



SANBI Business Requirements Specification for EDRMS System

TABLE OF CONTENTS

1	Introduction	4
1.1	Aim	4
1.2	Background	4
1.3	EDRMS Benefits	5
	The EDRMS will ensure the following benefits:	5
2	Requirements	7
2.1	Capture	8
2.1.1	Capturing of documents	8
2.1.2	Application Independence	8
2.1.3	User interface	9
2.1.4	Scanning	9
2.1.5	Unique identifier	9
2.2	Manage	9
2.2.1	Metadata	9
2.2.2	Electronic signatures	10
2.2.3	Version Control	10
2.2.4	Workflow	10
2.2.5	File Plan	10
2.2.6	Hybrid records Management	10
2.2.7	Integration	11
2.3	Store	11
2.3.1	Search and Retrieval	11
2.3.2	Searching	11
2.3.3	Security	11
2.4	Preserve	12
2.4.1	Deletion of records	12
2.4.2	Retention	12
2.5	Deliver	12

2.5.1	File Format Display	12
2.5.2	Collaboration	12
Appendix A: Acceptance Criteria		14
2.6	General	14
2.6.1	Vendor Certification	14
2.6.2	Licenses	14
2.6.3	Integration with Microsoft Sharepoint and Office 365	15
2.6.4	Professional services	15
2.6.5	Development of policies and procedures	15
2.6.6	Migration and back-scanning	16
2.6.7	Training	16
2.6.8	Change Management	16
2.6.9	Project Management	17
Appendix B: Required Metadata (From NARSSA Minimum Mandatory Metadata Requirements)		71

1 Introduction

1.1 Aim

The aim of this document is to outline the Electronic Document and Records Management System (EDRMS) requirements for the South African National Biodiversity Institute (SANBI).

1.2 Background

Since its inception as a government entity SANBI has created and inherited a large number of documents. These documents, both paper and electronic, are stored in various places that are geographically spread across all nine provinces of the country.

This creates a culture of electronic documents not being easily accessible, and paper documents presenting their own set of problems e.g.

- being labour-intensive to process;
- requiring substantial storage space;
- hard to control;
- easily lost; and
- characterised by slow access times averaging five to fifteen minutes per document.

In addition to the identified inefficiencies, SANBI needs to comply to the requirements of the National Archives and Records Service of South Africa (NARSSA) and implement a solution to manage records in all formats. SANBI has therefore taken the decision to acquire an Electronic Document and Records Management Solution (EDRMS).

A sustainable SANBI EDRM Solution impacts every department, business process, and employee working with information. Technology alone will not resolve the issues.

Change management, resources, roles, training, policy, information analysis and process automation are all critical parts of the Solution.

However, these components cannot work without a core system that has the capacity to automate the process of creating and reporting information, from beginning to end.

This document specifies the business needs and requirements from the EDRMS.

1.3 EDRMS Benefits

The EDRMS will ensure the following benefits:

- Improved efficiency – Automation and standardisation of content and document processes will result in the elimination of many unnecessary steps and improve quick and easy access to information. The Institute can adopt an electronic mind-set thus improving the process associated with managing, accessing and distributing said documents.
- Security and Access control - improved management achieved through standardisation, allocation of access rights, and consistent information security controls at content and document level compliment working methods and the availability of audit trails.
- Improve stakeholder and customer service – the ability to quickly service requests by accurate and consistent flow of information. Consistency in the processes leads to greater predictability in levels of response to customers and other key stakeholders.
- Flexibility – the sharing of information as a resource, the capability to use multi channels for delivery, and enhance the user experience.
- Interoperability – varied platforms, services, systems, schemas, files, ERP and more can be brought together into a singular view and information resources can be shared.
- Capability - makes the Institute more responsive to productivity and performance objectives. Redundant duplication and manual activities are reengineered for performance, accuracy and cost effectiveness.
- Communications - employees and other role players are able to collaborate immediately and effectively on content or decision-making information which is distributed via electronic channels from an EDRMS enterprise capability.
- Information as a Resource – the capabilities and functionalities in the EDRMS allow the Institute to position itself to use the information stored in documents and content, structured and unstructured, effectively across varied channels and process instantaneously to multiple users, employees and stakeholders.

- Cost Reduction initiatives – manual tasks can be converted to Institute rule driven process oriented digital information delivery across platforms and institutional divisions and locations.
- Governance – complete corporate governance, accountability and responsiveness to regulatory compliance through audit ability in content management and applied Institute rules, secured stores that reflect accurate and audited information.
- Performance – quick turnaround times are possible because information is available when needed. This eliminates much manual process tasking and possibly even rework. Information resources are shared across multiple Institution Units and Airports.
- Agility – the ability to find information from many sources more often, more accurately and more relevant empowers the Institute, Institution Units and individual users.
- Accuracy – search and retrieval disciplines enable a measure of consistency, bring with it an improved degree of accuracy through common process and methodology to searching, finding, collating and managing information retrieved.
- Commonality – the EDRMS practices mature over a period of time, become more pervasive through the Institute and allows for commonality in approach, method and principle.
- Reusability – information retrieved and stored is available across the Institute, for varied use, multiple purposes process and decision points using same toolsets, technology infrastructure, standards and principles.

2 Requirements

The following high-level requirements must be met:

- The system must manage electronic documents and records
- Ability to manage and track physical (paper) records
- It must have a User-friendly interface
- It must provide for efficient and effective search and retrieval of information.
- The ability to integrate with other systems through Application Programming Interfaces (APIs), to allow users access to information from various systems; providing a single interface to access to organisational information.
- Collaborative functionality that can assist with knowledge sharing
- Version control.
- Audit trails and functionality to track documents throughout the organisation.
- Identification and reduction of duplicates.
- Incorporate file plans and retention schedules
- Incorporate security classification schemes
- Information Security to manage and protect user access and permissions

For purposes of this document, the EDRMS requirements are presented in a format similar to the AIIM model as illustrated in Figure 1: Enterprise Content Management (ECM) processes:

