Annex VII

TECHNICAL REQUIREMENTS FOR THE Implementation of the Integrated Information System Concept for the Ministry of Foreign Affairs and European Integration

The document was created as part of the United Nations Development Programme's Project "Building Institutional Capacity of the Ministry of Foreign Affairs and European Integration"

CONTENTS

1. INTRODUCTION

Full Name: ***Ministry of Foreign Affairs and European Integration - Integrated Information System***

Short Name: ***MFAEI IIS or IIS***

Through "Building Institutional Capacity of the MFAEI" project, United Nations Development Programme (UNDP) is assisting the Ministry of Foreign Affairs and European Integration (MFAEI) in strengthening the institutional capacity of the Ministry of Foreign Affairs and European Integration (MFAEI) in the process of achieving its European Integration goals and commitments.

Currently, the ordinary activities of MFAEI staff include development, expedition and processing of large amounts of data, under supervision of MFAEI leadership, coordination with MFAEI subdivisions and subordinated structures, monitoring implementation of international treaties and international agreements Republic of Moldova is part of.

An increase in the efficiency of the actions above is possible by implementing an Integrated Information System (IIS), providing a proper environment for cooperation, document creation and storage, which would increase overall organizational efficiency, ensure secure access to truthful and up-to-date information, accelerate shared internal processes and facilitate information exchange irrespective of user location.

Apart from that, the IIS will offer a set of tools to organize decision-making policy, control and manage document workflows, provide reporting facilities etc.

In order to ensure authenticity and genuineness of decisions made by MFAEI management bodies, IIS will rely on Digital Signature Infrastructure.

2. GENERAL

The requirements mainly address the software needs of the Integrated Information System so the solutions also concentrate on this aspect of the system. Still, it is acknowledged that the provider relies as much of on existing hardware and networking equipment in MFAEI ownership. Additional hardware and networking equipment that MFAEI needs to acquire in order to achieve all system capabilities is identified.

The document lists the specifics important to MFAEI operation. Still, there are multiple related features that are present in Commercial Off-The-Shelf Software and that are not listed in these requirements. While fully custom built systems are not prohibited, a strong preference will be given to solutions based on commercial off-the-shelf software. In case a single COTS package that covers all the MFAEI needs is not available the solution should be built by integrating a series of such packages as well as custom developing the components that are not available.

Finally, a series of customizations will be applied to the integrated solution to accommodate specifics of the MFAEI. These will be limited in scope and will be agreed upon during the detailed analysis and design phases of the project. The MFAEI expects to further customize the solution and to adjust it for less frequent processes or its changing needs in the future. The MFAEI expects that the different components will have documented APIs for programmatic extension when needed. The ease of customization procedures and their extent will be an important advantage when choosing the solution.

The MFAEI understands that the success of such a project - an Integrated Information System deployment - is dependent on its acceptance and everyday use by its personnel. While the requirements include extensive personnel training and training materials the MFAEI recognizes that this alone is not sufficient. The MFAEI expects guidance in this area and strong preference will be given to solution providers that can:

- **demonstrate similarly deployed systems for a group of early adopters**
- **consult MFAEI Top Management in the adoption steps to take and incentives to offer**
- **suggest business improvement initiatives that will improve IIS acceptance.**

3. REFERENCES

The technical requirements are developed based on the MFAEI Integrated Information System and this document should be used extensively as reference to other legal, normative, practice and guideline documents.

These technical requirements are based heavily on good international practice in this field and these are mentioned specifically here:

- ***Electronic Information*:**
  - **Guidelines on best practices for using electronic information by DLM Forum, http://dlmforum.typepad.com/gdlines.pdf**
- ***Document/Records Management Systems*:**
  - **MoReq2 - Model Requirements Specification for the Management of Electronic Records, http://www.moreq2.eu/**
  - **DoD 5015.02-STD RMA Design Criteria Standard by US Department of Defence, http://jitc.fhu.disa.mil/recmgt/standards.html**
  - **ISO 15489 Information and documentation - Records Management by ISO, http://www.iso.org/iso/catalogue_detail?csnumber=31908**
- ***Metadata standards*:**
  - **DCMI Element Set (ISO Standard 15836) published by The Dublin Core Metadata Initiative, http://dublincore.org/**

4. TERMINOLOGY AND ABBREVIATIONS

4.1. Abbreviations

COTS - Commercial Of the Shelf Software

EDMS - Electronic Document Management System

ERMS - Electronic Records Management System

IIS- Integrated Information System

MFAEI - Ministry of Foreign Affairs and European Integration

4.2. Key Terminology

Capture (verb)

(1) The act of recording or saving a particular instantiation of a digital object.
(2) Saving information in a computer system.

Case file - A file relating to one or more transactions performed totally or partly in a structured or partly-structured way, as a result of a concrete process or activity.

Note: there is no universally-accepted definition of these terms, nor of the distinction between case files and the other kinds of files often managed by an ERMS.

Class (noun) - The portion of a hierarchy represented by a line running from any point in the *classification scheme* hierarchy to all the files below it.

Note: this can correspond, in classical terminology, to a "primary class", "group" or "series" (or sub-class, sub-group, sub-series etc.) at any level in the classification scheme.

Classification - In records management, the systematic identification and arrangement of business activities and/or *records* into categories according to logically structured conventions, methods, and procedural rules represented in a classification system.

Classification scheme - A hierarchic arrangement of classes, files, sub-files, volumes and records.

Document (noun) - Recorded information or object which can be treated as a unit.

Electronic record - A *record* which is in *electronic* form.

File (noun) - An organised unit of *records* grouped together because they relate to the same subject, activity or transaction.

Note: this is the Records Management usage of the term *file*. It differs from the IT usage.

Metadata - Data describing context, content and structure of records and their management through time.

record (noun) - Information created, received, and maintained as evidence and information by an organisation or person, in pursuance of legal obligations or in the transaction of business.

sub-file - Intellectual subdivision of a file.

Volume - A subdivision of a *sub-file*.

4.3. Key Concepts

The key concepts required to understand this specification are:

Record and electronic record

Records can be viewed as consisting of:

- **content;**
- **structure;**
- **context;**
- **presentation.**

The content is present in one or more physical and/or electronic documents that convey the message (the informational content) of the record. These are stored in such a way as to allow future users to understand them and their context. This view implies that a well-managed record consists of, in addition to the content of its document(s), information about its structure and metadata that provides information on its context, and its presentation to users. The presentation depends on a combination of the record's contents, structure and (in the case of electronic records) the software used to present it.

A record is made from one or more electronic documents. These documents can be word processing documents, e-mail messages, spreadsheets, moving or still images, audio files or any other type of digital object. The documents become records when they are set aside, that is, "captured" into the system. Upon capture, the records are "classified", that is they are assigned codes corresponding to the classification scheme class to which they belong, allowing the system to manage them. The records usually are assigned to a file – though not always.

For preservation purposes, it is necessary to appreciate that electronic records are often made up of several components. Each component is an object managed by a computer operating system, and they may be in different formats; but they are all needed together to make up a record. Not all records have more than one component; for example, most word processing documents are made of only one component. An example of a record with several components is a web page with text, graphics and style sheets; it is not unusual for a web page to contain one HTML component, dozens of JPEG image components, and a handful of CSS (cascading style sheet) components.

An essential quality of records is that their informational content is fixed. One consequence of this is that no action carried out on electronic records can be allowed to interfere with the relationships between its components; in other words, all actions carried out on any

record must preserve the correct relationships between all its components. So, for example, whenever any record is moved or copied, it must be moved or copied in a way that keeps all its components and all their relationships.

Authoritative Records

ISO 15489 describes an "authoritative record" as being a record that has the characteristics of:

- **authenticity;**
- **reliability;**
- **integrity;**
- **usability.**

As explained in ISO 15489, the aim of all records management systems should be to ensure that records stored within them are authoritative. Summarising, an authoritative record:

- **can be proven to be what it purports to be;**
- **can be proven to have been created or sent by the person purported to have created or sent it;**
- **can be proven to have been created or sent at the time purported;**
- **can be depended on because its contents can be trusted as a full and accurate representation of the transactions, activities or facts to which it attests;**
- **is complete and unaltered;**
- **can be located, retrieved, presented and interpreted.**

The requirements are designed to ensure that records stored in a compliant system are authoritative. However, compliance with these requirements alone is not sufficient; the existence of, and compliance with, corporate policies is also required.

Electronic File, Sub-file and Volume

Paper records generally are accumulated in physical files, contained in paper folders. The paper files are aggregated into a structure, or classification scheme. In an ERMS electronic records can be managed as if they are accumulated in electronic files and stored in electronic folders. Strictly, electronic files and folders need not have a real existence; they are virtual, in the sense that they do not really "contain" anything; in fact they consist of the metadata elements of the records assigned to them. Further, in many cases, there need be no real distinction in the electronic system between file and folder.

In some environments it is useful to divide files into sub-files. The division into sub-files is an "intellectual" one; that is it requires human input to decide into which sub-file a record should be stored. A sub-file is therefore a division of a file by type of content. As a result, a sub-file can be used to permit the application of a different retention and disposition schedule to a set of records within the file.

Regardless of whether sub-files are used or not, files are sometimes divided "mechanically" into file volumes, according to predetermined conventions. This practice originated with paper files, in order to restrict them to a manageable size and weight. It can be continued with electronic files, to limit them to a manageable length for appraisal, transfer, or other management purpose. It is especially appropriate for the management of files which are open for long periods and/or which grow to contain a large number of records.

Classification scheme

Records management aggregates files in a structured manner, and good practice dictates that this structure should reflect business functions. The representation of this aggregation is referred to as a "classification scheme". The classification scheme is commonly a hierarchy.

Just as files appear to exist even though they are really no more than aggregations of records, so higher levels of the classification scheme hierarchy seem to exist, though they are no more than aggregations of files and/or lower levels. As with files, this specification states requirements for the hierarchy without mandating the manner in which it is implemented.

Class

The specification uses the term "class" to describe the portion of a hierarchy represented by a line running from any point of the hierarchy to all the files below it. The term class therefore corresponds to a "group" or "series" (or sub-group, sub-series etc.) in some texts.

Visually, a class of a hierarchy corresponds to a branch of a tree. A class may thus contain other classes, just as a series contains sub-series and sub-sub-series.

The specification also uses the term "class" to mean all the files, records etc. assigned to a class. This double usage is intentional, and the appropriate interpretation of the term is always clear from the context.

The specification uses the terms "child" and "parent" to describe the relationships between entities. A "child" of one entity is an entity that is below it in the hierarchy (in other words, is a descendant entity). A "parent" of one entity is an entity that is above it in the hierarchy.

Capturing Records

Documents made or received in the course of business become records when they are set aside, that is, "captured" into the system. During capture, the records are "classified", that is they are assigned codes corresponding to the class to which they belong, allowing the system to manage them; and they are also assigned a unique identifier.

In many cases, documents that are set aside, or captured, become records by being bound to a business process, as often happens in a workflow. For example, when an invoice is raised it should automatically cause a record to be captured. In other cases there may be a policy that every document relating to a business matter must become a record, even if it does not formally participate in a business process. In yet other circumstances however, the process of capture will be initiated selectively by a user. In some situations, the drafts will be deemed to be significant and will become records, whereas in other situations drafts will not become records.

User and Administrative Roles

The specification uses the concept of "user" to mean any person with valid permissions to work using the system. Therefore anyone who is allowed to log on is a user, including administrators. However, the distinction between administrators and other users can be complex and is sometimes unclear. Therefore we use the concepts of "roles" in defining many requirements.

There are two kinds of roles:

- **"user roles" and**
- **"administrative roles".**

Administrative roles take actions related to the management of records themselves; their interest is in managing records as entities rather than their content or business context. They also manage the hardware, software and storage, ensure backups are taken and manage the performance of the system.

Unlike administrative roles, user roles have access to facilities which an office worker or researcher needs when using records. This includes adding documents, searching for and retrieving records; their interest is primarily in the contents of records rather than their management – in other words, they are interested in the business processes evidenced by the records.

