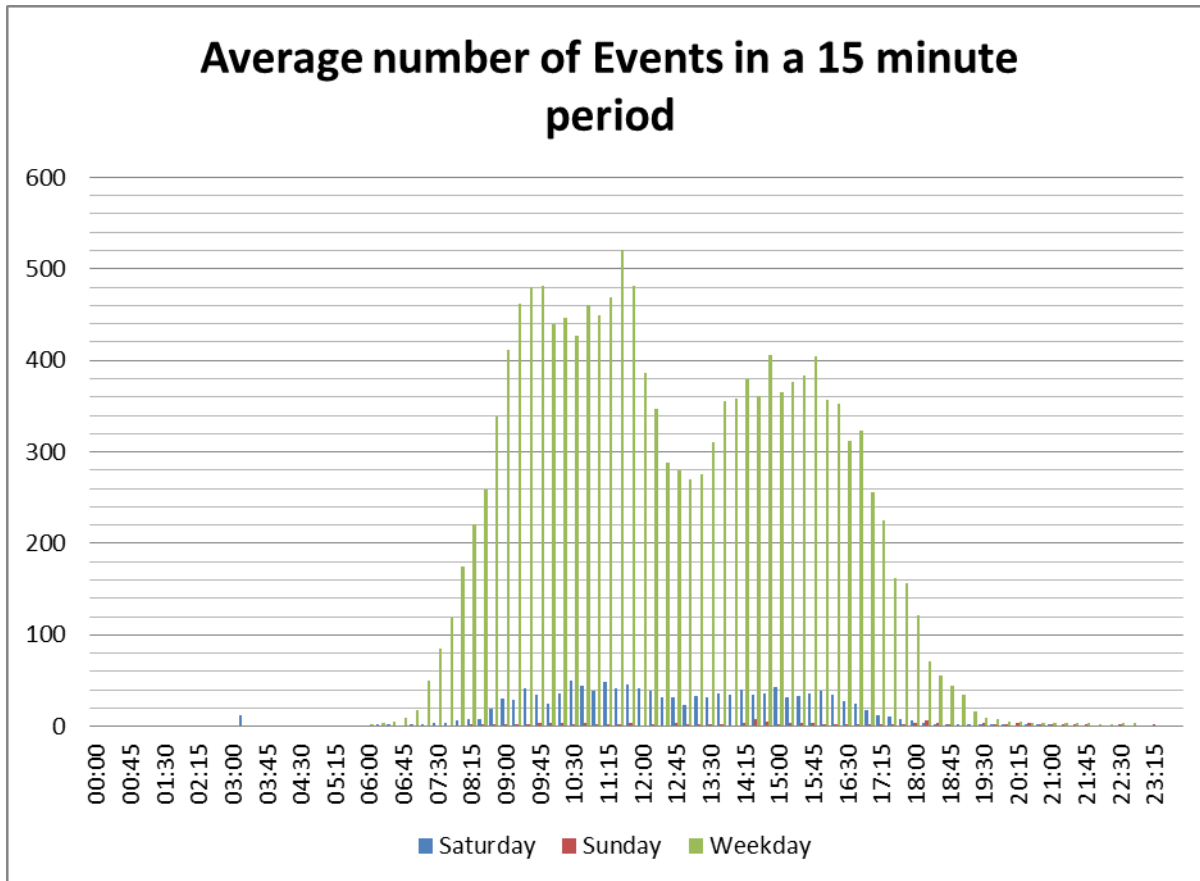
Date	No. non-emails	No. emails	Total number of document versions	Total Volume (Gb)
01/09/2015	1269297	1781664	5171367	1369
01/12/2015	1280338	1798999	5237478	1407
01/03/2016	1292722	1825750	5310842	1442
01/06/2016	1313668	1873401	5360966	1484
01/09/2016	1325162	1907405	5440565	1523

(Emails are .msg documents and any embedded attachments; "non-emails" are all other document formats. Overall the system is approximately 60% email, 33% Office documents, 4% images and 3% other, by document count. "Total number of document versions" is for email and non-email, and also includes previous document versions still available in the system).