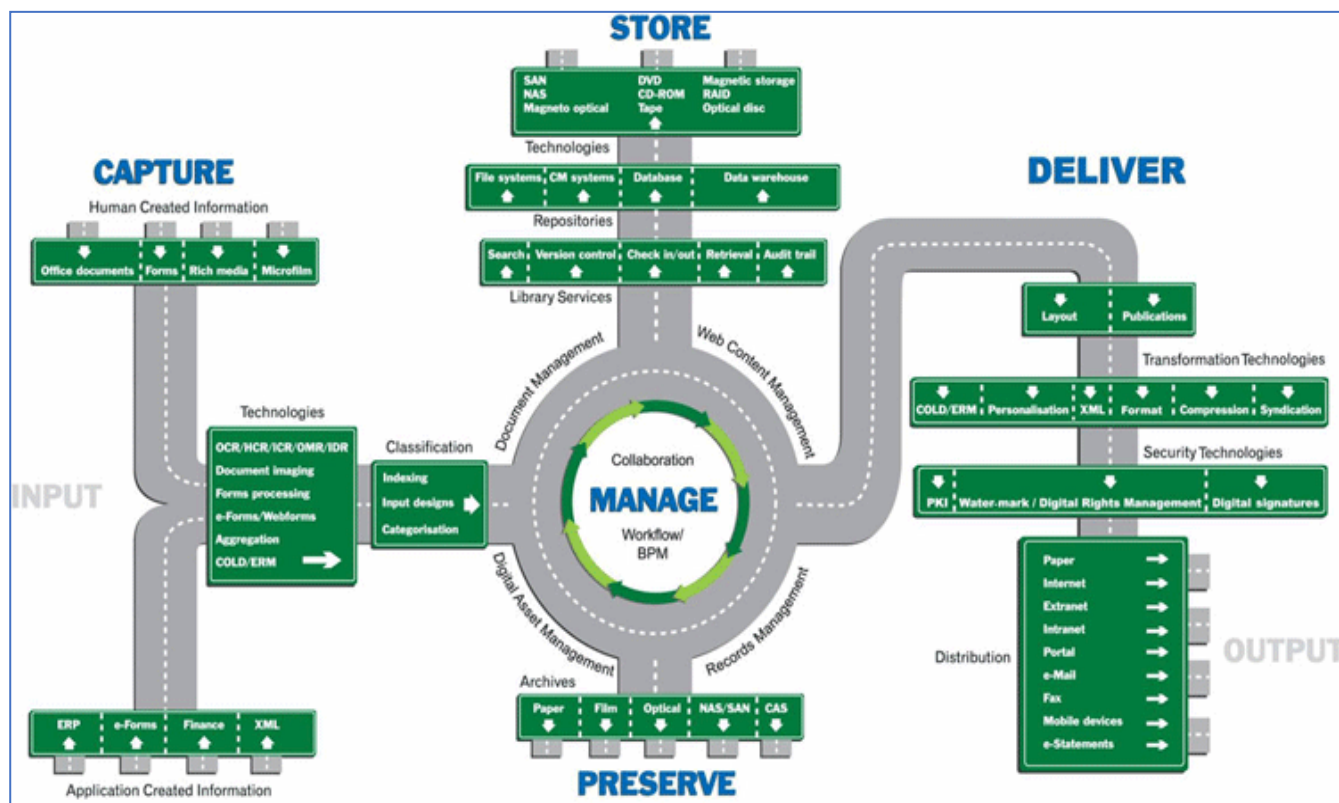


Figure 1: Enterprise Content Management (ECM) processes

2.1 Capture

2.1.1 Capturing of documents

A secured, user-friendly Electronic Document and Records Management System where documents will be captured for centralised access, re-use, management, storage, and distribution must be implemented.

2.1.2 Application Independence

The Electronic Document and Records Management System must provide functionality to capture all documents irrespective of format.

These documents can include (but not limited to) the following:

- Office documents (mostly in Microsoft office but can include other applications).
- Graphical images and schematics (including technical drawings and plans).
- Digital assets such as photographs and videos.
- Email messages together with attachments.
- Scanned images

2.1.3 User interface

The user interface must be user friendly and intuitive. Any system installed must be simple, easy to use and accessible at all times.

2.1.4 Scanning

2.1.4.1 Indexing

The system must be able to integrate with a scanning interface. If a scanning interface is provided it must provide for Optical Character Recognition (OCR) functionality (to ensure that full text retrieval is possible on scanned images). OCR functionality can also be used to determine certain elements on scanned documents (like invoice number, customer name or numbers etc.)

2.1.5 Unique identifier

When captured the system must provide a unique identifier for the specific document. Both external (user defined) and internal (system generated) numbering must be allowed.

2.2 Manage

2.2.1 Metadata

Metadata is descriptive data that provides context to electronic documents and records. Without the necessary metadata, a document cannot be considered to be a record. Metadata gives information about where a document comes from, who the creator is, when was it created, where it is located, etc. Metadata can be described as structure information that describes and or enables finding, managing, controlling, understanding, or preserving other information over time.

2.2.1.1 Required Metadata Elements

The system must be able to include metadata as per NARSSA Minimum Mandatory Metadata Requirement s. Please see Appendix B: Required Metadata (From NARSSA Minimum Mandatory Metadata Requirements)

The system must provide flexibility and ease of use balanced with compliance and records management considerations. The system must have the ability to automate as many as possible of the recommended minimum metadata fields and to configure additional metadata fields only where absolutely required for structured retrieval, workflow, lifecycle management, control, provision of context or reporting. This will promote ease of use as users will only have to select metadata fields from a drop-down menu.

2.2.2 Electronic signatures

As part of managing reviews and approval of documents, the system must allow for integration with electronic signatures.

Suppliers must provide specifications and costs of their preferred Electronic signature platforms.

2.2.3 Version Control

The system must provide the ability to store modifications to a document as a new version or as a revision on a specific version. An audit trail of all modifications must be available.

2.2.4 Workflow

The system must provide workflow functionality:

- Allow different workflows for different document types.
- Provide workflows which consist of a number of steps, each step being (for example) movement of a document from one participant to another for action.
- Not practically limit the number of steps in each workflow.
- Provide a function to alert a user participant that a document has been sent to the user's electronic "in tray" for attention and specify the action required.
- Allow the use of E-mail as a notification system.
- Allow pre-programmed workflows to be defined and maintained by the Administrator.

2.2.5 File Plan

The EDRMS must allow for the use of and incorporation of a NARSSA approved File Plan. The File Plan is to be used for records management to classify records in terms of retention, archival value, disposition, retrieval, and security.

2.2.6 Hybrid records Management

The EDRMS must include functionality for managing records and files in both electronic and physical format. It must support consistency between paper, electronic and hybrid records (kept in both formats). It must provide for the ability to track location and movement of paper files, using bar-code, RFID, or other technologies.

2.2.7 Integration

The EDRMS must provide ability to integrate with other systems in order to allow for information to be exchanged thereby maintaining data integrity and documents to be linked to their system objects or transactions.

2.3 Store

2.3.1 Search and Retrieval

The system must provide for extensive retrieval functionality. The system must provide for full text retrieval and must allow users to search via metadata fields; content types, browse the SANBI file plan or Classification Scheme, browse various taxonomies and allow the user to define profiles in order for information to be pushed to the user when relevant new reports or records are submitted to the repository. It must also allow users to save output and search queries.

2.3.2 Searching

The system must provide the ability to search on the content or text of documents (full text retrieval) using natural language queries – similar to a Google type search on the internet. This functionality must also support retrieval of documents on specific words or concepts and must include the use of Boolean operators (and or not etc.).

2.3.2.1 Browsing

The system must provide the ability to browse the File Plan where documents are aggregated based on metadata or other representation.

2.3.2.2 Metadata Searching

The system must provide the functionality to search on metadata elements and combinations of metadata elements.

2.3.2.3 Presenting Search Results

The system must present the result set in such a way that direct access to an individual document can be gained with one click.

2.3.3 Security

The Electronic Document and Records Management System must provide a security model that will safeguard all files. Functionality must allow for access to documents to be linked to positions (roles), not persons. It must also make allowance for complex security in relation to electronic documents. Security must address maintaining access, availability and integrity of information minimizing the risk of loss, corruption, and unauthorised access. It is regarded as a critical component of the system.

The system must also allow the administrator to limit access to documents, files, and metadata to specified users or user groups. It must also be possible to assign certain security rules to specific document types.

2.4 Preserve

2.4.1 Deletion of records

The system must prevent the deletion of an electronic record or any part of its contents at all times, with the exceptions of:

- Destruction in accordance with a retention schedule.
- Deletion by an Administrator as part of an audited procedure.

2.4.2 Retention

In line with the Retention Periods applicable, the system must:

- Provide a function that specifies retention schedules, automates reporting and destruction actions, and provides integrated facilities for exporting documents and metadata.
- Provide notification to the administrator when retention period is due.
- Be capable of associating a retention schedule with any document, file or folder of the classification scheme.
- Must be able to accommodate the following type of retentions:
 - passage of a specified period of time after the document is created;
 - passage of a specified period of time after a specific event;
 - specified as “indefinite” or “permanent” to indicate long term preservation of the documents.

2.5 Deliver

2.5.1 File Format Display

The Electronic Document and Records Management System must provide the functionality to display all electronic documents irrespective of whether there is a native application or viewer available.

2.5.2 Collaboration

Collaboration relies on openness and knowledge sharing but also some level of focus and accountability on the part of the Institute. Governance must be established

addressing the creation and closing of team workspaces with assignment of responsibility for capturing the emergent results of the collaborative effort for preservation in the repository.

In addition, a central location to capture best practices, share information, and promote standardized Institute processes is imperative, whereby staff can capture and share collective team knowledge or important information through:

- Tracking updates and information with alerts or Really Simply Syndication (RSS)
- Using blogs to share or promote information
- Capturing community knowledge or documenting internal processes by using a wiki
- Using surveys or discussions to gather information or encourage dialogue

Appendix A: Acceptance Criteria

2.6 General

2.6.1 Vendor Certification

Records management functionality must meet the requirements as per:

- Model Requirements for the Management of Electronic Records (MoReq)
- United States Department of Defense Directive 5105.2 (US DoD 5105.2)
- International Organization for Standards - Standard 16175 - Information and documentation — Processes and functional requirements for software for managing records (ISO 16175)

NB: Vendors must provide evidence that they are certified against or can prove that the systems meet the functional requirements of at least one of these specifications.

2.6.2 Licenses

SANBI has a total of 1074 registered users, and a total staff complement of 1500.