5. SYSTEM DESTINATION

The system is designed to automate processes within MFAEI and serving MFAEI employees and institutions with which it is related. The Concept Paper for MFAEI IIS sets forth the following goals:

- **Implement a secure and protected collaboration environment, which offers collaboration means to MFAEI employees no matter where they are physically located, as well as means to ensure informational integration with external systems;**
- **Introduce a reliable and efficient document management system powered by workflow procedures in order to ensure fast documents delivery to recipients and deadline monitoring;**
- **Offer accurate and quick data in order for MFAEI employees to fulfil their functions;**
- **Reduce image risks caused by delays, contradictory messages or actions due to lack of information from decision makers part;**
- **Generation of data repositories related to the activities of the Ministry and its subdivisions, in order to make MFAEI activity more efficient;**
- **Transparency of activities and decisions within MFAEI;**
- **Offer authentic, true, up-to-date and consistent information to all involved actors;**
- **Reduce response time and offering support for decision-making;**
- **Fast, guaranteed access to data and information irrespective of location;**
- **Continuous information of population;**
- **Homogenize information, messages and actions in subdivisions and representatives;**
- **Reduce costs, increase quality and diversity of communication means;**

It is important to note that the Concept paper for MFAEI IIS identifies a series of specialized systems - eDiplomat, eConsul, Bookkeeping and Accounting, Budgeting, Public Procurements. Current requirements document does not provide details about these specialized systems since these are extensive and require specialist approach to them. This document assumes that the specialized systems will be analysed and developed independently. More so, it is known that such projects have already started for eDiplomat, eConsul, Accounting and are at various stages of completion.

6. BUSINESS MODEL

6.1. IIS main processes

The IIS main process is to serve as a communication platform that allows MFAEI personnel to rely on it as their main workspace where they

- **React to external events and register them as actionable items that need approval**
- **Get approval from superiors before proceeding**
- **Create, store and collaborate on responses**
- **Follow the review and approval procedures for each type of response**
- **Capture approved documents as records (records have a permanent nature and cannot be modified)**
- **Classify captured records to a designated file/folder according to the record's type**
- **Issue copies of the response/record for distribution**
- **Ensure proper archival and disposition of old records.**

Mostly this process is semi-structured and thus is driven by personnel. Increasingly, the regulated processes for particular types of documents will become structured and rigorously driven by the IIS. Additionally, this semi-structured process imposes authorisation restrictions on personnel. Also, it is expected that authenticity of records will become increasingly reliant on digital signature.

A series of important business processes that the IIS should facilitate include:

- **Arrangement, preparation and organization of High Level Officials visits**
- **Bilateral relations, activities and events (politic, economic, collaboration etc)**
- **Consular affairs**
- **European Union - Republic of Moldova relations**

- **Foreign diplomatic corps and journalists accreditation**
- **Foreign Diplomatic Mission transportation unit accreditation**
- **International and Regional organization relations and participations**
- **International reunions, conferences, seminars organisation or participation**
- **International Security**
- **Transnistria conflict resolution plans.**

The exact list of business processes and details to be supported by IIS will be agreed upon during project analysis and implementation.

6.2. Business roles

The business roles can be identified from the list of MFAEI employees and the organisational structure:

- **Minister or Deputy Prime Minister,**
- **Deputy Minister,**
- **Heads of Diplomatic Missions,**
- **Head of departments,**
- **Departments users,**
- **Head of directions,**
- **Directions users,**
- **Users from auxiliary subdivisions – logistics, human resources, budget and accounting,**
- **Users from Foreign Missions – Embassies, Consular Offices, Permanent Representatives, Delegations,**
- **Local experts,**
- **Foreign experts,**
- **Trainees,**
- **Visitors.**

6.3. Services

No.	Service name	Notes
1.	Intranet	The single point of entry to IIS. This is maintained as a Web Application available to all internal personnel. Authorisation restrictions apply when accessing parts of the Intranet.
1.1.	Virtual Private Network	The service that allows remote and "on the go" personnel to get access to MFAEI internal network. This service imposes technical security measures that make the distributed nature of users transparent.
2.	Document management	The service that allow users to manage in a centralized way the electronic documents.
2.1.	Document version control	After each document modification the system will store the new version, and the user will write some notes describing changes.
2.2.	Document based workflow definition	Defining the steps / people who have to pass the document to be examined and if necessary to apply notes, changes, signatures
2.3.	Search and Retrieval	Allow users to locate metadata, classes, files, sub-files, volumes or records.
2.4.	Presentation	The system must be able to present class, file, sub-file, volume, document or record contents.
2.5.	Referencing	Allow users to process the entities, retrieve, refer to, and use the entities.
3.	Capturing and Declaring Records	Capture information (records, metadata, and in some cases documents) and saving it in the computer system according to the classification scheme.
3.1.	Classification Scheme and File Organisation	Allows an electronic record to be stored together with other records that provide its context, by defining the way in

No.	Service name	Notes
		which the electronic records will be organised into electronic files, and the relationships between the files.
3.2.	Retention and Disposition	Define how long the records have to be kept by the system, and how they may be disposed of.
4.	Task Management	The service that treats unfinished processes as tasks assigned to personnel.
4.1.	Track task status changes and notification of task status changes	System will record any status change of a task, which will help superiors track its progress. At any status change the superiors can be notified.
5.	User and group management	Security services that define authorised personnel, their credentials and their levels of access.
6.	E-mail	Helps users manage large volumes of customer emails, Web forms and sending documents (in the form of messages and as attachments), within and between organisations, responsively and effectively.
7.	Instant messaging	Sharing knowledge information, team working and collaborative environments amongst employees.
8.	Voice service	Allows users to make telephone calls over the Internet. Calls to other users of the service and to free-of-charge numbers are free. Additional can be used for video conferencing.
9.	Remote connection	Allows users to temporarily control a remote computer over a network or the Internet – use IIS outside of MFAEI to resolve issues.
10.	System of Management of installed software licenses	Deliver software license management functionality that supports identifying installed software products, Matching installed software products to existing software licenses and Reporting compliance status.

6.4. Service scenarios

This section lists a series of service scenarios specific to MFAEI operation. Many other scenarios must be supported by IIS as part of the basic functionality offered by its individual components.

This section identifies and lists examples of the range of scenarios to be covered by IIS. The scenarios described are provided for informative purposes and are not mandatory for automation within the IIS as long as the requirements in section 8 are fulfilled.

6.4.1. INTRANET

The most important aspect of the Intranet service is that it offers a single point of entry to other IIS components. The Intranet offers a Web based User Interface that is accessible to ALL MFAEI personnel.

The Intranet is available in MFAEI WAN to authorised personnel. The information available is only for Internal Use and Confidential levels of security. Usually these are templates, internal documents or draft version of documents that eventually become publicly available.

Besides the Web based UI the Intranet offers a File based access path that allows personnel to handle their outputs as usually - by creating and storing files on a File server.

Workload Dashboard

Each employee uses a personalized workload dashboard that allows tracking of current and urgent tasks, drafts, notifications, emails etc.:

- **MFAEI user logins to Intranet**
- **IIS identifies his personal and workgroup tasks. IIS highlights urgent, overdue tasks.**

- IIS presents shortcuts to all the workspaces the user has access to
- IIS registers user presence
- IIS gives access to user accessible functionality and facilitates user requests.

Workspace creation

A new workspace is needed to accommodate a change within MFAEI organizational structure or to assign to an ad hoc workgroup such as diplomatic mission, delegation, conference participation, subdivision creation etc. At this stage:

- MFAEI Top Management issues/approves an order regarding the change and specifies the personnel involved,
- System Administrator creates a workgroup and workspace on the Intranet and assigns the workgroup to it,
- System Administrator assigns workflows and records templates to the new workgroup,
- If appropriate, System Administrator assigns Administrative Roles to workgroup leaders.

Remote access

The Intranet ensures access to remote personnel - both "on the go" authorised employees as well as employees of diplomatic missions. Remote access features make transparent the concerns regarding with connectivity and transport of data so that everybody accesses the Intranet in the same manner given that they are authorised and have properly configured their workstations.

6.4.2. DOCUMENT AND RECORD MANAGEMENT

An integral part of IIS is the functionality related to information creation, grouping, presentation and classification. These features represent functionality for:

a. Document Management system - allowing creation and distribution of documents,
b. Records Management system - handles records differently due to their constant nature.

Both, Document and Records management systems must:

- ensure user friendliness to authorised users via clear and easy to identify system functions,
- impose restrictions for un-authorised or limited access users via mandated security policies,
- keep audit logs of user and system actions for administrative purposes.

By way of clarification, the following table shows typical differences between an EDMS and an ERMS.

Document Management	Records Management
allows documents to be modified;	prevents records from being modified;
allows documents to exist in several versions;	allows a single final version of a record to exist;
may allow documents to be deleted by their owners;	prevents records from being deleted except in certain strictly controlled circumstances;
may include some retention controls;	must include rigorous retention controls;
may include a document storage structure, which may be under the control of users;	must include a rigorous record arrangement structure (the classification scheme) which is maintained by an administrative role;
is intended primarily to support day-to-day use of documents for ongoing business.	may support day-to-day working, but is primarily intended to provide a secure repository for business records.

Electronic Document Management

Electronic Document Management Systems – EDMSs – are widely used in organisations to provide management and control over electronic documents. EDMSs typically include:

- workflows that advance a document from a stage to another till it is done,
- indexing of documents that facilitate search and information retrieval,
- storage management that ensure proper preservation of document parts,
- version control that preserves the changes a draft document went through,

- close integration with desktop applications that produce actual artefacts and
- retrieval tools to access the documents and present them.

EDMSs often form part of a wider system implementation and contain collaborative working tools to enable a number of users to participate in document drafting.

Electronic Records Management

Once documents become official, say when these are received externally or a particular version of a document is approved and a decision to distribute/act upon is made, the document can no longer be changed and it must be preserved for reference. This type of document becomes a record and handling, manipulation and preservation must follow rigorous procedures. These more stringent and rigorous procedures are undertaken by an Electronic Records Management System - ERMS. ERMS typically include:

- capture of objects, documents, information as records, i.e. declaration of a version of an object as final so that it enters the records "realm". During capture an entire package of objects is grouped - an aggregation - into the record entity and it might include, actual content of one or more documents, their metadata, digital signatures, notes and decisions possibly digitally signed as well and much more.
- rigid classification scheme to categorize records by their nature and implications.
- assignment of identifiers to records for future reference.
- record retention control that ensures record preservation in conformance with legal and business practice.
- record archival or disposition that ensures correct archival or destruction of records once they are no longer in current use.
- record redaction that allows distribution of some parts of a record while hiding other, more sensitive parts. Redactions are done by administrative roles and are themselves preserved as records.

6.4.3. WORKFLOW MANAGEMENT

The IIS integrates a Workflow Management component that allows records and documents to pass all the required stages of development and approval before becoming resolved. It is needed to assist in handling vast numbers of documents. The component includes functionalities such as searching, editing, sharing, and distributing documents, with a familiar, easy to understand user interface.

Initially only a few of the workflows will be rigidly applied in the IIS - workflows for processes that the MFAEI must comply with legal requirements such as hiring, transferring, petition resolution etc. Otherwise, the IIS will rely on generic, personnel driven workflow as presented below.

The workflow depicted in Figure 1 - Generic Document Workflow presents how a generic document enters the MFAEI Integrated Information System, what additional records it generates and what activities are performed in order to prepare an output. The generic workflow can be summarised as:

- for urgency reasons documents are received as a copy of the original (by Fax and with increased frequency by email)
- Secretariat registers the document and assesses its further processing steps
- Top Management reviews and approves further processing
- Secretariat forwards documents to the main contributor
- if needed, Secretariat forwards document to other workgroups for contribution
- Workgroup management reviews and assigns for resolution
- Workgroup personnel prepares response and integrates external contributions when available
- Workgroup management reviews resolution and forwards to Secretariat
- Secretariat registers resolution and approves with Top Management when necessary
- Secretariat distributes copy of resolution (via Fax or Email) and forwards original resolution via diplomatic channels
- Later when the original is received, Secretariat identifies the records captured previously received as a "copy" and replaces them with original. The replacement should be undertaken carefully so that any of the written resolutions are not lost.