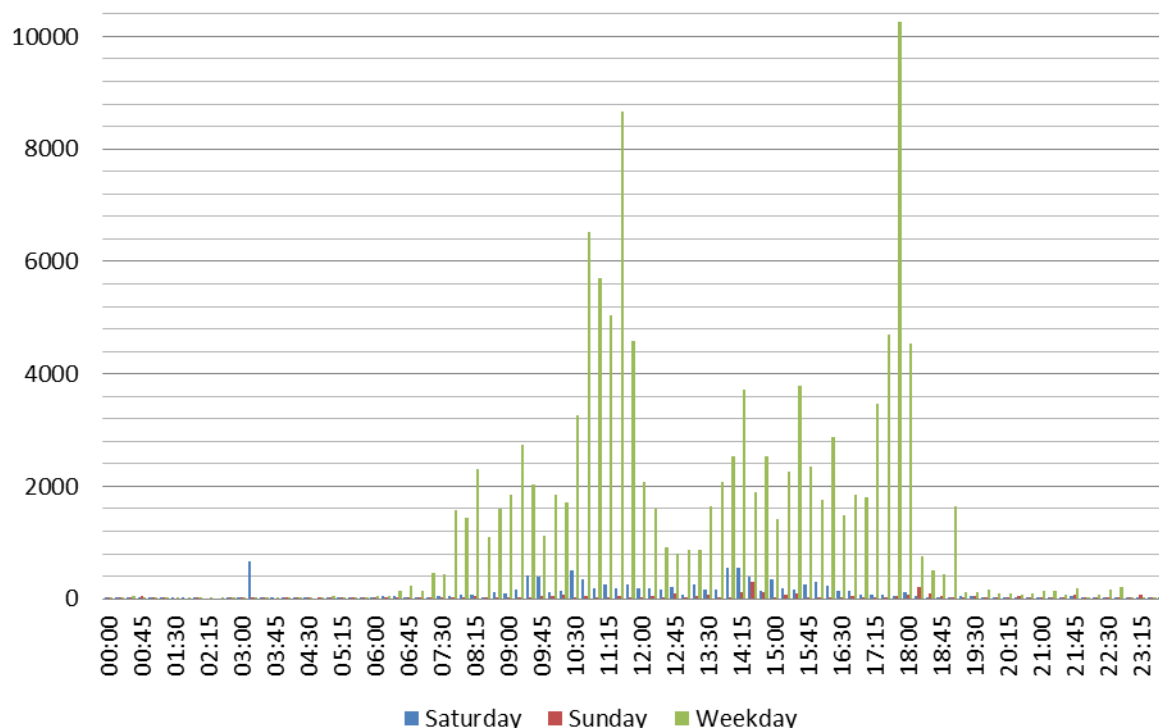
There are currently around 300,000 container objects, including folders and "aggregations" (see section below on information structure).

## 2.4 Activity over time of day:

The charts below show the average number of events occurring in a fifteen minute period, and the maximum number. Events include opening, creating, saving and deleting documents; opening, creating, deleting folder objects; searching; logging in; all logged activity. The data is 52 weeks from 31 August 2015 to 29 August 2016.



## Maximum number of Events in a 15 minute period



### 3. INFORMATION STRUCTURE

#### 3.1 Business classification scheme:

Policy is for all information to be saved into a single corporate file plan. The file plan is organised on a departmental (structural) basis. The structure of the top three levels is controlled by records management administrators. These top level folders are known as classification folders. Below this, users create and manage "files", which are analogous to paper files in that they are intended to group related objects together<sup>1</sup>. Documents cannot exist outside these files. Records management administrators apply retention schedules to these aggregations on a functional basis, and close these aggregations to make them read-only and to start the retention schedule period. While a file is open, users are able to create, delete, edit, rename or move documents in that file. Users are permitted to create subfolders within aggregations, but are prevented from creating further levels, which means they cannot create a subfolder within a subfolder. This helps to restrict the size of each aggregation. The intention is to ensure the documents are of a logical grouping and the retention schedule is appropriate to all its contents, and that there is an available trigger to start the retention period. Similarly, it is impossible to create an aggregation within an aggregation. Annualised filing is encouraged where appropriate.

An example structure is below:

<sup>1</sup> Much like [http://moreq.info/files/moreq2010\\_vol1\\_v1\\_1\\_en.pdf](http://moreq.info/files/moreq2010_vol1_v1_1_en.pdf), figure 1i, p.26.