SANBI has decided to encourage staff who do not have access to workstations to access the EDRMS via portable devices where required, so as to reduce the number of licences required.

Therefore, the total number of licenses required is:

Component	No of Licenses
-----------	----------------

Document Management	1200
Records Management	1074
Collaboration	1074
Electronic Signatures	100
Workflow	1200

Pricing must be per user, to allow for flexibility in increasing or reducing the number of licences to be procured.

2.6.3 Integration with Microsoft Sharepoint and Office 365

SANBI has licences for Microsoft 365 including Sharepoint. Vendors may opt to use Sharepoint functionality where feasible and then add additional functionality if required using add-on products. If Sharepoint is included in the solution, Adoption and Change Management of Sharepoint must form part of the solution. Design and configuration of Sharepoint sites, libraries, metadata and records management compliance and policies must form part of the solution.

Currently Sharepoint is On Premise.

Vendors may also decide to use a complete suite of products to replace Sharepoint.

2.6.4 Professional services

Design and implementation costs will comprise a large part of the solution. Vendors are to show the proposed approach in detail, outlining activities and costs in detail.

2.6.5 Development of policies and procedures

The following must be included in the pricing:

- Development of a NARSSA approved file plan

- Development of a retention schedule
- Development of a records management policy
- Development of user records management procedures (in addition to system procedures)
- Review of registry procedures

2.6.6 Migration and back-scanning

Volumes of paper records to be back scanned, and electronic records to be migrated have not been ascertained yet. Vendors are to provide unit prices for scanning per million pages or part thereof, and per terabyte for migration of electronic records.

2.6.7 Training

All users are to be trained on the functionality of the EDRMS system.

Super User Training should also be provided with one Super User providing the role of first line support to ten users.

Two administrators should be trained with one administrator performing the function of a dedicated EDRMS administrator.

In line with this the following number of users should be trained:

Type of Training	No of Users
User Training	1500
Super User Training	150
Administrator Training	At least 5

2.6.8 Change Management

The proposed change management methodology and plan must be included

2.6.9 Project Management

The project management methodology and approach must be included. Project management should follow a recognised standard such as Prince 2 or PMBok.

A proposed project plan must be included.

The following table must be completed, as follows:

The Compliance column must be completed with either Yes, No or Partly. If compliance is “partly” then an explanation must be provided.

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
SCANNING					
1.	Scanning	Access	The EDRMS must allow authorised users to be able to open digitised records directly from the EDRMS.		
2.	Scanning	Batch	The EDRMS must allow batch/bulk import of digitised images.		
3.	Scanning	Batch	The EDRMS must separate records in a batch using barcode separation, patch codes or separator sheets.		
4.	Scanning	Capture	The EDRMS must allow single/ad hoc import of a digitised image.		
5.	Scanning	Capture	The EDRMS must provide for a confirmation box for editing, saving, and deleting images.		
6.	Scanning	Control	The EDRMS must alert/prompt users of outstanding indexing of digitised records, quality assurance and exceptions handling, if applicable.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
7.	Scanning	Control	The EDRMS must keep an audit trail of the verification process.		
8.	Scanning	Control	The EDRMS must make provision for thumbnail viewing of digitised pages per record.		
9.	Scanning	Control	The EDRMS must provide for digitised re-import in mid-batch in case of interruption.		
10.	Scanning	Control	The EDRMS must provide for the management of digitised images as multiple pages of a single record.		
11.	Scanning	Control	The EDRMS must ensure that QA and verification includes a matching count of physical pages with digitised pages.		
12.	Scanning	Control	The EDRMS must ensure that the number of pages of a digitised imaged are managed for each record digitised.		
13.	Scanning	Image Enhancement	The EDRMS must ensure that the following functions are performed automatically as well as manually:		
13.1.	Scanning	Image Enhancement	• Deskew.		
13.2.	Scanning	Image Enhancement	• Despeckle/background clean-up.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
13.3.	Scanning	Image Enhancement	Black border removal.		
13.4.	Scanning	Image Enhancement	Blank page removal.		
13.5.	Scanning	Image Enhancement	Enhancing characters (for example, where they are faint or incomplete).		
13.6.	Scanning	Image Enhancement	Hole filling (from hole punches).		
14.	Scanning	Image Enhancement	The EDRMS must ensure that authorised users are able to perform the following image enhancements manually:		
14.1.	Scanning	Image Enhancement	Rotate.		
14.2.	Scanning	Image Enhancement	Trim.		
14.3.	Scanning	Image Enhancement	Rearrange, remove, or add pages to a record.		
15.	Scanning	Image Quality	The EDRMS must ensure that various Scanning profiles are available for different combinations of technical resolution, bit depth, formats and		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
			compression based on specific formats of the original paper record:		
15.1.	Scanning	Image Quality	- Text only, black, and white: - Resolution: Minimum 300 ppi, - Bit Depth: 1 bit (bi-tonal), - Format: TIFF PNG PDF/A containing TIFF or JPEG 20004, - Lossless compression.		
15.2.	Scanning	Image Quality	- Documents with watermarks, grey shading grey graphics: - Resolution: Minimum 600 ppi, - Bit Depth: 8-bit grey scale, - Format: TIFF PNG JPEG 2000 PDF/A containing TIFF or JPEG 2000, - Lossless compression.		
15.3.	Scanning	Image Quality	- Documents with discrete colour used in text or diagrams: - Resolution: Minimum 600 ppi, - Bit Depth: Minimum 8-bit colour, - Format: TIFF PNG JPEG 2000 PDF/A containing TIFF or JPEG 2000, - Lossless compression.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
15.4.	Scanning	Image Quality	• Black and white photographs: ○ Resolution: Sufficient to provide > 3000 pixels across long dimensions, ○ Bit Depth: 8-bit grey scale, ○ Format: TIFF PNG JPEG 2000 PDF/A containing TIFF or JPEG 2000 ○ Lossless compression.		
15.5.	Scanning	Image Quality	• Colour photographs: ○ Resolution: Sufficient to provide > 3000 pixels across long dimensions, ○ Bit Depth: 24-bit colour, ○ Format: TIFF PNG JPEG 2000 PDF/A containing TIFF or JPEG 2000, ○ Lossless compression.		
15.6.	Scanning	Image Quality	• Black and white negatives: ○ Resolution: Sufficient to provide > 3000 pixels across long dimensions, ○ Bit Depth: 8-bit grey scale or 24-bit colour,		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
			- Format: TIFF PNG JPEG 2000 PDF/A containing TIFF or JPEG 2000, - Lossless compression.		
15.7.	Scanning	Image Quality	- Colour negatives and transparencies: - Resolution: Sufficient to provide > 3000 pixels across long dimensions, - Bit Depth: 24-bit colour, - Format: TIFF PNG JPEG 2000 PDF/A containing TIFF or JPEG 2000, - Lossless Compression.		
16.	Scanning	Metadata	The EDRMS must ensure that metadata fields/attributes used in the indexing solution are tightly integrated with the metadata defined in the EDRMS to minimise synchronisation issues.		
17.	Scanning	OCR	The EDRMS must ensure that authorised users are able to capture OCR data and manually copy it to other records, metadata (after record is stored in the EDRMS), etc.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
18.	Scanning	OCR	The EDRMS must ensure that OCR accuracy is above 95%.		
19.	Scanning	OCR	The EDRMS must ensure that Optical Character Recognition (OCR) is performed on digitised images.		
20.	Scanning	Output	The EDRMS must ensure that the Scanning output do not affect the layout of the original paper version.		
21.	Scanning	Output	The EDRMS must ensure that the output format of digitised records is searchable PDF/A that includes an accurate resemblance of the original record in an image as well as the OCR data.		
22.	Scanning	Storage	Before original physical records are filed in the specific physical registry, the user who indexed the record during Scanning must receive a notification from the EDRMS specifying the File Plan Ref # in order to file in the same location as stored in the EDRMS.		