- **Another serious issue is caused by the impossibility to identify the previously emitted resolution and this causes another round of processing of the document with potentially different results.**

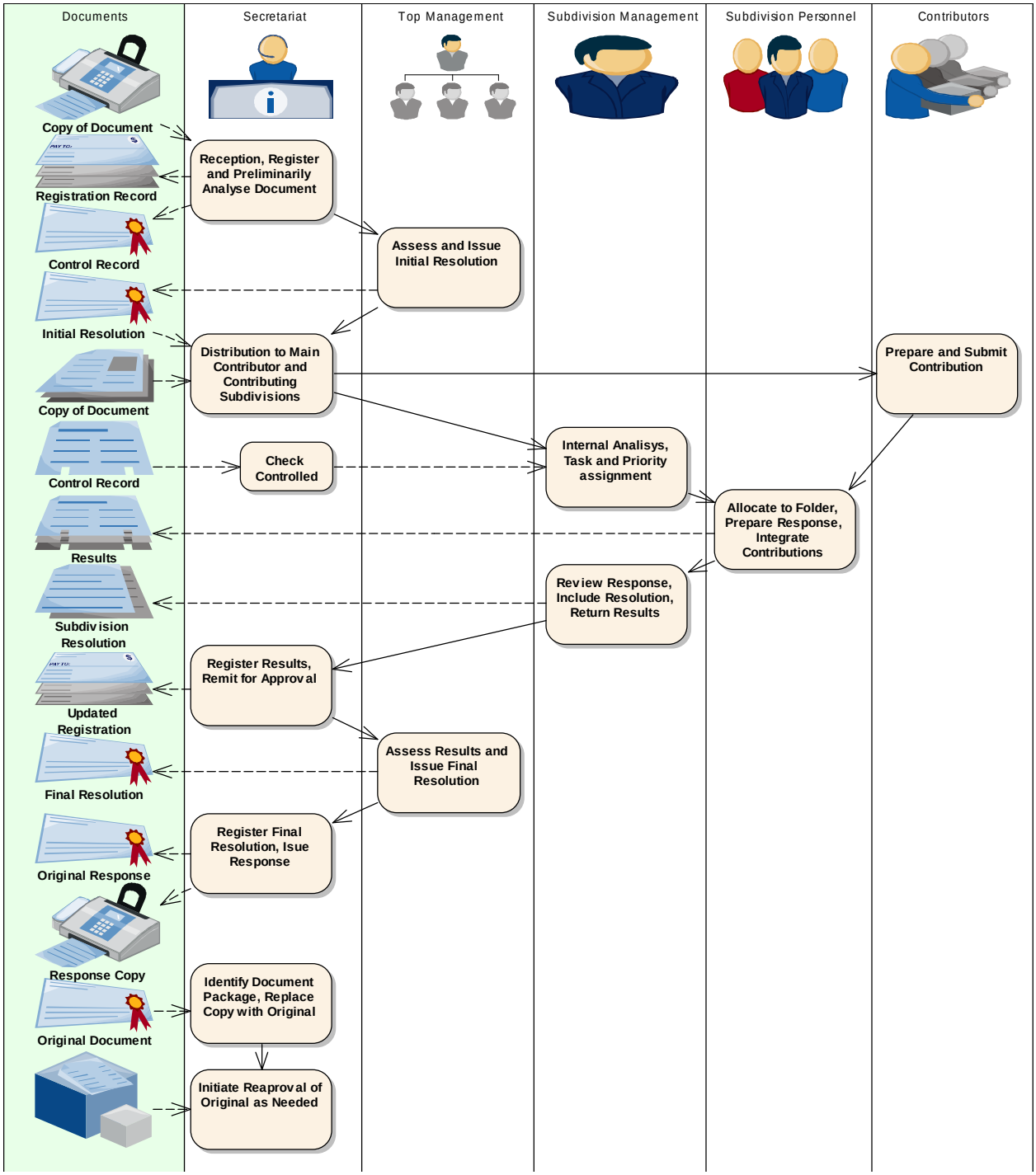

Figure 1 - Generic Document Workflow

As can be seen, most of the processes are personnel driven still, there are multiple types of documents that are handled by the MFAEI and for many of them the workflow process is regulated. One of the goals of the Integrated Information System is to attempt to reduce the number of documents received as "Copy" and only later in "Original". This goal is achievable by reliance on Digital Signature of Electronic Documents having the same legal weight as the paper signatures.

The system is not able to completely eliminate this drawback because the majority of documents are received from external bodies and reliance on a Digital Signature Infrastructure for production cannot be achieved.

Hiring Process

When a new person is hired a series of work procedures must be followed:

- **HR department receives an hiring request for an open position, registers it and starts the selection process**
- **HR collects personal profiles of people interested in the advertised position**
- **HR arranges interview and assessment sessions with the interviewee and the interview panel**
- **Interview Panel members are notified of the interview and accept or refuse participation**
- **Participating Panel Members provide their feedback about the interviewee**
- **HR identifies the best interviewees and shortlists them for approval**
- **Subdivision managers, panel members express opinion about the shortlisted candidates**
- **HR checks candidate background for acceptability for the position**
- **HR presents the shortlisted candidates for approval to Top management**
- **Top management examines interview results, opinions, background check results and issues hiring order**
- **HR notifies accepted candidates about decision**
- **Candidates accepts offer and signs employment contract**
- **HR registers new employee details, completes hiring process.**

The registration of a new employee starts a series of other internal processes:

- **for example, System Administrators, Accounting, Logistics department manager are notified of new employee**
- **system administrators issue user credentials, create user accounts, assign user rights and workgroup membership;**
- **accounting starts salary calculation, benefits procedures;**
- **logistics identifies and allocates physical workspace, desk, computer etc.**

Personnel reassignment

Many MFAEI personnel is mobile and frequently re-assigned to temporary roles and positions such as delegations, foreign missions, panels, exchange and training programmes. Reassignment must follow a series of strict rules and interested parties should be kept aware of the change. The detailed process can be summarized as:

- **HR receives a request to identify internally personnel to temporarily fill a position**
- **HR reviews personal records for matching candidates and checks whether their current or previous assignments do not conflict with the requirement**
- **HR shortlists the most adequate candidates and notifies them, their superiors and Top management with the context of the need**
- **Candidates, their superiors offer opinions about the offering**
- **HR presents the best candidates to Top management for approval**
- **Top management issues decision about reassignment**
- **HR registers decision and notifies candidate and their superiors.**

This generates a series of reassignment processes in other subdivisions:

- **System Administrator creates workspaces for the new workgroup, assigns users, rights and administrative roles to workspace, upgrades credentials package where necessary (issues digital certificates, passwords for VPN access etc)**
- **Accounting reassigns personnel to the new subdivision, potentially changing salary, benefits and expenses**
- **Logistics allocates resources required for remote personnel (e.g. notebooks instead of desktops)**
- **HR starts travel documents preparation processes when necessary.**

6.4.4. TASK MANAGEMENT

A task is an activity that needs to be accomplished within a defined period of time. An assignment is a task under the responsibility of an assignee which should have a start and end date defined. One or more assignments on a task put the task under execution. A task is judged to be completed when all the assignments for the task have been completed. Tasks can be linked together to create dependencies.

When completed, an item on a task list is *checked* or *crossed* off. The traditional method is to write these on a piece of paper with a pen or pencil, usually on a note pad or clip-board.

The Task Management System should allow:

1. **Adding notes by anyone assigned to a task with control over who sees it.**
2. **Grouping of tasks by type to provide more informative reporting. There is no restriction to the task types available as the system administrator sets them dynamically.**
3. **Prioritization of tasks. This will support the escalation of an issue and improve the task management process. Task assignees will be notified when a task has been escalated.**
4. **The update of the task status by the user who is currently assigned to it. This status is displayed keeping them informed throughout the task management cycle.**
5. **The automatic generation of tasks at regular intervals.**
6. **Users to schedule events related to a task. The system should provide a weekly snapshot of meetings related to specific tasks in the system. Reminders via e-mail of pending events and the scheduled time should be sent.**
7. **The attachment of links to documents associated to the task.**

The Task Management System works in two different ways:

- **Independently where superiors, MFAEI personnel or external staff manually create new tasks/calls for MFAEI to solve and assigns them to groups or individuals.**
- **Integrated with Document Management system - when a document reaches a specific state, tasks are automatically created and assigned to responsible group or personnel to handle the situation.**

6.4.5. MFAEI WEB SITE INTEGRATION

MFAEI operates a web portal that is accessed via Moldova's eGovernment Portal. The MFAEI portal is administered internally by its various subdivisions. Once materials are published, these integrate into the eGovernment Portal automatically, without need of further human intervention.

Also, the contents on the portal will be published directly from within Intranet without any other publishing tool support.

It must be mentioned that many diplomatic missions still have web pages of their own. While these are less complex the IIS will offer content creation, update and publication facilities for each of the Web Page administrators. The web pages will all have a similar structure and template so that all diplomatic mission web pages have a consistent look and feel. As an additional feature will be the possibility to administer diplomatic mission web pages from a single location - MFAEI central offices. While the actual content might be generated remotely within the mission, web page administrators will get access to publishable material and publish it without the need to be remote.

Communicate with the public

MFAEI is a public administration body, which reports its activities to the public and the media through the governmental portal of ministry. To achieve this aim the ministry includes a Mass Media Directorate that will accomplish following actions:

- **monitor news and media coverage to meet the needs of the Ministry;**
- **maintain, develop and coordinate external and internal web communications of the Ministry;**
- **guide and train staff to meet the Ministry's needs and related support;**
- **communicate matters concerning development policy and development cooperation to the citizens, the media and other stakeholders;**
- **provide education information and materials to educational institutions and society at large;**

- customer service and information service related to development policy and development cooperation;
- technical development and maintenance of online and mobile services and their coordination with other information systems;
- audio-visual services and their development and graphic design.

The workflows for the processes above will be defined incrementally to provide details to Mass Media Directorate personnel about newly published information so that they are current with all the developments and progress in MFAEI. Increasingly these workflows will include automatic publishing mechanisms directly in the workflow and to reduce the workload on dedicated personnel.

6.4.6. TELEPHONY, FAX AND VOICE SERVICES INTEGRATION

Voice services have the potential to significantly reduce costs of exchanges via telephone networks. While conversation over the phone in the central building are free of charge and convenient, exchanges via ordinary telephony services with remote and "on the go" personnel incurs significant costs.

This concept envisions reliance on a "transparent" internal telephony service to connect ALL its personnel. The service relies on a server that transfers automatically calls to and from remote users via VoIP. Callers do not need to check in advance the location of the phoned party, they use the service as currently by using an internal directory and dialling the number. The system will identify the location of the called party, the best current route and channel and will transparently establish the connection that users will use un-aware of the underlying technology in use. The same is applicable for Fax interchanges only that data will be routed to dedicated recipients.

Redirect Calls

MFAEI personnel are assigned personal phone numbers. These are used by the integrated voice system to call someone wherever he is given that the presence service was able to locate the user:

- an employee calls a receiver.
- the integrated voice system identifies the last location of the receiver, the best calling mode and route to him and establishes a connection with the receiver.
- in case the receiver is available only via Instant Messaging, the IIS notifies receiver of the details of the Caller by sending and Instant Message.
- in case the receiver is not available at all, a voice mail is taken and sent as an attachment to receiver's inbox via email.
- faxes are captured as records and routed as attachments to email directly to user or workgroup inboxes or workspaces.

6.4.7. MANAGEMENT OF INSTALLED SOFTWARE LICENSES

The reasons that follow cause the need for a distinct System of Management of software licenses as it is not fully supported by other IIS components. It also generates a separate Information Space item.