- > Department 1
  - > High level functions, e.g. .
  - > Advice
    - ◆ Internal Advice 2014 🔒
    - ◆ Internal Advice 2015 🔒
    - ◆ Internal Advice 2016
      - Case 1
        - Email
        - Email
        - Document
      - Case 2
      - Case 3
      - (etc.)
  - > Projects - complete
    - ◆ Project 1 🔒
      - Accreditation
        - Document 1
        - Document 2
      - Communications
      - (etc.)
    - ◆ Project 2 🔒
  - > Projects - ongoing
- > Department 2 ...
- > Department 3 ...
- > ...
- > Department 30 ...

*Key to symbols:*

- > The top level containers (classification folders), set by information management administrators.
- ◆ File containers which contain the documents.
- 🔒 File containers that are closed, which makes them read-only and triggers the start of the retention period.
- Optional subfolder within the aggregate container.
  - Emails and documents inside the folder.

Document and container names may contain punctuation and higher characters, including those not normally permitted in a Windows system, such as colons, backslashes, forward slashes, pound currency symbols, and European accented characters. Aggregations must be uniquely named in their classification folder, but there are no other constraints on unique names. This means that a document's name and path is not necessarily unique. There are no technical constraints on the length of document names or container names, which means the total length of a document's name and path may exceed 255 characters.

The file plan is occasionally restructured when departmental changes merit this. This may involve moving a function from one department to another department, or a function may be promoted so that it is moved to the top level and deemed to be a department of its own. In these cases, the structure further down is otherwise left intact, with internal references and links remaining valid, and carrying out the operation is a matter of drag and drop. This work is done by records management administrators.

### 3.2 **Government Security Classification scheme:**

All data held in the EDRM is of the OFFICIAL classification, including OFFICIAL-SENSITIVE. Users have the ability to set protective marking metadata on documents to denote sensitivity, and this metadata is available to search on.

### 3.3 **Permissions:**

Users are organised into permissions groups according to department, and occasionally smaller teams or project groups. Permissions for opening, editing, deleting and seeing the existence of documents can be applied or revoked at any level of the file plan, to individual users or to groups, and permissions settings are inherited down through the file plan structure unless specifically overridden.

The overriding principle with permissions is openness and sharing. Most users can see and open most documents, and documents only have more restricted permissions where there is a particular need-to-know security requirement. There are a small group of users excluded from this principle, who can access only those documents or folders for which they have explicitly been given permissions.

Administrators have full access to all documents and functions. They are supported by departmental super-users, who have full access to all documents within their departmental area, and can carry out retention actions.

### 3.4 **In place records:**

Users do not declare documents as records. Instead, all documents including drafts are saved in the file plan, and retention is applied according to the container ("file") in which they are placed. While containers are active, documents may be deleted, edited, renamed or moved, where permissions allow. Containers are closed according to specific criteria (e.g. end of year, superseded or end of project), which makes them read-only and triggers the start of the disposal schedule period. At the end of the period, the aggregations are deleted or transferred to an archive.

### 3.5 **Metadata:**

The system automatically generates metadata for creator and dates. Additionally, email header information is automatically extracted and made available as structured metadata for emails. Users manually add protective marking metadata from a set list. Some other custom metadata fields are available but infrequently used and of negligible value.

### 3.6 **Home areas:**

Every user has a personal filing area in the EDRM, which is accessible only by themselves and administrators. Users are encouraged to use this area only for rough drafts or data personal to themselves. Users do not share documents directly from their Home area; instead, they move these documents to an appropriate location in the main file plan. Approximately 67% of documents are saved in the file plan; approximately 90% of open/edit activity concerns documents in the file plan.

### 3.7 **Navigation:**

The file plan is presented as nested folders with different symbols according to container type. Users can browse or search based on keywords or metadata to find records. Users can set up cross-referencing links, aliases and shortcuts for documents and document containers. These references are based on the object's unique ID number, which is persistent even when the object is moved, renamed or deleted.

### 3.8 **Network drives and other information systems:**

Network/shared drives are in use for databases, programming/web development files, image collections, and other documents which cannot be saved in the EDRM due to size or format.

TNA has an in-house intranet based on Confluence. All staff members have access to this. It is used primarily for news, staff information, and published versions of internal policies. Staff members create pages through a WYSIWYG-type web interface. Policies are drafted in the EDRM and published on the intranet via a manual export and upload process.

Some departments at TNA use Microsoft Dynamics CRM. Users may track email correspondence through the CRM, but they are required to separately file important email to the EDRM. Users can link to EDRM documents from the CRM, such as meeting minutes, using a URL.