Document Management

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
23.	Document Management	Capture	The EDRMS must provide for storing redlining, annotations, and highlighting separately but associates them with the original.		
24.	Document Management	Capture	The EDRMS must be able to manage virtual documents (documents linked in a virtual structure).		
25.	Document Management	Capture	The EDRMS must ensure that documents can be edited whilst preventing <i>records</i> from being edited.		
26.	Document Management	Capture	The EDRMS must only allow an author to edit a document once it has been checked out.		
27.	Document Management	Capture	The EDRMS must provide a check-out facility which locks the original document and identify documents which authors have checked out.		
28.	Document Management	Capture	The EDRMS must provide the functionality to check in / check out single files or objects as well as batch or mass methods for document check-in/check-out.		
29.	Document Management	Capture	The EDRMS must provide functionality for an author of a document to check-in		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
			or unlock a document checked out by another author.		
30.	Document Management	Capture	The EDRMS must create a new version of a document/record upon check-in.		
31.	Document Management	Capture	The EDRMS must facilitate the use of templates.		
32.	Document Management	Capture	The EDRMS must ensure that users have the ability to drag and drop files from the Windows environment to the EDRMS.		
33.	Document Management	Capture	The EDRMS must ensure that users have the ability to save a document to the EDRMS directly from within Office Applications		
34.	Document Management	Capture	The EDRMS must ensure that version control can include revisioning.		
35.	Document Management	Document Management	The EDRMS must allow created documents to be stored in their native formats.		
36.	Document Management	Document Management	The EDRMS must be able to import any file type.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
37.	Document Management	Document Management	The EDRMS must be able to manage the following files Microsoft Word, Microsoft Excel, Microsoft PowerPoint, Microsoft Project, Microsoft Visio, PDF, HTML, MS Outlook, Lotus Notes, JPEG, GIF, PNG, BMP, TIFF, CSV, RTF, Voice, Digitised sounds, Executable documents, Compressed documents		
Bulk Importing					
38.	Bulk Importing	Bulk Importing	- The EDRMS must be able to capture in bulk records exported from other systems, including capture of: - electronic records in their existing format, without degradation of content or structure, retaining any contextual relationships between the components of any individual record;		
39.	Bulk Importing	Bulk Importing	electronic records and all associated records management metadata, retaining the correct contextual relationships between individual records and their metadata attributes		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
40.	Bulk Importing	Bulk Importing	The EDRMS must be able to produce a report detailing any failure during a transfer, export or destruction. The report must identify any records destined for transfer that have generated processing error, and any records that are not successfully • transferred, • exported or • destroyed.		
System Portability					
41.	System Portability	System Portability	The EDRMS must have an up-to-date, commonly used and supported software framework, be web-based, and be accessible via standard internet browsers, mobile web devices, and tablets		
42.	System Portability	System Portability	The EDRMS must provide all the functionality of the system via remote access		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
Metadata					
43.	Metadata	Administrative Metadata	The EDRMS must allow the administrator to change any user-entered metadata element.		
44.	Metadata	Administrative Metadata	The EDRMS must allow the administrator to pre-define (and re-define) the metadata elements associated with each record, including whether each element is mandatory or optional.		
45.	Document Management	Document Management	The EDRMS must allow the following metadata to be captured by default:		
45.1.	Metadata	Administrative Metadata	Unique Identifier: EDRMS must be able to generate a sequentially assigned alpha numeric identifier with no intelligence and structure in the numbering. The EDRMS must further.		
45.1.1.	Metadata	Administrative Metadata	enable the identifier to be numeric or alpha numeric, or to include the concatenated identifiers of the volume and electronic records above the records in the File Plan.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
45.2.	Metadata	Descriptive Metadata	be able to display the unique identifiers of related items.		
45.3.	Metadata	Administrative Metadata	Date /Time of last edit: The EDRMS must be able to display record date time of last edit based on a standardised convention to be used for the date and time of last edit.		
45.4.	Metadata	Administrative Metadata	Date Booked-in/Checked out: The EDRMS must be able to indicate date record was booked-in/checked out of the system.		
45.5.	Metadata	Administrative Metadata	Date Distributed: The EDRMS must be able to capture the date/time the document/record was distributed based on a standardised convention.		
45.6.	Metadata	Administrative Metadata	Date/Time Created: The EDRMS must be able to generate/display date/time the document was created in the system based on a standardised convention.		
45.7.	Metadata	Administrative Metadata	Application format: The EDRMS must capture information regarding the application (used for processing the original application file).		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
45.8.	Metadata	Descriptive Metadata	• Author: The EDRMS must be able to capture the author of a document as a multiple entry. Author referring also to co-authors, co-collaborators, committees, groups, etc. based on a standardised convention to be used.		
45.9.	Metadata	Descriptive Metadata	• Creator: The EDRMS must be able to capture the creator of a document as a single entry based on a standardised convention to be used.		
45.10.	Metadata	Descriptive Metadata	• Originating Domain: The EDRMS must allow user to indicate from which Institute unit a document originates.		
45.11.	Metadata	Descriptive Metadata	• Record Title: The EDRMS must be able to display an assigned title or description of the record.		
45.12.	Metadata	Descriptive Metadata	• Document Types: The EDRMS must support the definition of different document (or record types) that are associated with a specified set of metadata to be applied at capture.		
45.13.	Metadata	Descriptive Metadata	• Record Type: The EDRMS must be able to display and allow for a default		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
			setting of a list of predefined record types		
45.14.	Metadata	Descriptive Metadata	Version Indicator/Number: The EDRMS must be able to generate the creation version of the record in the electronic repository according to a standardised convention.		
45.15.	Metadata	Descriptive Metadata	Revision Indicator/Number: The EDRMS must be able to generate a sequential number for each revision of a document before it is finalised and declared as a record based on a standardised convention.		
45.16.	Metadata	Descriptive Metadata	State Indicator: The EDRMS must allow user to select from a list of predefined document lifecycle states that are based on standardised conventions to be used.		
45.17.	Metadata	File Plan Administration	File Plan Metadata: The EDRMS must support metadata for all the levels within the File Plan.		
45.17.1.	Metadata	File Plan Administration	The EDRMS must allow the inheritance of metadata values from all the levels in a File Plan down to the record level		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
45.18.	Metadata	Records Management Metadata	Physical Location: The EDRMS must display the physical location of a record.		
45.19.	Metadata	Security Metadata	Access Control List: During creation of a record, the EDRMS must allow users to choose who can view the records based on the access control list.		
45.20.	Metadata	Security Metadata	Access restriction review Date: The EDRMS must capture the access restriction review date.		
45.20.1.	Metadata	Security Metadata	The EDRMS must be able to capture and store information about violations (that is, a user's attempts to access a record or record, including volumes, to which they are denied access), and (where violations can validly be attempted) attempted violations of access control mechanisms.		
45.20.2.	Metadata	Security Metadata	The EDRMS must ensure that only authorised users and administrators can change the content of records management metadata elements.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
45.21.	Metadata	Security Metadata	Security Classification: EDRMS must allow user to select a security classification from a list of predefined security classifications.		
45.22.	Metadata	Structural Metadata	Original Format: EDRMS must be able to capture the original record format.		
45.23.	Metadata	Structural Metadata	Rendered Format: EDRMS must be able to capture the formats to which records have been rendered.		
Records Management					
46.	Records Management	Classify	The EDRMS must support the use of an institutional File Plan.		
47.	Records Management	Classify	The EDRMS must support a File Plan that can represent records (at the function, activity, transaction level) organised in a hierarchy with a minimum of three levels.		
48.	Records Management	Classify	The EDRMS must support the initial and on-going construction of the File Plan.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
49.	Records Management	Classify	The EDRMS must allow the creation of more than one view for the same File Plan.		
50.	Records Management	Create	If the EDRMS provides functionality to capture e-mail as records it must:		
50.1.	Records Management	Create	• Provide capability to capture the e-mail and the attachment as a single record.		
50.2.	Records Management	Create	• Provide capability to capture the e-mail and the attachments as separate records.		
50.3.	Records Management	Create	• Provide capability to capture the e-mail and the attachments as separate but linked records.		
50.4.	Records Management	Create	• Provide capability to capture only the attachments as a record.		
51.	Records Management	Create	The EDRMS must prevent the destruction or deletion of any record by a user.		
52.	Records Management	Create	The EDRMS must prevent the destruction or deletion of any record by an administrator, with the exceptions of:		