Management of software licenses is based on concurrent and interdependent technical and organisational/process measures. The technical tools will rely on an inventory system, a discovery system, and a mechanism for automatic comparison and alerting both administrators and end-users. The process measures will include instructions, user guides, process and policy definitions, as well as on-going effort to educate end users and to maintain the orderly status in the licensing part of work.

Management of software licenses usage and compliance is done via an integrated series of networked services that automatically gather information about software installed on personnel workstations and MFAEI servers. The accuracy of this information is pre-conditioned by using a monitoring and managing system running on both workstations and as a central records database.

7. SYSTEM FUNCTIONAL REQUIREMENTS

7.1. Intranet

7.1.1. USER INTERFACE TO IIS/DASHBOARD

The main User Interface to IIS is via Internal Web Sites/Applications maintained as a single Intranet. The Intranet include means to manage the internal web sites and configure their parts for work with different constructs that allow integration of the other modules such as document management, records-keeping, task management, workflows, document templates etc.

Ref	Requirement
REQ7.1.1.1.	The system must provide facilities to create new workspaces within existing workspaces. These facilities are offered to administrative roles of the existing workspace.
REQ7.1.1.2.	The system must provide referencing/linking capabilities between workspaces.
REQ7.1.1.3.	The system must provide facilities for administrative roles to configure workspace dashboard content.
REQ7.1.1.4.	The system must provide a choice of templates for workspaces.
REQ7.1.1.5.	The system includes templates for workspace elements such as: - lists, - information pages, - document and record types, - predefined workflows, - tasks and events, - calendars/agendas.

7.1.2. DISTRIBUTED AND REMOTE ACCESS

Distributed System

The MFAEI is a distributed organization. In order to satisfy its needs it is expected that the IIS offers sufficient means and controls to address the distributed nature of the organization. The solution will rely on a single instance of the system controlling a single repository.

Ref	Requirement
REQ7.1.2.1.	The system must be capable of being configured by an administrative role for use across multiple locations.
REQ7.1.2.2.	The system must prevent or resolve any conflicts caused by changes made in different locations.

Offline and Remote Working

The requirements in this section cover all types of mobile and offline usage by users who are not permanently connected to the system (or to the network hosting it). Users need to be able to download and synchronise records and data so that they can work on them whilst offline.

There are several possible scenarios including:

- **users who access the system using portable computers (such as mobile, laptop, or notebook computers) or PCs that are connected to the system intermittently;**
- **users who connect to the system remotely through a dial up connection, or any other connection with low bandwidth connection (e.g. for telecommuting or in a temporary location).**

Ref	Requirement
REQ7.1.2.3.	The system should allow an administrative role to specify aggregations containing information that cannot be downloaded by any user.
REQ7.1.2.4.	The system must enable a user to download any aggregation or record(s) with accompanying metadata for the user to work on whilst not attached to the network.
REQ7.1.2.5.	The system must allow users the option of checking documents out when they are downloaded.
REQ7.1.2.6.	If a user checks out a document and works on it while not connected, the system must allow version numbering to be applied to the document.

7.1.3. FILE BASED UI

The IIS includes facilities to offer access to Documents and Records management systems via computer/network file system means using existing operating system or third party tools on user workstations.

Ref	Requirement
REQ7.1.3.1.	The system must provide facilities to navigate and work with documents and records by means of WebDAV or similar open protocols, integrating with the files/directory system of user workstations

7.2. Document and Record Management

7.2.1. DOCUMENT MANAGEMENT

The rest of this section sets out key requirements to be considered in the provision of an integrated ERMS/EDMS solution with a single interface to it - the Intranet.

A central feature of these requirements is the concept that documents can be stored in (that is, classified to) the same classes and files as records, though this is optional. This allows draft documents to be filed in the same aggregations as the final versions, which will be records.

Note that the word 'document' is used here specifically to describe information or an object that has not been declared as a record.

Ref	Requirement
REQ7.2.1.1.	The system should be able to manage electronic documents and records in the context of the same classification scheme, using the same access control mechanisms.
REQ7.2.1.2.	It must clearly indicate which items are documents and which are records.
REQ7.2.1.3.	The EDMS must be able to pass automatically electronic documents arising in the course of business to the ERMS for automatic capture as records.
REQ7.2.1.4.	The system must be able to copy the contents of an electronic record, in order to create a new and separate electronic document without automatically creating a new record, while ensuring retention of the intact original record.
REQ7.2.1.5.	The system must allow user roles to check out and check in any document to which they have appropriate access rights.
REQ7.2.1.6.	When a document is checked out by a user, the system must prevent any other user from checking it out or changing it.
REQ7.2.1.7.	Users should be able to capture a document from within the system.
REQ7.2.1.8.	The system must be capable of version control, which is, managing different versions of an electronic document as a single entity.

Ref	Requirement
REQ7.2.1.9.	The system must maintain a version number for each document, and must make it clearly visible when the document is retrieved or searched for.
REQ7.2.1.10.	The system should allow users to have a "personal" workspace for documents.

7.2.2. SEARCHING, RETRIEVAL AND PRESENTATION

An integral feature of an integrated system is the ability for the user to locate files and retrieve documents and records, including their parts - text, signatures, images, media content etc. This includes searching for them, whether or not precise details are known, and presenting them. Presentation is producing a representation on-screen ("displaying") or printing; it may also involve, as necessary, playing audio and/or video.

Search and Retrieval

The search and navigation tools are used to locate metadata, classes, files, sub-files, volumes or records. These require a variety of searching techniques to support users ranging from (for example) the sophisticated "research" user to the "casual" and less "computer literate". This causes the need for:

- **advanced search capabilities where users specify multiple search criteria,**
- **simple search where users specify one or more search words to locate.**

Ref	Requirement
REQ7.2.2.1.	No search or retrieval function must ever reveal to a user any information where the access and security controls prevent access by that user.
REQ7.2.2.2.	The system must allow users to search for the text content of records.
REQ7.2.2.3.	The system must allow users to search for objects by their keyword(s), where the objects have keywords.
REQ7.2.2.4.	The search system must rely on an full text indexing mechanism that is able to return search results by relevance.
REQ7.2.2.5.	The system should allow users to save and re-use search terms.

Presentation: Displaying Records

The system contains records with different formats. The user requires generic presentation facilities that will accommodate the display of a range of formats.

Ref	Requirement
REQ7.2.2.6.	Whenever a user reaches a view that indicates the existence of a class, file, sub-file, volume, record, document or parts the system must be able to present its contents.

Presentation: Printing

The system must provide printing facilities, to allow all users to obtain printed copies of printable records, their metadata, and of other administrative information. Printing does not apply to audio or video files.

Ref	Requirement
REQ7.2.2.7.	The system must be able to print the content of records and specified elements of their metadata.

7.2.3. CAPTURING AND DECLARING RECORDS

The term "capture" is used with its natural language sense, in an information management/information technology context. Here, "capturing" information means saving it in a computer system. This is consistent with the archival meaning of "capture", ("the act of recording or saving a particular instantiation of a digital object") given in the InterPARES 2 Project Terminology Database.

The fact that it's possible to capture documents as well as records suggests that the term "capture" is imprecise, because capturing a record involves more processes than capturing a document that is not a record. For example, capturing a record includes the processes of classification, registration, and locking against change whereas this is not necessarily the case for documents. Hence the term "declare" is sometimes used synonymously with "capture" in the case of records.

Input and Output Mechanisms

The IIS should be capable to accept, intercept, register, import documents, records, information objects, data from various sources such as Fax, Email, computer files, manual data entry etc. Figure 2 depicts the various sources of input data into the system.

Once the results are ready the system should be able to output them in different ways depending on the destination. Again the list includes Fax, Email, computer files. It also should be capable to print on paper, to send forth digitally signed documents as well as store and register internal records for further processing in an internal loop.

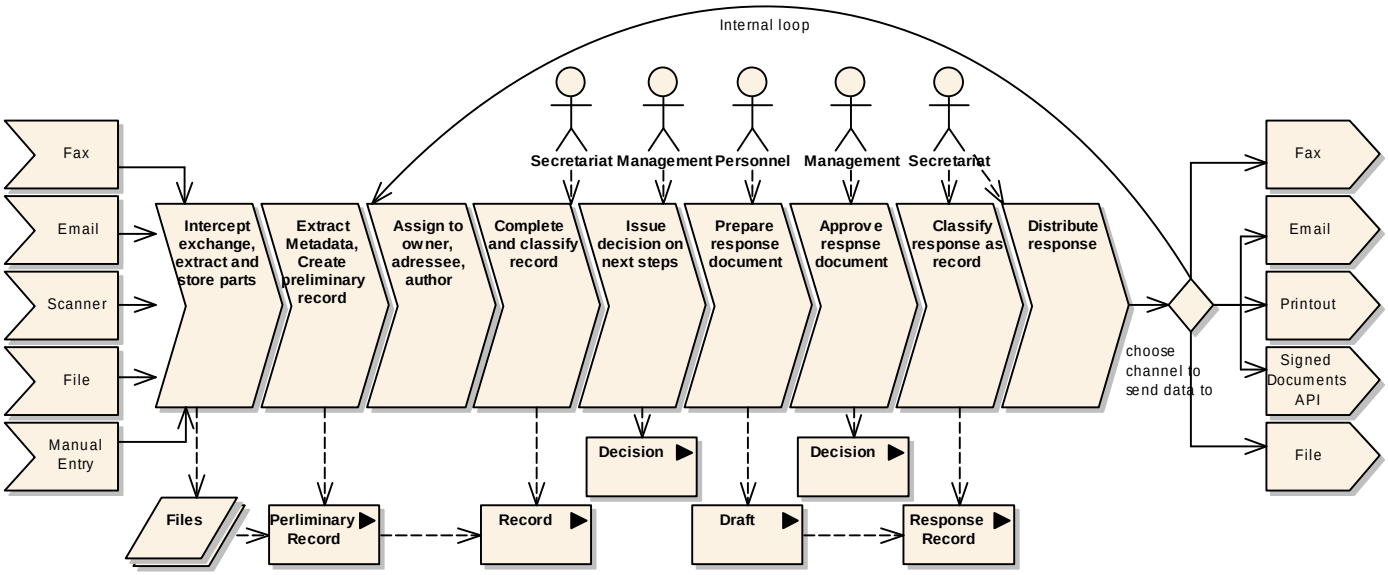

Figure 2 Input and Output mechanisms

Capture

Electronic documents that are made or received in the course of business processes originate from both internal and external sources. The electronic documents will be in various formats, be produced by different authors and may be received either as single documents or as documents comprising several components.

Some records are created within the organisation, in the course of its business processes. Others are received through various communication channels, for instance electronic mail, facsimile, letter post (optionally to be scanned), by hand, and at variable arrival rates and volumes. A flexible capture system with good management controls is required to capture documents so that their diverse requirements are addressed.

Ref	Requirement
REQ7.2.3.1.	The capture process must provide the controls and functionality to allow users to: • capture electronic records regardless of file format, method of encoding or other technological characteristics, with no alteration of their content; • ensure that the records are associated with a classification scheme; • ensure that the records are associated with one or more file(s) or class(es).
REQ7.2.3.2.	When capturing a record made up of several components, the system must capture all of its components.
REQ7.2.3.3.	When capturing an electronic record that has more than one component, the system must allow the record to be managed as a single unit, retaining the relationship between the components, and retaining the record's structural integrity.
REQ7.2.3.4.	The system should allow users who wish to capture a record but who are unable to provide all the mandatory metadata values for it to store it temporarily.
REQ7.2.3.5.	The system should allow the process of capturing a record to be completed by more than one user.
REQ7.2.3.6.	The system should issue a warning if a user attempts to capture a record that has the same content as another record which has already been registered.

Bulk Import

Records may reach the system in bulk in a number of ways. For example:

- a bulk transfer from a compatible EDMS;
- a bulk transfer from a compatible ERMS;
- as a single compatible data file containing a series of records of the same type;
- from a compatible scanning or imaging system;
- records from a hierarchy of operating system folders.

The system needs to be able to accept these, and must include features to manage the capture process and maintain the content and structure of the imported records.

e-Mail Management

The standard protocol used for e-mailing is defined by the Network Working Group documents RFC 2821 and RFC 2822.

e-Mail is used for sending documents (in the form of messages and as attachments) within and between organisations. The characteristics of e-mail management software combined with user attitudes towards e-mail, makes it difficult to apply records management functionality to e-mail. The system needs to provide users with the capability of capturing selected e-mails and attachments.

e-Mail exchange may be the basis of MFAEI processes, e.g. daily reports, or the distribution of list of works to be completed.

Ref	Requirement
REQ7.2.3.7.	Whenever an e-mail is captured, the system must capture it in a format that retains its header information.
REQ7.2.3.8.	The system must support the capture of e-mails in an integrated way, such that the user relies on a single view/application to both work with email and capture records.
REQ7.2.3.9.	The system must support automated assistance in the capture of outgoing and incoming e-mails, with and without attachments, as records, by automatically extracting the following metadata from them to the extent that these are present: • date e-mail was sent (and in some settings, time); • recipient(s); • any copy recipient(s); • subject line (title); • sender; • embedded electronic signature; • certification service provider.

Scanning and Imaging

Physical records in the form of paper need to be considered. There are two main issues:

- existing records that are held on paper and need to be referred to in conjunction with electronic records;
- documents on paper that continue to be received or created by the organisation, but which the organisation wishes to hold as electronic records.

Centralised scanning is most appropriate for the MFAEI.

Ref	Requirement
REQ7.2.3.10.	The system must be capable of integration with at least one scanning solution.
REQ7.2.3.11.	The system must be capable of integration with at least one Optical Character Recognition solution.
REQ7.2.3.12.	The system scanning feature must be capable of saving images in standard formats, including, but not limited to: • TIFF (see TIFF 6.0 Specification); • JPEG (see ISO 15444, required only if colour is supported); • PDF/A (see ISO 19005).

Fax Integration

While e-mail has taken over from facsimile as the preferred method of rapid communication, fax is still in wide use. This can be, for example, where the original document is not in electronic format and a copy needs to be sent to another organisation, or where a visible representation of, e.g., a signature is required.

Ref	Requirement
REQ7.2.3.13.	The system should provide an application programming interface (API) to enable it to interface with a fax server.
REQ7.2.3.14.	The system must be capable of storing faxes in standard formats, for example TIFF v6 image format with Group IV compression.

7.2.4. CLASSIFICATION SCHEME AND FILE ORGANISATION

The classification[2] scheme is the foundation of the records preservation requirements. It allows an electronic record to be stored together with other records that provide its context, by defining the way in which the electronic records will be organised into electronic files, and the relationships between the files.

While structuring the classification scheme the following aspects should be taken into consideration:

- **Classification Scheme elements and hierarchy**
- **Types of objects**
- **Business document types.**

Classification Scheme elements and hierarchy

In a system that keeps paper records, subdivision of large files is essential for reasons of ergonomics and the physical survival of folders, binders, jackets etc. Similarly there are benefits in splitting large electronic files into volumes, for example, when users need to work remotely or when files are worked on for long periods of time and are never closed.

This allows a record to be captured into any of the following:

- **Class;**
- **File;**
- **Sub-File;**
- **Volume.**

In summary:

- **Each file may contain one or many sub-files;**
- **Each sub-file may contain one or many volumes;**
- **Volumes of different sub-files are created independently;**
- **All the sub-files of an open file can be open or closed by users as required;**
- **Only one volume can be open in each sub-file.**
- **Records will most commonly be captured into volumes.**

Object types

By content the objects can be classified as:

- **Records of documents,**
- **Resolutions, Notes, Confirmations regarding document responses or tasks,**
- **Signatures for digitally signed documents, resolutions, records etc.,**
- **Scanned images of documents,**
- **Paper variants of documents and records about their location,**
- **Text of documents,**
- **Document Lists relating to a particular domain of activity (subdivision, mission etc),**
- **Access groups having access to a document list,**
- **User Lists and their rights,**
- **Publically available documents and information.**

Business document types

It is essential that the classification scheme (technically, a records classification scheme) is closely aligned with the business needs of the organisation.

---

[2] It must be stressed that the terms file, record, class, volume have specific meaning in this document and the glossary should be consulted for better understanding of the material. Classes, files, sub-files, volumes can be understood as Folders but have exact meanings that differentiate them.

Currently the MFAEI relies on the Classification of Records for diplomatic services of the Republic of Moldova approved by Minister Order no. 226/b/39 of 19 March 2007 that regulates more than 500 types of documents. Many of the categorized items in this list are rarely used and will be added by administrative roles once there is a real need to support a particular type of document. The following table lists the Classes, Subclasses defined by the Classification and provides example documents registered under the specified class/subclass.

Code	Class / subclass	Example documents
0	ORGANIZATIONAL, PERSONNEL, TRAINING, ARCHIVAL, LIBRARY AND OTHER GENERAL PROBLEMS	
01	Organizational problems of MFAEI activity	Laws, Presidential Decrees, Government Decisions and Orders, Addresses, Declarations, Memorandums, Work Instructions, Circulars, Programmes, Activity reports etc.
02	Requesting and transferring correspondence with Republic of Moldova and foreign organizations	Correspondence, Incoming/Outgoing document registries, Lists regarding document execution control, Petition registries, etc.
03	Organizational, personnel and training	Normative acts relating to personnel, Minister/Ambassador/Consular orders regarding personnel movement, Personal profiles, Diplomatic personnel records etc.
04	Legal matters	Draft laws, decrees, decisions, Assessments of draft statutory acts, Contracts, Correspondence etc.
05	Librariral and Archival matters	Classifications, Inventory of folders, Minutes about acceptance-transfer to archive, requests about issuance of copies of archived documents, correspondence etc.
06	Deputy Prime-Minister, Minister of Foreign Affairs and European Integration documents	Documents printed on Government templates with Minister signature
1	PROTOCOL, CEREMONIAL, REPRESENTATIONAL AND PRIVILLEDGES MATTERS	
10	Protocol, Ceremonial, Representational and Priviledges matters	Statutory acts regarding protocol and ceremonial, Minister and Deputy Minister agendas, Letters of accreditation-recall, Invitations, Speeches etc.
2	POLITICAL, ECONOMIC, SOCIAL, PRESS, CULTURAL, MILITARY MATTERS	
	BILATERAL RELATIONS	
20	General matters	Strategies, Concepts, Statutory acts, Projects, Synthesises, Evaluations, Forecasts, Informative bulletins regarding bilateral relations
21	Press matters	Press releases, Declarations, Synthesises, Articles etc.
22	Bilateral relations	Motivations, Country fiches, Informational, analytical notes, Informations, Articles etc.
23	Economic matters	Statutory acts, Work instructions, Circulars, Economic reports, Analyses, Correspondence etc.
24	Cultural and Educational matters	Programmes, Notes, Suggestions etc.
29	Bilateral Treaties	Treaties, Conclusion of treaties, Full powers, Ratifications,

		International conventions,
3	INTERNATIONAL, SUBREGIONAL ORGANIZATIONS.	
	MULTILATERAL RELATIONS.	
33	UN and specialized agencies	Reports, Analyses, Synthesises, Programmes, Speeches, Articles, Notes, Informations etc.
34	International organizations	idem
35	European organizations	idem
36	International organizations with military and security orientation. Transdnester Conflict.	idem
37	Subregional organizations	idem
39	Negotiations and Multilateral treaties. Treaties with international organizations.	Treaties, Conclusion of treaties, Accessions, Letters, Full powers, Assessments, Informations etc.
4	CONSULAR MATTERS. CONSULAR LAW.	Consular statutory acts, Circulars, Assessments, Verbal notes, Informational notes, Consular correspondence etc.
5	FINANCE, ACCOUNTING, PROCUREMENT, TECHNICAL AND LOGISTICS	
50	Finance. Accounting.	Bookkeeping notes, Contracts, Statement of accounts, Registers, General Ledger, Cash registers, Inventory lists, Statistical reports etc.
55	Procurement, Technical and Logistics	Acceptance, transfer, ascertainment and destruction documents, Stamp and seal issuance records, Correspondence etc.
6	UNIONS	Meeting Minutes, Expenditure reports, Correspondence etc.
9	OTHER	

Table 1 Classes/subclasses of documents and examples

Configuring the Classification Scheme

Ref	Requirement
REQ7.2.4.1.	The system must support and be compatible with the organisation's business classification scheme.
REQ7.2.4.2.	The system must support extension of the classification scheme by administrative roles.
REQ7.2.4.3.	The system should support the definition and simultaneous use of multiple classification schemes.
REQ7.2.4.4.	The system should allow management of individual classes by specified user roles and/or by a specified group of users.

Referencing

All of the entities stored in the system repositories (classes, files, sub-files, volumes, records etc.) need identifiers. These identifiers are needed to:

- **Allow the software to process the entities;**
- **Allow users to retrieve, refer to, and use, the entities.**

Each class has a Classification Code that can be combined with the Classification Codes of its parent classes to make a "Fully-Qualified Classification Code". Records and components are also allocated classification codes, to allow them to be referenced uniquely.

Ref	Requirement
REQ7.2.4.5.	Whenever a new occurrence of any of the following is created in or captured by the system, the system must associate with it a Classification Code: • class; • file; • sub-file; • volume; • record; • component.
REQ7.2.4.6.	Whenever a new occurrence of any of the following is created, the system must associate with it a System Identifier: • classification scheme; • class; • file; • sub-file; • volume; • record; • redaction; • retention and disposition schedule; • document.

7.2.5. RETENTION AND DISPOSITION

Retention and disposition schedules define how long the records have to be kept by the system, and how they may be disposed of. The processes that can take place at the date specified by retention and disposition schedules are

- **review processes listed in section 0, and**
- **transfer, export and destruction listed in section 0.**

According to circumstances, retention and disposition schedules apply to classes, files and/or sub-files and/or volumes. Retention and disposition schedules can also be applied to record types, for example to apply short retention periods to sensitive personal data.

Disposal holds are used in response to unexpected events to ensure that specified records are not destroyed. The common example is to ensure that records that are, or that may be, required as evidence in legal proceedings are not routinely destroyed as a result of a disposition decision.

Retention and Disposition Schedules

Ref	Requirement
REQ7.2.5.1.	The system must allow administrative roles, and only administrative roles, to create and maintain retention and disposition schedules.
REQ7.2.5.2.	The system should be able to apply a default retention and disposition schedule to record types.
REQ7.2.5.3.	Each retention and disposition schedule must include either: • a retention period and a trigger event; or • a disposition date.
REQ7.2.5.4.	Each retention and disposition schedule must include: • a disposition action; • a reason.
REQ7.2.5.5.	Each retention and disposition schedule should include a: • a description; • a mandate. *The mandate specifies the justification for the retention and disposition schedule. This is often a reference to a law, regulation or corporate policy.*
REQ7.2.5.6.	When the retention period applicable to some record(s) because of a retention and disposition schedule reaches its end, the system must automatically initiate the processing of the disposition decision.
REQ7.2.5.7.	The system should not limit the length of retention periods.
REQ7.2.5.8.	The system must enable a disposal hold to be placed on a class, file, sub-file, or volume by an authorised user.

Review of Disposition Actions

Retention and disposition schedules are used to govern disposition without a review.

Retention and disposition schedules trigger a review of the specified disposition action on an aggregation that has reached the date or event specified in the schedule. The review may consider metadata, contents or both in deciding on the disposition action (a further retention period, transfer to another system, destruction or combination of these).

The disposition of certain records is subject to laws and regulations.

Ref	Requirement
REQ7.2.5.9.	The system must support the review process by presenting classes, files, sub-files and volumes to be reviewed, together with their metadata and retention and disposition schedule information.
REQ7.2.5.10.	The system must allow the reviewer to take at least any of the following actions for each class, file, sub-file or volume during review: • mark for destruction, immediately or at a future date; • mark for transfer, immediately or at a future date; • mark for a further review, immediately or at a future date; • mark for indefinite retention.

Transfer, Export and Destruction

MFAEI needs to be able to move records from the system to other locations or systems for archival or other purposes. This is referred to here as "transfer".