52.1.	Records Management	Create	• destruction in accordance with a disposal authority; and		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
52.2.	Records Management	Create	authorised deletion by an administrator.		
53.	Records Management	Create	The EDRMS may permit the administrator to set limitations on the quantity of items associated with a record if required for Institute purposes.		
54.			Alert the Records Manager to records due for disposition before implementing disposal actions, and on confirmation from the Records Manager must be capable of initiating the disposal actions specified in this section		
Search and Retrieval					
55.	Search & Retrieval	File Formats	The EDRMS must allow full text searches on OCR'ed records.		
56.	Search & Retrieval	metadata	The EDRMS must allow users to conduct searches on a combination of both metadata and full text.		
57.	Search & Retrieval	metadata	The EDRMS must allow users to set metadata fields to be displayed as default fields on the retrieval screen.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
58.	Search & Retrieval	Records Management	The EDRMS must allow searching within a single record or across more than one record in the File Plan.		
59.	Search & Retrieval	Search execution	The EDRMS must enable user to browse the File Plan.		
60.	Search & Retrieval	Search execution	The EDRMS must provide word proximity searching that can specify that a word has to appear within a given distance of another word in the record to qualify as a search result		
61.	Search & Retrieval	metadata	The EDRMS must enable users to search using all metadata fields and to sort on all fields.		
62.	Search & Retrieval	Search Execution	The EDRMS may provide for an option to display the latest additions to a domain(s) in a user-defined date/time parameter.		
63.	Search & Retrieval	Search Operators & symbols	The EDRMS must allow specialised users or system administrators to "tweak" the retrieval system to balance precision and recall.		
64.	Search & Retrieval	Search results	The EDRMS must allow full text searches.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
65.	Search & Retrieval	Search results	The EDRMS must allow users to browse taxonomies.		
66.	Search & Retrieval	Search results	The EDRMS must enable users to define personalised search results screens.		
67.	Search & Retrieval	Search results	The EDRMS must provide users with a functionality to add and save favourite searches.		
68.	Search & Retrieval	Search results	The EDRMS must provide a highlight function for search terms indicated search results screen as well as in the document after opening.		
69.	Search & Retrieval	Search results	The EDRMS must provide display formats configurable by users or administrators for search results, including such features and functions as: • select the order in which the search results are presented; • specify the number of search results displayed on the screen; • set the maximum number of search results; • save the search results; and		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
			choose which records management metadata fields are displayed in search result lists.		
70.	Search & Retrieval	Search results	Provide relevance ranking of the search results		
Printing					
71.	Printing	Printing	The EDRMS must provide the user with flexible options for printing records		
72.	Printing	Printing	The EDRMS must allow the user to be able to print out a summary list of selected records (for example, a user specified subset of records management metadata elements (for example, Title, Author, Creation date) for each record		
73.	Printing	Printing	The EDRMS must allow the user to print the results list from all searches		
Email Management					
74.	Email Management	Email Management	The EDRMS must allow users to capture emails (text and attachments)		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
			as single records as well as individual records linked by metadata.		
75.	Email Management	Email Management	The EDRMS must allow individual users to capture email messages (and attachments) from within their email application.		
76.	Email Management	Email Management	The EDRMS must allow users to choose whether to capture emails with attachments as: • email text only; • email text with attachments; or • an attachment only		
77.	Email Management	Email Management	The EDRMS must ensure the capture of email transmission data as metadata persistently linked to the email record.		
Collaboration					
78.	Collaboration	Real-time information exchange.	The EDRMS must support chat rooms, discussion threads, virtual meetings, application and desktop sharing, and white boarding.		
79.	Collaboration	Content sharing.	The EDRMS must allow users to access shared documents, illustrations, photographs, presentations, animation,		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
			video, and other content from a variety of sources.		
80.	Collaboration	Project-based tools.	The EDRMS must provide tools, such as calendars and automatic e-mail alerts, in shared workspaces to support project teams and manage the complexity of project activity.		
81.	Collaboration	Inter-enterprise workflow.	The EDRMS must enable contributors from any institution anywhere in the world to participate seamlessly in collaborative projects.		
82.	Collaboration	Virtual teams.	The EDRMS must provide a workspace for ad hoc assemblies of contributors across disparate functional departments, institutions, geographies, and time zones.		
83.	Collaboration	Integration with EDRMS platform.	The EDRMS must leverage core EDRMS functionalities, such as centralized repositories, workflows, and library services.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
84.	Collaboration	Robust security features.	The EDRMS must provide secure workspaces for collaboration and the ability to invoke SSL encryption, support for digital certificates, and other security features.		
Workflow					
85.	Workflow	Workflow Design	The EDRMS must allow for multiple workflow instances, submitted by multiple users or a single user, must be managed sequentially or concurrently with or without scheduling.		
86.	Workflow	Workflow Design	The EDRMS calendar must distinguish workdays, holidays, and start and end times for the workflow engine.		
87.	Workflow	Workflow Design	The EDRMS may allow for user update-able calendar to ensure workflows are not assigned to absent staff.		
88.	Workflow	Workflow Design	The EDRMS must allow for the integration of third party or external workflow engines.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
89.	Workflow	Workflow Design	The EDRMS must allow a variety of roles within a workflow to be established.		
90.	Workflow	Workflow Design	The EDRMS must allow all document / record types to be attached to a workflow.		
91.	Workflow	Workflow Design	The EDRMS must allow assigning of workflow to roles and users.		
92.	Workflow	Workflow Design	The EDRMS must allow assignment of a workflow to a user, role and or position.		
93.	Workflow	Workflow Design	The EDRMS must allow non-technical authors to create simple workflows.		
94.	Workflow	Workflow Design	The EDRMS must allow target date and times to be assigned to workflows.		
95.	Workflow	Workflow Design	The EDRMS must allow the assignment of a mandatory or optional status to a workflow or workflow step.		
96.	Workflow	Workflow Design	The EDRMS must allow the re-routing of workflow automatically if not responded to within a certain time frame.		
97.	Workflow	Workflow Design	The EDRMS must allow workflow to be assigned based on record type.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
98.	Workflow	Workflow Design	The EDRMS must be able to restrict workflows to specific content object types.		
99.	Workflow	Workflow Design	The EDRMS must cater for substitutions on role, position, person, and user.		
100.	Workflow	Workflow Design	The EDRMS must provide for workflow processes that supports parallel actions.		
101.	Workflow	Workflow Design	The EDRMS must provide for workflow processes that supports sequential actions.		
102.	Workflow	Workflow Design	The EDRMS must provide workflow templates.		
103.	Workflow	Workflow Design	The EDRMS must allow workflow steps to access the related content object, the content object's metadata schemas, metadata elements, and metadata element values (including linked or related content objects), with the ability to update metadata element values.		
104.	Workflow	Workflow Design	The EDRMS must assign a mandatory or optional status to a workflow or workflow step.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
105.	Workflow	Workflow Design	The EDRMS workflow engine must be able to deal with dependencies (i.e. task only can be executed when its input data become available or when a dependent task is completed).		
106.	Workflow	Workflow Design	The EDRMS must provide the functionality to configure basic routing, simple workflows as well as more complex workflows based on lifecycle and flow inclusive of rules.		
107.	Workflow	Workflow Design	Workflow design must enable prototyping of task applications.		
108.	Workflow	Workflow Design	Workflow modelling tools (as part of the EDRMS) must include provisions for expressing roles, positions, structures, dependencies and parameterized inputs or constraints.		
109.	Workflow	Workflow Design	Workflow must allow rules for escalations.		
110.	Workflow	Workflow Design	Workflow must be extended to objects other than documents or records (i.e. Folder or another object).		
111.	Workflow	Workflow Design	Workflows must be graphically designed.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
112.	Workflow	Workflow Management	The EDRMS must allow authorised users to delegate rights to users.		
113.	Workflow	Workflow Management	The EDRMS must allow authorised users to enable and disable notification features.		
114.	Workflow	Workflow Management	The EDRMS must allow non-technical users to change workflow processes.		
115.	Workflow	Workflow Management	The EDRMS must allow users to interact with workflow via client and email.		
116.	Workflow	Workflow Management	The EDRMS must enable authorised users to cancel workflow in a controlled fashion.		
117.	Workflow	Workflow Management	The EDRMS must manage and track sequential and parallel workflow actions.		
118.	Workflow	Workflow Management	The EDRMS must allow workflow steps to re-assign in real time.		
119.	Workflow	Workflow Notifications	The EDRMS must allow a single notification within a defined timeframe.		