Reasons for transfer may include:

- **permanent preservation of the records for legal, administrative or research reasons;**
- **the use of devolved or external services for the medium term or long term management of the records.**

This action often results in the records being transferred to a different environment.

The term transfer is used even though, initially, only a copy is sent to the other location or system. The records originally residing in the system are retained and only destroyed upon verification that the transfer has been successful.

The term export, on the other hand, refers to the process of producing a copy of complete aggregations, files and records for another system, while the records remain on the originating system – the process does not delete them. In effect the transfer process takes place in two stages – export of a copy with all associated metadata and audit trails, followed by destruction of the original.

In each case, the requirement is to execute the transfer, export or destruction in a controlled manner. In this context "destruction" is different from "deletion".

Ref	Requirement
REQ7.2.5.11.	Whenever the system transfers or exports any class, file, sub-file or volume, the transfer or export must include: • (for classes) all files and records in the class; • (for files) all volumes and sub-files in the file; • all records in all these files, sub-files or volumes; • all or selected metadata associated with all of the above; • all or selected audit trails for all of the above.
REQ7.2.5.12.	The ERMS must be able to transfer or export a file or the contents of a class in one sequence of operations, such that: • the content and structure of its electronic records are not changed; • all components of an electronic record, (when the record consists of more than one component) are exported as one unit; • all links between the record and its metadata and audit trails are retained; • all links between classes, files, sub-files, volumes and records are retained so that they can be reconstituted in the receiving ERMS.
REQ7.2.5.13.	The system must be able to transfer and export records in the format in which they were captured.
REQ7.2.5.14.	The system must be able to transfer and export records in any format(s) into which records have been rendered.
REQ7.2.5.15.	The system should be able to export the entire contents of a class of the classification scheme in one sequence of operations, ensuring that: • the relative location of each file in the classification scheme is maintained, so that the file structure can be reconstructed; • sufficient metadata to rebuild the whole parent class branch is retained and moved with the contents of the class.

REQ7.2.5.16.	The system must ensure that, when a record marked for destruction is destroyed, all its renditions are destroyed.

7.2.6. MANAGEMENT OF PHYSICAL (NON-ELECTRONIC) FILES AND RECORDS

In addition to the electronic records, the records repository may contain non-electronic records. These can include paper-based records and records on other analogue media. They may also include digital records stored on portable media, such as CDs, DVDs and computer tapes.

The system must be able to accommodate references to physical records as well as, and together with, electronic records; and to manage aggregations made up of both electronic and physical records. Classes, files, sub-files and volumes may all contain any combination of electronic records and physical records.

The System must provide features to allow physical containers to be managed. In order to manage physical records the system must be able to capture and manage metadata about them. This metadata enables administrative and user roles to, subject to access controls, locate, track, retrieve, review and dispose of physical records, and to allocate access controls to them in the same way as to electronic records.

Ref	Requirement
REQ7.2.6.1.	The system must allow an administrative role to identify classes, files, sub-files and volumes that exist as physical containers.
REQ7.2.6.2.	The tracking function must log information about the movements of a physical entity which includes: • unique identifier; • current location; • an administrative role-defined number of previous locations (the number to be defined at configuration time); • date moved from location; • date received at location; • user responsible for the move (where appropriate).
REQ7.2.6.3.	The system must allow a user role to see the current location of a checked-out physical entity, its custodian, and the date upon which the check out occurred, subject to access control rights.
REQ7.2.6.4.	The system must behave in an identical manner when dealing with physical or electronic records in searches, save that: • the content of physical records cannot be presented (instead, the system displays its location metadata, see below); • different metadata may be shown for physical and electronic records.

7.3. Workflow

Workflow technologies transfer electronic objects between participants under the automated control of a program. In our context, workflow is used to move electronic files and/or documents and records between users, departments and application programs. It is used for:

- **managing critical processes such as registration and disposition procedures of files or records;**
- **checking and approval of records before registration;**
- **routing records or files in a controlled way from user to user for specific actions, for instance check document, approve new version;**
- **notifying users of the availability of records;**

- **distribution of records;**
- **managing records through case work processes.**

The system should be compatible with the Workflow Management Coalition (WfMC) Reference Model.

Ref	Requirement
REQ7.3.1.1.	The system must allow workflows which consist of a number of procedural steps, each step being (for example) movement of a document, record or file from one participant to another for action or decision.
REQ7.3.1.2.	The system must recognise as "participants" both users and work groups.
REQ7.3.1.3.	The system must allow pre-programmed workflows to be defined by administrative roles.
REQ7.3.1.4.	The system should manage the files and records in queues which can be examined and controlled by administrative roles.
REQ7.3.1.5.	The system must allow users to monitor the progress of workflows they initiate and in which they are participants.
REQ7.3.1.6.	The system should be able to rely on priority attributes and organise items in queues by priority.
REQ7.3.1.7.	The system should include "rendezvous" processing. *This requires the workflow to be paused to await the arrival of a related electronic document or record. When the awaited item is received, the flow resumes automatically.*
REQ7.3.1.8.	Administrative roles should be able to allocate permissions to individual users so that they are able to reassign tasks/actions in a workflow to a different user or group. *A user may wish to send a file or record to another user because of the record content, because the assigned user is on leave, or for other reasons.*
REQ7.3.1.9.	The system should enable participants to view queues of work addressed to them
REQ7.3.1.10.	The system should provide conditional flows that depend on user input or system data to determine the direction of the flow.
REQ7.3.1.11.	The system must notify a user participant when a file or record(s) has been received in the user's electronic "in tray" for attention.
REQ7.3.1.12.	The system should support tracking of files and records by the provision of bring forward (also referred to as "tickler") facilities which enable a user to request a reminder to access the file or record on a future date.
REQ7.3.1.13.	The system must provide a mechanism to allow users to notify other users of records requiring their attention.
REQ7.3.1.14.	The system should allow the receipt, in specified folders, of electronic documents or records to trigger workflows automatically (the workflow being determined by the document type or other metadata value).
REQ7.3.1.15.	The system must ensure that all access controls are maintained at all times.

7.4. Task Management

Task management system must provide work groups with a flexible easy to manage tool that gives customer service managers, team leaders, clients and service providers access to all relevant current and historic information associated to their tasks. Because the task management system supports direct collaboration with clients and service providers, communication efficiency is significantly improved.

Effective task management suppose managing all aspects of a task including its status, priority, time, human and financial resources assignments, recurrences, notifications and so on.

Ref	Requirement
REQ7.4.1.1.	Task management must be able to manage resource information assigned to each task.
REQ7.4.1.2.	Task management system should allow task notes to be added by anyone who has been associated to a task with the user entering the note having control over who sees it.
REQ7.4.1.3.	A provision should be made within the task management system to attach links to documents associated to the task. The system must store the link so it can be opened from the task or attach it to an e-mail notification.
REQ7.4.1.4.	Task management system should allow tasks to be grouped by type providing more informative reporting. There is no restriction to the task types available as the system administrator dynamically sets them.
REQ7.4.1.5.	An open task can have its priority raised by the client or owner at any point, allowing them to escalate an issue and improve the task management process. Task recipients should be notified by e-mail when a task has been escalated.
REQ7.4.1.6.	Task management system should allow tasks to be automatically generated at regular intervals. The system will store a task template and uses the current due date assigned to that template to determine when a task is generated and then uses the frequency period assigned to that template to calculate the next due date.
REQ7.4.1.7.	Task management system should provide an interface for users to schedule events related to a task. The interface must provide a weekly snapshot of meetings related to specific tasks in the system. Users to be sent reminders via e-mail of pending events and the scheduled time also appears in the user's task list.
REQ7.4.1.8.	Task management system should provide reminders (based on clocks and watches, but with computer implementation possible) that can be used to alert of the time when a task is to be done.

7.5. Administrative Functions

These facilities allow administrative roles to manage change in the user population and parameters affecting the behaviour of the system. The system must provide monitoring capability for system errors.

7.5.1. General Administration

This section includes requirements for managing system parameters, system management and configuration, and user administration. The functionality described in this section may be assigned to an operations function rather than to an application administrator.

Ref	Requirement
REQ7.5.1.1.	The system must allow administrative roles to retrieve, display and re-configure systems parameters and settings made at configuration time.

REQ7.5.1.2.	The system must allow administrative roles to: • allocate functions to users and roles; • allocate one or more users to any role.
REQ7.5.1.3.	The system must monitor available storage space, and notify administrative roles when action is needed because available storage is below a level set at configuration time, or because of another error condition.

7.5.2. REPORTING

Flexible reporting is required so that administrative roles can manage the system; and so that management can monitor the system to ensure that it is used appropriately.

The system needs to be able to provide a number of management, statistical and ad hoc reports so that administrative roles can monitor system activity and status. This reporting is required across the entire system, including:

- the classification scheme;
- files and records;
- user activity;
- access and security permissions;
- disposition activity.

The system must provide a number of standard reports capable of being configured by administrative roles and should be flexible to enable ad hoc reports to be produced on demand.

Ideally the ERMS will include or integrates with a flexible report-writing sub-system.

Ref	Requirement
REQ7.5.2.1.	The system must allow administrative roles to produce periodic reports (daily, weekly, monthly, quarterly) and to specify ad hoc reports.
REQ7.5.2.2.	A user viewing a report within the system should be able to capture it as a record.

7.5.3. CHANGING, DELETING AND REDACTING RECORDS

A basic principle of recordkeeping is that records cannot normally be changed, and (except at the end of their life cycle) files, sub-files, volumes and records cannot normally be destroyed.

This section deals with the requirements for exceptional situations where the content of a declared record may need to be amended, or a record deleted and replaced.

The action of deletion may mean one of two things:

- destruction;
- retention, accompanied by a notation in the record's metadata that the record is considered removed from records management control.

In either case, deletion is to be exceptional, and so the ability to delete must be tightly controlled in order to protect the general integrity of the records. In particular, information about deletions must be stored in the audit trail.

Administrative roles sometimes need to publish, or make available, records containing information which is still sensitive, without revealing the sensitive information. This can result from data protection rules, security considerations, commercial risk, etc. For this reason, administrative roles need to be able to mask the sensitive information, without affecting the underlying record.

The process is referred to here as redaction. When this process is carried out, the result is the original record (unchanged), and a copy of the record which has been masked in some way (the redacted copy, or redaction of the original record). The system stores both the original record and the redaction.

Ref	Requirement
REQ7.5.3.1.	The system must allow user roles to mark classes, files, sub-files, volumes and records as candidates for deletion.
REQ7.5.3.2.	The system must allow administrative roles to create one or more redaction(s) of a record while retaining the original record.
REQ7.5.3.3.	Upon creation of a redaction the system should automatically declare redactions as records, classifying them in the same aggregation as the original record and prompting the creator of the redaction for: • a reason; • security category (where applicable).

7.5.4. SYSTEM ADMINISTRATOR LOAD

The MFAEI will need to handle significant amounts of support and assistance tasks to allow personnel undertake their ordinary tasks.

It is required that the IIS allows for delegation of administrative tasks to workgroups so that someone is able to take the Administrative role and responsibility for the outputs of the workgroup. This will reduce the need for administrative tasks to handle all the requests from personnel regarding rights, allocation, available functions etc.

In order to reduce System Administrator load the MFAEI needs a clear description of administrative tasks that can be delegated to workgroups, the possible impact of errors, guidelines and practices for their use. This way System Administrators will be able to assess the implications and delegate administrative tasks according to organization policies and will thus be able to reduce their own load.

7.6. MFAEI Web Site integration

In order to better facilitate a clear, consistent image of Moldova's government and the services it offers, the solution should include a centralized publishing tool that gives each embassy access to Web portals, without requiring sophisticated IT knowledge.

The solution will makes government services more accessible, enabling citizens to access a wide variety of electronic consulate services. The system provides an official, centralized portal for government news.

The multilingual (Romanian/English) portal will allows citizens to customize their experience, while the platform incorporates the latest standards-based security technologies.

The requirement for MFAEI Web Site integration consists of two aspects:

- **Web Site content management and the role of the IIS and**
- **integration of MFAEI Web Site with the Government Portal.**

7.6.1. INTEGRATION WITH CONTENT MANAGEMENT SYSTEMS

CMSs include and extend EDMS functionality across all forms of information (content), not just records. CMSs Common characteristics are:

- **publishing information, often to websites or portals, and sometimes to several channels using different renditions;**
- **managing information that originates from several sources;**
- **reformatting information and/or migrating it to some different rendition(s);**
- **relating different versions, renditions and translations of documents to each other;**
- **managing components of documents.**

7.6.2. WEB SITE CONTENT PUBLICATION

The MFAEI currently operates a Web Site that is independent of other MFAEI systems. The published content on the site is manually administered by MFAEI personnel – Web Site Administrators. At the current stage, the MFAEI does not intend to replace the current implementation.

Still there is a difficulty identifying the publishable information and Web Site Administrators must double check and ensure what information can be published. This causes delays in publishing content on the site. More so, due to limited knowledge of the entire body of documents, resolutions and records produced within MFAEI, some of the publishable information is never published. This reduces transparency of MFAEI activities and impacts its trustworthiness with the population.

It is therefore required that the IIS automatically includes the publishable information/documents in Web Site Administrator team's workspaces so that they know every single information item produced by the MFAEI. This is achieved by use of a publishable/public attribute assigned to records either manually or automatically within workflows.

For specific document and records types Web Site Administrators can define additional workflows within IIS that automatically

- **double check with superiors before actually transferring the information items to the Web Site**
- **automatically publish parts or entire documents on the Web Site.**

At the current moment Web Site administrators will continue to publish the information manually, i.e. once they have the publishable information items confirmed they will manually transform them into formats acceptable for Web Site publication with references to originals.

7.6.3. MFAEI WEB SITE - GOVERNMENT PORTAL INTEGRATION

The MFAEI Web Site implementation must conform to The Decision of the Government of the Republic Of Moldova on the Concept of governmental portal (no. 916 of 06.08.2007) currently in force.

In short, this requires the current Web Site implementation to be extended with a portlet publication mechanism that will allow the Government Portal to subscribe to various information areas of the MFAEI Web Site to be published in the portal.

Exact implementation details will be obtained from the decision mentioned above and from Government Portal Administrators who will provide with exact requirements for integration.

7.7. Instant Messaging, Voice and Fax integration

The IIS incorporates the new infrastructure for phone, fax services, and instant messaging. These work transparently both internally and in remote locations so that MFAEI personnel can call each other without the need to know exactly how the message is routed - via PSTN, VoIP, Instant Message notifications or file attachments (faxes and voice mail).

It is important that facsimile exchanges are not corrupted by reliance on voice specific services such as VoIP.

Integrating telephony and fax, voice internet services, instant messaging relies on specialist skills and equipment. These requirements and needs are not listed here and should be clarified as part of a separate exercise. Only the requirements specific to IIS are presented here.

Ref	Requirement
REQ7.7.1.1.	The IIS must keep a log of all exchanges made via phone, fax, voice message or instant message.
REQ7.7.1.2.	The system integrates information about phone, fax, voice message or instant message in user personal workspaces.
REQ7.7.1.3.	The system allows participants to an exchange to capture as records details of the conversation. Attachments to a conversation might be captured individually.

REQ7.7.1.4.	Failed or cancelled exchanges are registered as notifications to receivers of the call.

7.8. Management of installed software licenses

When businesses and governmental agencies direct their IT organizations to establish a practice of software license management to meet compliance standards and minimize the risk of external audit, IT leaders seek technology designed and provided by commercial vendors. The expectations are seemingly straightforward; deliver software license management functionality that supports:

- Identifying installed software products,
- Matching installed software products to existing software licenses,
- Reporting compliance status.

System of Management of installed software licenses should scan the network and automatically discovers all software available in each of the workstations. Asset Managers can easily ensure compliance by keeping a check on list of compliant, under licensed and over licensed software.

Ref	Requirement
REQ7.8.1.1.	The system should scan all installed software in the network and automatically discovers all software available in each of the workstations. That will help to understand how many installations of software are available in your network.
REQ7.8.1.2.	The system should classify all paid software as managed to effectively focus on software license management, to group scanned software as Freeware, Open source, Shareware, Prohibited, and Excluded.
REQ7.8.1.3.	The system should scan and fetch Microsoft Windows and Office Keys during IT inventory audit. Key-in all the licenses that was purchased earlier, the system should match the discovered license and license in store automatically in the next scan.
REQ7.8.1.4.	The system should help the asset manager to easily track and ensure that the installed software does not exceed purchased software. To gives a software violation warning when installation exceeds purchase. Asset Managers to purchase new software licenses or uninstall existing installations to ensure compliance.
REQ7.8.1.5.	As anyone can install software in the network, the software compliance can be violated anytime. The system scheduled will scan software compliance and should alert asset manager via e-mail when someone violates it.

8. SYSTEM NON-FUNCTIONAL REQUIREMENTS

8.1. Controls, Security and Data Integrity

When moving to the new Integrated System the MFAEI expects to be able to control who is permitted to access records and in what circumstances, as records may contain personal, commercial or operationally sensitive data.

Restrictions on access also need to be applied to external users, i.e. to shared parts of the repository with partner organisations.

Any access to records and all other activities involving them and related documents or data also need to be logged in the audit trail to ensure legal admissibility and to assist in data recovery. Security of records also includes the ability to protect them from system failure by means of backup, and the ability to recover the records from backups.

Vital records are mission-critical records that need to be recovered rapidly after a disaster.

8.1.1. ACCESS

Access control to records is typically achieved by the specification and implementation of security policies, i.e. access to records is granted based on the business role an individual plays in the MFAEI. Users are managed centrally and simultaneously granted access rights to a number of ministry systems.

In addition to the entitlement to access specific parts of the classification scheme, permissions also restrict the actions that a user, role or group can perform on entities within the system, such as inspecting their metadata or their contents, modifying or deleting them and creating or viewing entities of a particular type.

Permissions are applied to groups and are inherited by the group members. Applying permissions at the group level, rather than the user level improves the management of the system over time as new users arrive, and existing users change and leave.

Ref	Requirement
REQ8.1.1.1.	The system must not allow any person to carry out any action in the ERMS unless the person is an authorised user who is successfully identified and authenticated.
REQ8.1.1.2.	The system must allow administrative roles to allocate access to records, sub-files, files, classes and metadata to specified users and/or user roles and/or user groups and for specified periods of time.
REQ8.1.1.3.	The system must allow administrative roles to use permissions to: • restrict access to specific files or records; • restrict access to specific classes of the classification scheme; • restrict access according to the user's security clearance (where applicable); • restrict access to particular features and functions (e.g. read, update and/or delete specific metadata elements); • deny access after a specified date; • allow access after a specified date.
REQ8.1.1.4.	The system relies on integrated network log-on.
REQ8.1.1.5.	The system allows administrative roles to set up and maintain groups of users.
REQ8.1.1.6.	Examples of groups might be Human Resources, Northern sales team.
REQ8.1.1.7.	The system must allow roles with ownership of records to specify which other users or groups can access those records.
REQ8.1.1.8.	If a user performs any search that includes content searching (typically, but not necessarily, a full text search or free text search), the system must not include in the result list any record for which the user does not have the permissions to access.

8.1.2. ELECTRONIC SIGNATURES

An electronic signature is:

- **uniquely linked to the signatory;**
- **capable of identifying the signatory;**
- **created using means that the signatory can maintain under his sole control;**
- **linked to the data (e.g. record) to which it relates in such a manner that any subsequent change of the data is detectable.**

Electronic signatures are also used to provide non-repudiation – repudiation refers to any act of disclaiming responsibility for a message. Non-repudiation provides proof of the integrity and origin of data which can be verified by any third party at any time. It prevents an individual or entity from denying having performed a particular action related to data such as approval, sending, receipt, knowledge (recognizing the content of a received message) or delivery (receipt and knowledge).

Ref	Requirement
REQ8.1.2.1.	The system must be able to capture, verify if required, and store, at the time of record capture, electronic signatures, associated electronic certificates and details of related certification service providers.
REQ8.1.2.2.	The system must enable administrative roles to configure the system, either at configuration time, or at a later date, to store verification metadata for electronically signed records, including public keys, with the record at time of capture in one of the following ways: • the fact of successful verification; • specified information regarding the verification process; • all verification data.
REQ8.1.2.3.	The system should have a standards-based interface which permits the introduction of new electronic signature technologies as they are introduced.
REQ8.1.2.4.	The system should be capable of checking the validity of an electronic signature, including checking the certificate of a record at the time of capture against an electronic certificate revocation list and should store the result of the check in the record's metadata. It should report any invalid check result to a specified user or administrator role.
REQ8.1.2.5.	When capturing e-mail messages the system must be able to capture automatically, and preserve as metadata, details about the process of verification for an electronic signature, including: • the fact that the validity of the signature was checked; • the identity of individual initiating the check (where relevant); • the certificate issuer; • the serial number of the electronic certificate, verifying the signature; • the certification service provider with which the signature has been validated; • the date and time that the checking occurred.
REQ8.1.2.6.	The system should include features which demonstrate that the integrity of records bearing electronic signatures has been maintained.
REQ8.1.2.7.	The system should be able to store with the electronic record: • the electronic signature(s) associated with that record; • the electronic certificate(s) verifying the signature.

8.1.3. ENCRYPTION

Encryption is the process of applying a complex transformation to an electronic object so that it cannot be presented by an application in a readable or understandable form unless the corresponding decryption transformation is applied. This can be used to secure electronic objects, by use of transformations which require the use of secure electronic key codes.

The requirements in this section apply only where there is a requirement to manage records which are encrypted.

Ref	Requirement
REQ8.1.3.1.	Where an electronic record has been sent or received in encrypted form by a software application which interfaces with the system, the system must be capable of restricting access to that record to users listed as holding the relevant decryption key, in addition to any other access control allocated to that record.
REQ8.1.3.2.	The system must be able to capture and store, at the time of record capture, information relating to encryption and details of related verification agencies.
REQ8.1.3.3.	The system must be able to support the automatic encryption and distribution of the same message to many addressees, i.e., a circular note to the heads of missions.

8.1.4. SECURITY CATEGORIES

Clearances take precedence over any access rights which might be granted. This is achieved by allocating one or more "Security Categories" to classes, files, sub-files, volumes and/or records.

The term "Security Category" is used in this specification to mean "one or several terms associated with a record which defines rules governing access to it."

Users can be allocated a single security clearance which prevents access to all aggregations or records which have been allocated higher security categories.

Ref	Requirement
REQ8.1.4.1.	The system must allow one of the following options to be selected at configuration time: • security categories are assigned to classes, files, sub-files and/or volumes (and not to individual records); • security categories are assigned to individual records (and not to classes, files, sub-files and/or volumes); • security categories are assigned both to individual records and to classes, files, sub-files and/or volumes.
REQ8.1.4.2.	For at least one sub-category, the IIS must support a hierarchy of at least five levels, from unrestricted access at the highest level to highly restricted access at the lowest level.
REQ8.1.4.3.	The system should recognize security clearance allocated to a role and inherited by users. Where a security clearance is inherited from a role, the system must allow a different security clearance to be applied at the individual user level.

8.1.5. VITAL RECORDS

Vital records are the records that are considered absolutely essential to the MFAEI's ability to carry out its business functions. The identification and protection of such records is of great importance to any organisation and it is likely that it is these records that will need to be recovered first in the event of a disaster.

Records may be considered as vital records either for the organisation as a whole or part of the organisation.

8.1.6. AUDIT TRAILS

An audit trail is a record of actions taken which involve the system. This includes actions taken by users or administrative roles, or actions initiated automatically by the system as a result of system

parameters. The audit trail shows whether business rules are being followed and ensures that unauthorised activity can be identified and traced.

In order to support accountability it is essential that the system is able to log in the audit trail any action where any degree of automated or machine assisted processing is implemented within the system.