120.	Workflow	Workflow Notifications	The EDRMS must be able to immediately notify users when an event occurs that is set to trigger the notification.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
121.	Workflow	Workflow Notifications	The EDRMS must prevent users from switching notifications off.		
122.	Workflow	Workflow Notifications	The EDRMS must provide notification and/or escalations to overdue workflow actions.		
123.	Workflow	Workflow Notifications	The EDRMS must provide reminder notifications as scheduled tasks deadlines approaches.		
124.	Workflow	Workflow Reporting	The EDRMS must allow a full audit trail of triggers, events, participants of a workflow.		
125.	Workflow	Workflow Reporting	The EDRMS must be store workflow execution history.		
126.	Workflow	Workflow Reporting	The EDRMS Workflow engine must track the execution of workflows and must record and display relevant states / status of all the executing workflows.		
127.	Workflow	Workflow Reporting	The EDRMS Workflow system must report on parameters such as Role/Position/Participant status (creators, Reviewers, Approvers, Quality Controllers, Ready, waiting on a dependency, Running, finished (success		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
			or failure), Participant time parameters, Start time, Elapsed time, Finish time.		
128.	Workflow	Workflow Use	The EDRMS must display workflow steps actions and requirements in a text report display.		
Electronic Signatures					
129.	Electronic Signature	Electronic Signature	The EDRMS must be able to retain the information relating to electronic signatures, encryption, and details of related verification agencies		
130.	Electronic Signature	Electronic Signature	The system must include features which allow the integrity of documents bearing electronic signatures to be maintained (and to prove it has been maintained).		
131.	Electronic Signature	Electronic Signature	The EDRMS must have a natural signature capability, as well as an option for auto generation of an E-signature		
132.	Electronic Signature	Electronic Signature	The EDRMS must be able to retain and preserve as metadata, details about the process of verification for an electronic signature		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
133.	Electronic Signature	Electronic Signature	The EDRMS must be capable of checking the validity of an electronic signature		
134.	Electronic Signature	Electronic Signature	The EDRMS should have multiple interfaces for different functions. For example, there should be a capability to provide an E-signature through different devices (mobile, tablet, laptops, desktop computer)		
135.	Electronic Signature	Electronic Signature	The EDRMS must have the ability to automatically detect if changes have been made to a document after it has been signed, and if so, must nullify the signature on the edited document.		
Security					
136.	Security	Security: General	The EDRMS must have the ability to implement industry best practice information security management. (ISO/IEC 17799).		
137.	Security	Security: General	The EDRMS must be able to immediately revoke all access and privileges from a specified group or		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
			selected user(s), thereby preventing access to the EDRMS.		
138.	Security	Security: General	The EDRMS must be capable of implementing a default 'deny' access policy for users and content objects.		
139.	Security	Accountability: Audit Trails	The EDRMS must link electronic signatures to the specific content object and stored as part of the document.		
140.	Security	Accountability: Audit Trails	The EDRMS must keep audit trails of all permission and authorisation changes made to objects, indicating responsibility, action type, date, and time.		
141.	Security	Accountability: Audit Trails	The EDRMS must retain audit trails of all actions performed on objects, indicating responsibility, action type, date, and time.		
142.	Security	Accountability: Monitoring	The EDRMS must allow reporting on audit trails for security.		
143.	Security	Accountability: Monitoring	The EDRMS must enable the downloading of audit trails to utilise for reporting, i.e. .csv files.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
144.	Security	Authentication: User Authentication	The EDRMS must ensure that signatures are date and time stamped.		
145.	Security	Authentication: User Authentication	The EDRMS must ensure that signatures include the identity of the person providing the signature as well as a justification for signing.		
146.	Security	Authentication: User Authentication	The EDRMS must ensure remote devices and external EDRMSs use strong authentication mechanisms when accessing EDRMS resources.		
147.	Security	Authentication: User Authentication	The EDRMS must ensure that authentication is encrypted when stored or transmitted.		
148.	Security	Authorisation: Privilege Management	The EDRMS must ensure that, based on permission levels (Read Permission), the hit list only shows documents/records that the user has access to.		
149.	Security	Authorisation: Privilege Management	Must the default access restriction for a specific document need to be adjusted, the EDRMS must allow the option to specify the audience (person / group / role / function / area) as well as the		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
			necessary permissions that must be allocated.		
150.	Security	Authorisation: Privilege Management	The EDRMS must ensure that the administrator is able to alter the security category of individual records.		
151.	Security	Authorisation: Privilege Management	The EDRMS must ensure that an end user cannot use the EDRMS in any way to identify the presence of objects which they are not unauthorised to see.		
152.	Security	Authorisation: Privilege Management	The EDRMS must allow establishment of discrete access rights for all objects (including custom objects and functions).		
153.	Security	Authorisation: Privilege Management	The EDRMS must allow nominated end-users to assign security levels and temporary privileges to nominated users to access nominated content objects to which the end user already has access (e.g.; delegate rights downstream).		
154.	Security	Authorisation: Privilege Management	The EDRMS must allow nominated end-users to have temporary privileges to nominated content objects in a workflow.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
155.	Security	Authorisation: Privilege Management	The EDRMS must assign security levels to individual authors/users or groups of authors/users.		
156.	Security	Authorisation: Privilege Management	The EDRMS must assign security levels to individual content objects or content collections.		
157.	Security	Authorisation: Privilege Management	The EDRMS must grant or withhold specific permissions based on role and assigned security level of content object and directory.		
158.	Security	Authorisation: Privilege Management	The EDRMS must provide ability for administrators (or nominated roles) to override access controls to release/unlock content objects.		
159.	Security	Authorisation: Privilege Management	The EDRMS must provide security levels that can be set by the EDRMS administrator and nominated roles.		
160.	Security	Authorisation: Privilege Management	The EDRMS must restrict access to metadata element values based on the security.		
161.	Security	Authorisation: Privilege Management	The EDRMS must restrict content object metadata element value view access		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
			rights, based on a discrete role or privilege.		
162.	Security	Authorisation: Privilege Management	The EDRMS must restrict content object print access rights, based on a discrete role or privilege.		
163.	Security	Authorisation: Privilege Management	The EDRMS must restrict content objects search and reporting access rights, based on a discrete role or privilege.		
164.	Security	Authorisation: Privilege Management	The EDRMS must restrict modifications to metadata element values based on the security		
165.	Security	Authorisation: Privilege Management	The EDRMS must restrict object delete and destroy access rights, based on a discrete role or privilege.		
166.	Security	Authorisation: Privilege Management	The EDRMS must restrict object delete and destroy access rights, based on a discrete role or privilege.		
167.	Security	Authorisation: Privilege Management	The EDRMS must restrict object editing, access rights, based on a discrete role or privilege.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
168.	Security	Authorisation: Privilege Management	The EDRMS must restrict object view only access rights, based on a discrete role or privilege.		
169.	Security	Authorisation: Privilege Management	The EDRMS must restrict viewing metadata element values based on the security.		
170.	Security	Authorisation: Privilege Management	The EDRMS must separate internal and external authors/users to ensure explicit privacy.		
171.	Security	Authorisation: Role Management	The EDRMS must restrict access using authentication processes.		
172.	Security	Authorisation: Role Management	The EDRMS must assign authors/users to one or multiple roles on a permanent basis.		
173.	Security	Authorisation: Role Management	The EDRMS must assign role access requirements to a content object in the user repository.		
174.	Security	Authorisation: Role Management	The EDRMS must be capable of assigning a user multiple roles on a temporary basis.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
175.	Security	Authorisation: Role Management	The EDRMS must define role access requirements to content collections in the user repository.		
176.	Security	Authorisation: Role Management	The EDRMS must define roles within repository		
177.	Security	Authorisation: User Profiles	The EDRMS must restrict create rights to documents according to group.		
178.	Security	Authorisation: User Profiles	The EDRMS must restrict create rights to documents according to type of author.		
179.	Security	Authorisation: User Profiles	The EDRMS must restrict delete rights to documents according to author profiles.		
180.	Security	Authorisation: User Profiles	The EDRMS must restrict delete rights to documents according to group.		
181.	Security	Authorisation: User Profiles	The EDRMS must restrict delete rights to documents according to type of author.		
182.	Security	Authorisation: User Profiles	The EDRMS must restrict modify rights to documents according to author profiles.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
183.	Security	Authorisation: User Profiles	The EDRMS must restrict modify rights to documents according to group.		