The audit trail is a key factor in enabling the system to fulfil security requirements by maintaining a complete log of all the actions on every record (subject to the constraint of the level of security of the technical environment).

Ref	Requirement
REQ8.1.6.1.	The system must keep an unalterable audit trail capable of automatically capturing and storing information about: • any action taken on any record, any aggregate or the classification scheme; • the user undertaking the action; • the date and time of the action. *The term "unalterable" in this requirement means that it must be impossible for any user or administrator to change or delete any part of the audit trail.*
REQ8.1.6.2.	The audit trail parameters must be configurable so that administrative roles can configure which actions are automatically logged.
REQ8.1.6.3.	The system must maintain the audit trail for as long as is required by the organisation's records policy.
REQ8.1.6.4.	The system must log in an audit trail all actions performed on records, volumes, sub-files, files, classes and retention and disposition schedules, regardless of whether the action affects one or more of them.
REQ8.1.6.5.	Any annotation of or amendment to a record must be logged within the record's audit trail.

8.1.7. BACKUP AND RECOVERY

Backup and recovery functions lie within the ministry's IT operations area.

8.1.8. DATA MIGRATION

The MFAEI does not plan any extensive Data Migration from its existing file repositories and databases. Data Migration will not be performed as part of this project.

Still, MFAEI intends to do a series of bulk imports from both computer files as well as by scanning current and archived paper records at a later phase by itself. It might require some consultancy and assistance at that stage but this will be handled as a separate engagement.

8.2. Ease of Use

When considering non-functional requirements in developing a specification, these must include the degree of ease of use required, and how it is to be specified. This depends on the kinds of user for whom the system is intended, and the amount of training that is to be undertaken, on whether it is compatible with the way people work in real life situations. Even if an Integrated System contains all the features needed for records and document management, task management, seamless integration, configurability and extensibility etc., an implementation will only succeed if users find it easy to use. If users find it difficult to use, it will be rejected despite its capabilities.

This means that a user who is performing a process should:

- **have the option of performing the process, or of not performing it;**

- be able to initiate the function easily, preferably with a single click, and without needing to re-enter information that has already been entered;
- be able to choose, at the end of the function, either to cancel the original process or to return to it at the same point and with the same status as before the function was initiated (without needing to re-enter information that has already been entered).

Ref	Requirement
REQ8.2.1.1.	The system should offer a multilingual User Interface and it must be configured to support Romanian and English. Adding support for other languages should be possible.
REQ8.2.1.2.	The system should include help on use of the classification scheme, including, at a minimum, easy access to the description metadata for classes, files, sub-files and volumes.
REQ8.2.1.3.	The user interface should be suitable for users with the widest range of needs and abilities; that is, designed according to suitable accessibility standards and guidelines, and compatible with common specialised accessibility software.
REQ8.2.1.4.	The user interface rules and behaviour must be consistent across all aspects of the system including windows, menus and commands. These must also be consistent with the operating system environment in which the system operates.
REQ8.2.1.5.	Frequently-executed transactions must be designed so that they can be completed with a small number of interactions (e.g. mouse clicks or keystrokes).
REQ8.2.1.6.	The system should be tightly integrated with the organisation's e-mail system in order to allow users to send records and aggregations electronically.
REQ8.2.1.7.	The system should allow users to define cross-references between related records, both within the same aggregation and in different aggregations, allowing easy navigation between the records.
REQ8.2.1.8.	A user working with a file must be able to discover easily and quickly the keywords associated with that file.
REQ8.2.1.9.	The system should allow users to define classes, files and records as "favourites", so that they can find them easily on later occasions.

8.3. Performance and Scalability

The response times experienced by users will also depend on factors outside the system, including:

- network bandwidth;
- network utilisation;
- network latency;
- configuration and utilisation of various server resources.

Performance requirements will be checked using a clean, widely used, modern browser to be agreed upon with the customer.

Ref	Requirement
REQ8.3.1.1.	The system must provide adequate response times to meet business needs for commonly performed functions under standard conditions, for example: • <50> users logged on and active; • <50%> of the anticipated total volume of documents managed by the system; • with consistency of performance over at least ten transaction attempts.

Ref	Requirement
REQ8.3.1.2.	The system must be able to return the results of a simple search (the hit list) within <5 seconds> and of a complex search (combining four terms) within <10 seconds> regardless of the storage capacity or number of files and records on the system.
REQ8.3.1.3.	The system must be able to retrieve and display within <5 seconds> the first page of a record which has been accessed within the previous <2> months.
REQ8.3.1.4.	The system must be able to retrieve and display within <20 seconds> the first page of a record which has not been accessed within the previous <6> months, regardless of storage capacity or number of files/records on the system.
REQ8.3.1.5.	The system should provide comparable response times once the classification scheme significantly increases in size to accommodate the needs.
REQ8.3.1.6.	*The requirements above do not apply to playback of media files, download of large files, preparation of reports. These are not considered "typical use scenarios".*

8.4. System Availability

The introduction of an integrated system will increase users' dependence on the IT network to the extent that they will be unable to continue working if the system becomes unavailable. Due to this measures must be taken so that System Availability is as high as possible. Besides this, the system must support a series of features that allow users to work on ordinary tasks while offline - similar to Remote Users.

Ref	Requirement
REQ8.4.1.1.	Due to worldwide distribution of MFAEI diplomatic missions the system must be available to users for a full 24hours <on all work days>.
REQ8.4.1.2.	Planned downtime for the system must not exceed <3> hours per <rolling three month period>.
REQ8.4.1.3.	Unplanned downtime for the system must not exceed <3 hours> per <rolling three month period>.
REQ8.4.1.4.	The number of incidents of unplanned downtime for the system must not exceed <3> per <rolling three month period>.
REQ8.4.1.5.	In the event of any software or hardware failure, it must be possible to restore the system to a known state within no more than <1> hour of working hardware being available.

8.5. Technical Standards

The system should comply with relevant standards. It is desirable that the system relies on open interfaces.

Ref	Example Requirement
REQ8.5.1.1.	The system must support the storage of records using file formats and encoding which are fully documented.
REQ8.5.1.2.	The system should store all dates in a format compliant with ISO 8601, Data elements and interchange formats – Information interchange – Representation of dates and times.
REQ8.5.1.3.	The system should store all language names in a format compliant with ISO 639, Codes for the representation of names of languages.
REQ8.5.1.4.	The system is to manage records in multiple languages using non-English

Ref	Example Requirement
	characters, it should be capable of handling ISO 10646 encoding (Unicode).

8.6. Long Term Preservation and Technology Obsolescence

Electronic records held over a long term face technological risks from three directions:

- **media degradation;**
- **hardware obsolescence;**
- **format obsolescence.**

More detailed consideration is found in ISO 18492, and in a large number of guidance publications produced by cultural memory institutions and others.

Media degradation and Hardware Obsolescence risks should be mitigated by reliance on external procedures, processes and decisions. One of the mitigating measures is to rely on Archival Media and Hardware that is widely in use and with the smallest possibility of obsolescence.

Format obsolescence presents the most difficult problem for any period longer than a few years. Currently there is no simple, generic method which will guarantee long term access to electronic records. The consensus is that the most appropriate strategy is to hold information only in widely-accepted, stable, open formats (i.e. formats which are comprehensively documented in publicly-available specifications) which have a long expected life, such as XML and PDF/A.

Ref	Requirement
REQ8.6.1.1.	The system should be able to report on the file formats and versions of components.
REQ8.6.1.2.	The system should be able to render records from their original format(s) to any specified long term preservation file format(s) at the time of capture, at any subsequent time, or on export.
REQ8.6.1.3.	When a record has been rendered into a preservation file format, the system must provide suitable facilities to retrieve the original format and/or renditions, as appropriate.
REQ8.6.1.4.	The system should hold at a minimum the following metadata items for a rendered component: • the original file format and version; • date of rendition.
REQ8.6.1.5.	If the system uses any proprietary encoding or storage or database structures, these must be fully documented, with the documentation being available to administrative roles.

9. INTEGRATION WITH STATE INFORMATION RESOURCES

All state information resources – from departmental and regional basis, should be 100% integrated. Integrating information resources means that each information resource contains

- **complete information about its own objects and records.**
- **minimum necessary information (in perspective – just identifiers) of borrowed objects and records.**

The design phase of MFAEI SIA will describe in detail, the integration of state resources. Technologically, it ensures integration through:

- **Storing unique information objects;**
- **Use a general state scheme of information objects identifiers;**
- **Use a general state system of classifiers;**
- **Rely on unified telecommunications architecture.**

Such an approach allows the possibility of providing an integrated information space with preservation of autonomy of each individual component.

It must be mentioned that the IIS will at least integrate with:

- **Root Certification Authority and Government Certification Authorities in Moldova to establish chains of trust for digital certificates.**
- **Governmental and other Public Authorities Directory Services to establish to establish a single trusted domains user infrastructure.**
- **“State Register of Population” (“Registrul de Stat al Populatiei"), "State Register of Organizations" ("Registrul de Stat al Unitatilor de Drept") and “State Register of Transport” ("Registrul de Stat al Transportului"). Access to these will be made mainly from MFAEI missions abroad for consular purposes (to identify the undocumented persons, etc.) and represents an important component in consular work.**
- **Data bases of “Border Guard Service”, Directorate of Migration and Asylum of MAI, the SIA of the Ministry of Justice. These provide data on people movement and migration, criminal records, statutory documents etc.**

10. DOCUMENTATION AND TRAINING

It is essential to train people at all levels in the principles of information management, particularly with respect to filing and record capture discipline, the control of documents and managing their lifecycle.

It will not be possible to move entirely to the new system in a single step and the MFAEI expects to increasingly rely on IIS in line with personnel acceptance of the new system. Training will be required in the customer service aspects of working with and delivering information and also on information management standards. This will extensively involve the administrative personnel during the early stages of IIS implementation.

Where external training is available for COTS components of the system externally, these should be listed and estimate costs should be provided.

In order to ensure appropriate levels of competence it is required to perform extensive training to an "early adopters" group of personnel from different departments including system administrators. Training will be given in Romanian but it is expected that trainers are able to communicate in Russian too. The following training is required:

- **Training of trainers - extensive training of one group of selected users so that they are able to transfer knowledge to their colleagues.**
- **User training - basic training to cover most of the local personnel of MFAEI related to basic features of the systems available to user roles. The actual trainings will extend a longer period of time so that personnel can attend when the MFAEI activities a affected minimally.**
- **Administrator training - extensive training for a group of 3-5 in the internal/administrative features of the system and its components.**
- **Management training - short and small goal sessions that will introduce managers of various levels to specific review, approval and signing features available.**

The MFAEI expects commitment from the supplier to train in the future under a separate agreement.

Documentation will include:

- **User Guide(s) - that describe user facing features of the system. In case the solution is based on multiple components, there will be a User Guide for each of them.**
- **Administrator's Guide(s) - that describe administrative, configuration and maintenance features of the system. In case the solution is based on multiple components, there will be a User Guide for each of them.**
- **Installation Guide(s) including a general Installation Guide in case the solution is based on multiple components.**
- **Training materials prepared for training above.**
- **Knowledge base that includes answers to frequently asked questions, best practices etc.**

Documentation will be prepared in a single language and must include an electronic format. Documentation on paper is optional and can be included as part of the offer.

Any source code and configuration settings developed during this project will be transferred to MFAEI so that it is able to continue development and configuration in the future.

11. ACCEPTANCE AND SUPPORT

The MFAEI requires inclusion of both Acceptance and Support periods for the system.

Acceptance will take 6 weeks and during this period the MFAEI will operate the system and report any non-conformity. Acceptance criteria will be based on current requirements and will be agreed upon during analysis and design stages of the project. Non-conformities must be addressed in full by the Supplier. Critical non-conformities will extend the acceptance period for 2 weeks after a fix is delivered.

The MFAEI requires at least 6 months of Support and Maintenance of the IIS. The level of support will be proposed by the Supplier. It should take into account the fact that the system is operational 24 hours during workdays and the Supplier must specifically address this aspect in its Support offering.