184.	Security	Authorisation: User Profiles	The EDRMS must restrict modify rights to documents according to type of author.		
185.	Security	Authorisation: User Profiles	The EDRMS must restrict read rights to documents according to author profiles.		
186.	Security	Authorisation: User Profiles	The EDRMS must restrict read rights to documents according to group.		
187.	Security	Authorisation: User Profiles	The EDRMS must restrict read rights to documents according to type of author.		
188.	Security	Authorisation: User Profiles	The EDRMS must restrict write rights to documents according to author profiles.		
189.	Security	Authorisation: User Profiles	The EDRMS must restrict write rights to documents according to group.		
190.	Security	Authorisation: User Profiles	The EDRMS must restrict write rights to documents according to type of author.		
191.	Security	Identification: Directory Management	The EDRMS must integrate with a user profile directory structure where user profile attributes are available and updateable from within the repository.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
192.	Security	Identification: Directory Management	The EDRMS must store agency management structure hierarchically, i.e. a unique ID for each staff member, their location, reporting structure: e.g.: Division, Unit, Workgroup, Manager, External user/structure.		
193.	Security	Identification: Directory Management	The EDRMS must support a staff/location data directory that can be synchronised automatically via two-way interface with an external master directory.		
194.	Security	Identification: External User Identity Integration	The EDRMS must have the ability to integrate with a groups/rights repository in real-time: Where the groups/rights repository is a Microsoft Active Directory		
195.	Security	Identification: External User Identity Integration	The EDRMS must have the ability to synchronise with a user repository at scheduled times:		
195.1.	Security	Identification: Logon Procedures	The number of logon attempts must be limited by the EDRMS.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
196.	Security	Identification: Logon Procedures	The EDRMS must, after the number of logon attempts has been exceeded enforce a cool-off period.		
197.	Security	Identification: Logon Procedures	The EDRMS must ensure that application identifiers do not display until the logon process has been successfully completed.		
198.	Security	Identification: Password Management	The EDRMS must provide username and password management facilities such that:		
198.1.	Security	Identification: Password Management	• username length can be enforced.		
198.2.	Security	Identification: Password Management	• password length and composition can be enforced.		
198.3.	Security	Identification: Password Management	• password changes must be enforced after defined periods.		
198.4.	Security	Identification: Password Management	• password changes must be enforced after first use.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
198.5.	Security	Identification: Password Management	passwords cannot be reused.		
198.6.	Security	Identification: Password Management	usernames cannot be reused.		
Audit Trails					
199.	General	Audit Trail	The EDRMS must allow all authentication attempts (whether successful or not) to be tracked in the audit log to enable subsequent analysis of any authentication issue.		
200.	General	Audit Trail	The EDRMS must provide enable every event that is captured for audit trail purposes to include a user identifier and time stamp, if the activity is part of a workflow, the thread of events need to be recorded in the audit trail.		
201.	General	Audit Trail	The EDRMS must include the following in the audit trail record - Date and time of event. - User identity.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
			• Event type. • Success or failure of action. • Name of object, if any. • Origin of a request for identification/authentication / access request or permission (e.g. computer ID and User ID).		
Hybrid Records Management					
202.	Records Management	Store	The EDRMS must be able to define in the classification scheme non-electronic records and volumes, and must allow the presence of nonelectronic records in these volumes to be reflected and managed in the same way as electronic records		
203.	Records Management	Manage	The system must allow both kinds of records to be managed in an integrated manner.		
204.	Records Management	Manage	The EDRMS must allow a different records management metadata element to set to be configured for non-electronic		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
			and electronic records; nonelectronic records management metadata must include information on the physical location of the non-electronic record.		
205.	Records Management	Manage	The EDRMS must ensure that retrieval of non-electronic records displays the records management metadata for both electronic and non-electronic records associated with it.		
206.	Records Management	Manage	The EDRMS must include features to control and record access to non-electronic records, including controls based on security category, which are comparable with the features for electronic records.		
207.	Records Management	Manage	The EDRMS must support tracking of non-electronic records by the provision of request, check-out and check-in facilities that reflect the current location of the item concerned.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
208.	Records Management	Manage	The EDRMS must be capable of offering check-out and check-in facilities for nonelectronic records profiled in the system, in particular enabling the ability to record a specific user or location to which a non-electronic record is checked out, and to display this information if the nonelectronic record is requested by another user		
209.	Records Management	Manage	The EDRMS must support the retention and disposal protocols and routinely apply to both electronic and non-electronic elements.		
210.	Records Management	Manage	The EDRMS must ensure that a non-electronic record is allocated the same security category as an associated electronic record.		
211.	Records Management	Manage	The EDRMS must be capable of offering a request facility for non-electronic records profiled in the hybrid records system, enabling a user to enter a date		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
			that the non-electronic element is required and generating a consequent message for transmission to the current holder of that nonelectronic records or the Records Manager, according to configuration		
212.	Records Management	Dispose	The EDRMS must support the application of the same disposition authority to both the electronic and non-electronic records that make up a hybrid record.		
213.	Records Management	Dispose	The EDRMS must require the Records Manager to confirm that the non-electronic record has been transferred, exported, or destroyed before transferring, exporting, or destroying the electronic part.		
System Integration					
214.	System Integration	System Integration	The EDRMS must be able to integrate with SANBI Systems which include but not limited to the following: Sage Iqual HR Manage Barnowl		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
			DSpace/Opus Seis BGIS		
System Functions					
215.	System Functions	Administrator Functions	The EDRMS must allow the administrator to retrieve, display and re-configure system parameters and to re-allocate users and functions between user roles.		
216.	System Functions	Administrator Functions	The EDRMS must provide back-up facilities so that records and their records management metadata can be recreated using a combination of restored back-ups and metadata.		
217.	System Functions	Administrator Functions	The EDRMS must provide recovery and rollback facilities in the case of system failure or update error and must notify the authorised users of the results.		
218.	System Functions	Administrator Functions	The EDRMS must monitor available storage space and notify the		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
			administrator when action is needed because available space is at a low level or because it needs other administrative attention		
219.	System Functions	Administrator Functions	The EDRMS must allow the Records Manager to make bulk changes to the classification scheme, ensuring all records management metadata are handled correctly and completely at all times, in order to make the following kinds of organisational change: • division of an organisational unit into two; • combination of two organisational units into one; • movement or re-naming of an organisational unit; and • division of a whole organisation into two organisations.		
220.	System Functions	Administrator Functions	The EDRMS must support the movement of users between organisational units.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
221.	System Functions	Administrator Functions	The EDRMS must allow the definition of user roles and must allow several users to be associated with each role.		
222.	System Functions	Administrator Functions	The EDRMS must communicate any errors encountered in saving data to storage media		
223.	System Functions	Back Up and Recovery	The EDRMS must provide automated back-up and recovery procedures.		
224.	System Functions	Back Up and Recovery	The EDRMS must allow authorised users to schedule back-up routines by: • specifying the frequency of back-up; and • allocating storage media, system, or location for the back-up (for example, offline storage, separate system, remote site).		
225.	System Functions	Back Up and Recovery	The EDRMS must allow only the administrator to restore from electronic records management system back-ups. Full integrity of the data must be maintained after restoration.		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
226.	System Functions	Back Up and Recovery	The EDRMS must allow only authorised users to roll-forward the electronic records management system from a back-up to a more recent state, maintaining 62 full integrity of the data.		
227.	System Functions	Back Up and Recovery	The EDRMS must be able to notify users whose updates may have been incompletely recovered, when they next use the system, that a potentially incomplete recovery has been executed.		
Training					
228.	Training	Training Plan	A comprehensive training plan that outlines the objectives, needs, strategy, and curriculum to be addressed when training users on the EDRMS must be provided.		
229.	Training	User Training	Users must be trained in the use of the EDRMS system, covering all functionality the system offers		

No	Component	Area	Requirement	Compliance (Yes, No, Partly)	Comments and explanations if needed
230.	Training	Super User Training	This group of users must be trained to be the first line of support when users encounter issues with the system		
231.	Training	Train the Trainer	The users will eventually train users on the system		
232.	Training	Administrator Training	These users must be trained to administer the system and be able to add users, customise the database, create a predefined workflow and other administrative functions.		
233.	Training	Training Manuals	Manuals must be created and customised for all the above-mentioned courses and these manuals become the property of SANBI.		
Change Management					
234.	Change Management	Change Management Strategy and Plan	A change management strategy and plan detailing the direction and purpose for all change management activities must be provided		
235.	Change Management	Change Management Activities	All activities included in the Change Management plan must be executed.		

Appendix B: Required Metadata (From NARSSA Minimum Mandatory Metadata Requirements)

Metadata Element	Description
IDENTITY	
Unique identifier*	The system ID that uniquely identifies a particular record and distinguishes an object from others in a database.
Record title*	The title of the record given to it by the user. Must be a sensible name to assist with identification and retrieval. To be done according to a file naming convention where applicable. For e-mail messages usually the subject line of the message, however if the subject line is not a sensible description of the content of the message it must be able to be edited in the metadata capturing form.
Main series description	The main series title as it appears in the file plan. To populate automatically when lowest level subject is chosen.
Sub-series description	The sub series as it appears in the file plan. To populate automatically when lowest level subject is chosen. Repeatable depending on number of levels in the file plan.
File plan subject*	The formal subject of the folder as it appears in the file plan. To be picked by the user when creating a record or by the indexer at scanning time.
Folder volume/part number*	The consecutive number of the file/folder part as it appears in the file plan. The system must only allow filing in open folders and must populate the volume number automatically when a subject is chosen.
CONTEXT	

Metadata Element	Description
Author/originator/creator*	The intelligent name, rather than login id, of the person or team that is the author of the record. Preferably picked up from the network log-in. The person by who an e-mail was sent. Preferably picked up from the e-mail transmission data. The person who signed the paper-based record that was scanned/profiled into the system. This would be a user entry at scanning station.
Originating organization	The name of the specific unit in the organization in which the original record was created. Preferably picked up from the network log in if created internally. If the record was e-mailed this must preferably be picked up from the transmission data. If not, possible it must be user defined. If received from outside in paper-based format and scanned/indexed into the system it must be user defined at the scanning station at time of indexing.
Originating sub-office/unit	The name of the specific sub office/directorate/branch in the organization where the record was created. This must preferably be picked up from the network log in. If the record was e-mailed the information must be picked up from the transmission data. If received from outside in paper-based format and scanned/indexed into the system it must be captured at time of indexing.
Name of person who declared the record	The intelligent name, rather than login id, of the person that declared the record. It is the point at which the record came under the full control of the system. The information is necessary to prove the integrity of a record for admissibility purposes.

Metadata Element	Description
Addressee	Mandatory for e-mail. Preferably picked up from transmission data. Optional for other record types. Identifying the person(s) the record was dispatched to.
Distribution list/Recipients	Mandatory for e-mail. Preferably picked up from transmission data. The intelligent names of all recipients of an e-mail message.
RELATIONSHIPS	
Related file/folder	Identifies instances where records have direct relationships to other records, e.g. in a specific business process. Will assist in managing disposal conflicts, and the provision of information in terms of the Promotion of Access to Information Act, as well as with issues of legal admissibility.
Linkage between record elements	To enable the linking together of physically separate records or elements that constitute the complete record (for example, an attachment to an e-mail message, an e-form and its data, metadata).
DATE INFORMATION	
Creation date	the date that the document was first created prior to being declared as a record or the date of the e-mail sent/received. This must be generated by the system The date on the paper-based record that was scanned /indexed into the system. The date format is ccyy-mm-dd.
Date checked in	The date the record was checked into the system. The date format is ccyy-mm-dd.

Metadata Element	Description
Date declared as record	The date on which the document was declared as a record and entered into the electronic repository. It is the point at which the record came under the full control of the system. The information is necessary to prove the integrity of a record for admissibility purposes. The date format is ccyy-mm-dd.
Folder open/close dates*	The date the folder was created (or on which the first record was added) and the date the folder was closed (or on which the last record was added). The date format is ccyy-mm-dd.
Part/volume open/close dates*	The date the specific part or volume of the folder was created (or on which the first record was added) and the date the part or volume of the folder was closed (or on which the last record was added). This date will be used to calculate retention periods. The date format is ccyy-mm-dd.
Date/time delivered	Mandatory for e-mail. The date and time an e-mail was delivered into another system. The information is necessary to prove the integrity of a record for admissibility purposes. The date format is ccyy-mm-dd.
Date/time received	Mandatory for e-mail. The date and time an e-mail was received. The information is necessary to prove the integrity of a record for admissibility purposes. The date format is ccyy-mm-dd.

Metadata Element	Description
Date of last edit	Date of last changes made to the document before it was declared a record. The information is necessary to prove the integrity of a record for admissibility purposes. The date format is ccyy-mm-dd.
Record version creation date	Creation date of record version in the electronic repository. The information is necessary to prove the integrity of a record for admissibility purposes. The date format is ccyy-mm-dd.
VERSION CONTROL	
Document revision number	A sequential number for each revision of a document, before it is finalized and declared a record.
Record version number	A sequential number for each version of a record kept in the electronic repository.
ACCESS CONTROL	
Access restrictions	Identifying restrictions on access to the record as a whole by indicating permission to user and groups. Will be inherited from the file plan, and the record type.
Access restriction review date	The date, preferably annual, on which the access restrictions must be reviewed.
Security classification	Level of security classification, which will have implications for user access restrictions, as indicated by the Minimum Information Security Standard. Will be inherited from the file plan and record type or set by users.
Sensitivity review date	The date at, or time period after, which a review of the security classification is appropriate.
DISPOSAL CONTROL	

Metadata Element	Description
Disposal instruction	The action to be taken at the end of the life cycle of the record, e.g. destroy/delete or keep permanently. Inherited from the specific record type and the disposal schedule. Based on written disposal authority issued by National Archives and Records Service.
Retention period	The standard period of time for which records must be retained before the disposal action is carried out. Inherited from the specific record type and the disposal schedule.
Disposal authority number*	The unique disposal authority number issued by the National/Provincial Archives that authorises the action to be taken against the record. Inherited from the specific record type and the disposal schedule.
Disposal action review date	The date on which the scheduled disposal action was reviewed. The date format is ccyy-mm-dd.
Disposal action review comments	A textual description indication why the disposal action was reviewed and what decision has been taken against the record.
Destruction/ transfer date*	The date on which the records were destroyed/transferred. The date format is ccyy-mm-dd.
Identity of person authorizing the review/destruction/ transfer*	The intelligent name, rather than login id, of the person that authorised the review of the disposal instruction of the records and/or who authorised the destruction/deletion/transfer of the records.
Transfer location	A textual description of the location the records were transferred to.

Metadata Element	Description
RECORD TYPE	
Record type	A description identifying the logical document/record types – e.g. report, memo, letter, which may be a useful aid to identification or processing choices, and which is used as a disposal mechanism. When not inherited from a document template, the user must define from a pick list.
PRESENTATION AND MEDIUM	
Storage medium	Indicates the medium on which a record is kept e.g. paper, CD, magnetic tape, etc.
Format	The physical application format type/file e.g. the 3-letter file type, such as .doc, .ppt, .gif, .msg, used in a Windows environment.
Presentation format	Linking between versions where the same record is held in different formats for preservation and for viewing, or where sensitivity editing has resulted in creation of a variant version.
Language	Identify the language the records were created in to enable retrieval and linking to translations that might exist.
LOCATION INFORMATION	
Physical location	Physical storage location of the paper-based file and its contents. Also the location of electronic records within a hierarchical storage management system.
Barcode (paper)	Identifying label for paper files, or the paper or hard copy element of hybrid assemblies, only.
SYSTEM INFORMATION	
Technical platform	Information regarding the platform application and format on which the records were generated.
VITAL RECORD INFORMATION	

Metadata Element	Description
Vital record indicator	An indication if the records: protect the enduring civil, legal, financial, property and other rights of the citizens of a country. These records may never be destroyed. They are needed to continue operational responsibilities under disaster conditions. Office is to decide how many years' worth of records are needed to continue operating in disaster conditions – this will influence the retention period. protect the legal and financial rights of the governmental body. Office is to decide how many years' worth of records are needed to continue operating in disaster conditions – this will influence the retention period.
Vital record review date	The date at, or time period after, which a review of the vital record status is appropriate.
AUDIT INFORMATION	
Audit trail	Identification of users who have taken significant actions on the record through its lifecycle, the action taken (for example: create, edit, copy to new version, delete/transfer, etc), the date the action was taken.